

**НИЧТО ТАК  
НЕ ГОВОРИТ  
О ИБ, КАК  
ДЕСЯТОК  
ФАЙЕРВОЛ  
ЛОВ И  
БИОМЕТРИ  
ЧЕСКИЙ  
СКАНЕР**

---

### **Больше контента:**

[BOOSTY.TO](#)

[SPONSR.RU](#)

[TELEGRAM](#)

---

### **Бесплатное издание**

Для новичков в мире ИБ или для тех, кто предпочитает работать с контентом без финансовых обязательств.

---

### **Обычный читатель**

Для постоянных читателей, которые заинтересованы быть в курсе последних тенденций в мире кибербезопасности

---

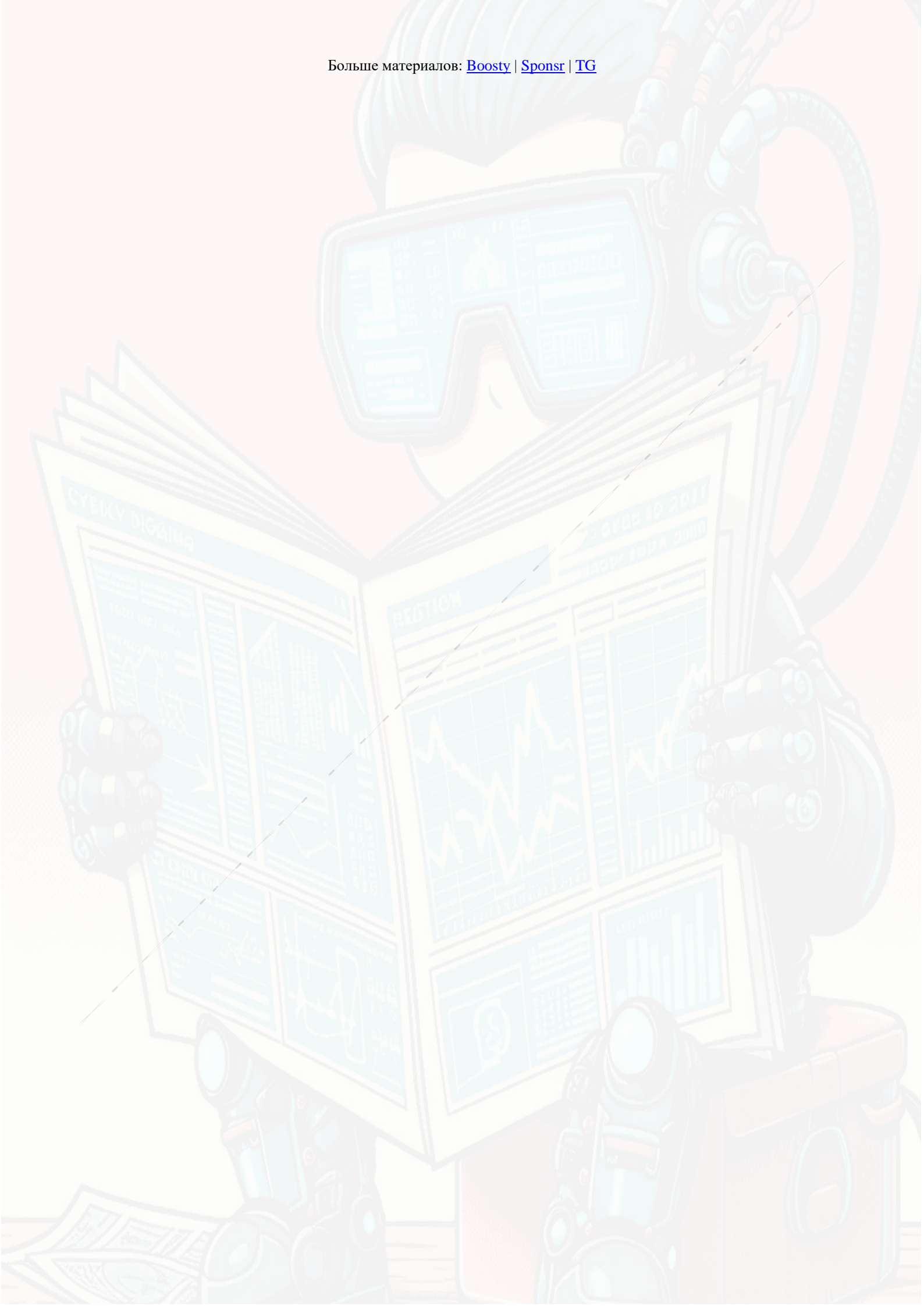
### **Профессионал**

Для ИТ-специалистов, экспертов, и энтузиастов, которые готовы погрузиться в сложный мир ИБ.

# **ХРОНИКИ БЕЗОПАСНИКА**

## **ДАЙДЖЕСТ. 2024 / 04**

Добро пожаловать в очередной выпуск ежемесячного сборника материалов, который является вашим универсальным ресурсом для получения информации о самых последних разработках, аналитических материалах и лучших практиках в постоянно развивающейся области безопасности. В этом выпуске мы подготовили разнообразную подборку статей, новостей и результатов исследований, рассчитанных как на профессионалов, так и на обычных любителей. Цель нашего дайджеста - сделать наш контент интересным и доступным. Приятного чтения!





# НОВОСТИ



## SHARPADWS.

SHARPADWS то инструмент, разработанный для Red Team, который фокусируется на разведке и эксплуатации сред Active Directory (AD) с помощью протокола веб-служб Active Directory (ADWS). В отличие от традиционных методов взаимодействия с Active Directory, которые часто используют облегченный протокол доступа к каталогам (LDAP), SharpADWS использует ADWS для выполнения своих операций. SharpADWS может выполнять различные действия без прямой связи с сервером LDAP. Вместо этого запросы LDAP облекаются в SOAP-сообщения и отправляются на сервер ADWS, который затем распаковывает и пересылает их на сервер LDAP. Это может привести к тому, что в журналах будет отображаться, что запросы LDAP исходят с локального адреса 127.0.0.1, что может быть пропущено системами безопасности.



## FIREBASE

Firestore – это платформа, которая как и другие, требует от разработчиков использования механизмов защиты. Однако, похоже, что разработчики либо не прошли необходимого обучения по безопасности, либо не выделили достаточно времени на протяжении жизненного цикла разработки, чтобы применить правильные средства контроля безопасности

### Причины неправильных настроек Firestore

Неправильные настройки экземпляров Firestore, которые привели к раскрытию 19 миллионов паролей в виде открытого текста и конфиденциальных пользовательских данных, в основном были вызваны двумя факторами:

♦ **Отсутствие настроек безопасности:** В некоторых экземплярах Firestore не были включены механизмы защиты, которые должны были выступать в качестве первой линии защиты от несанкционированного доступа.

♦ **Неправильная настройка:** настройки были настроены неправильно, что позволила сделать общедоступными данные, которые должны были быть конфиденциальными.

### Отрасли:

♦ **Розничная торговля и гостиничный бизнес:** сети быстрого питания и другие предприятия розничной торговли оказались в числе пострадавших, в частности, в результате внедрения Firestore в Chattr, данные пользователей были раскрыты.

♦ **Здравоохранение:** приложения для здравоохранения "публиковали" личные семейные фотографии и ID токены.

♦ **Электронная коммерция:** на платформах электронной коммерции произошла утечка данных с платформ обмена криптовалютами.

♦ **Образование:** Система управления обучением для преподавателей и студентов подверглась утечке 27 миллионах данных.

♦ **Разработка технологий и приложений:** проблема затронула широкий спектр мобильных и веб-приложений в различных секторах, т.к. Firestore используется как составной компонент в составе многих решений



## СЛУЧАИ НАРУШЕНИЯ ДОВЕРИЯ И БЕЗОПАСНОСТИ В ВВС США

♦ Подрядчик ВМС США, который в 2007 году внедрил вредоносный код в программное обеспечение системы обнаружения угроз на подводной лодке. Этот акт был преднамеренным саботажем, который мог поставить под угрозу безопасность и эксплуатационные возможности подводной лодки. Вредоносный код в таких критически важных системах потенциально мог отключить обнаружение угроз, что привело бы к необнаруженным навигационным опасностям или действиям противника.

♦ Роберт Бирчам, офицер разведки ВВС США в отставке, который был приговорен к трем годам заключения в федеральной тюрьме за незаконное хранение секретных документов. Бирчам, вышедший в отставку в 2018 году в звании подполковника, проработал 29 лет на различных должностях в разведке, включая должности, которые требовали от него работы с секретной разведывательной информацией для Объединенного командования специальных операций,

♦ Гарольд Мартин, бывший сотрудник Агентства национальной безопасности, был арестован в августе 2016 года за кражу и хранение особо секретных документов, которые хранились в течение 20 лет. Мартин хранил эти документы в своем доме и автомобиле. Украденные документы содержали конфиденциальную информацию о планировании АНБ, сборе разведданных, возможностях киберкомандования США и проблемах в кибервозможностях США.

♦ Джерри Чун Шинг Ли, бывший сотрудник ЦРУ, был арестован в январе 2018 года по обвинению в незаконном хранении информации о национальной обороне. У Ли были записные книжки, в которых содержались рукописные записи с секретной информацией, включая настоящие имена и номера телефонов сотрудников и секретные оперативные заметки ЦРУ.

♦ Джек Тейшейра, военнослужащий Национальной гвардии ВВС Массачусетса, признал себя виновным в утечке секретных военных документов в социальные сети.



## EDR TELEMETRY

Проект EDR Telemetry (github) направлен на отслеживание и сравнение функций телеметрии, реализованных в различных системах EDR для Windows. Документ представляет собой сравнительную таблицу телеметрии, в которой подробно описаны возможности различных продуктов EDR по сбору определенных типов телеметрических данных, имеющих отношение к кибербезопасности.

✦ В CrowdStrike и Microsoft Defender реализованы комплексные функции в нескольких категориях. В обоих продуктах большое количество функций, отмеченных как полностью реализованные (✓), в различных категориях функций телеметрии. Это указывает на широкий охват с точки зрения возможностей сбора телеметрических данных, что имеет решающее значение для эффективного обнаружения конечных точек и реагирования на них.

✦ С другой стороны, WatchGuard и Harfanglab обладают значительным количеством функций, помеченных как не реализованные (✗) или частично реализованные (⚠). Это говорит о том, что у этих продуктов могут быть пробелы в возможностях сбора телеметрических данных по сравнению с другими продуктами EDR, перечисленными в документе.



## META PIXEL TRACKER

Исследователи в области ИБ недавно обнаружили сложную операцию по скиммингу кредитных карт, которая умело маскируется под безобидный Facebook-трекер, а именно поддельный скрипт Meta Pixel tracker.

### ✦ Механизм атаки

Злоумышленники пользуются доверием к широко известным скриптам, таким как Google Analytics или jQuery, называя свои вредоносные скрипты так, чтобы они имитировали эти легитимные сервисы. Поддельный скрипт Meta Pixel tracker при ближайшем рассмотрении обнаруживает код JavaScript, который заменяет ссылки на законный домен "connect.facebook[.]net" на "b-connected[.]com", законный веб-сайт электронной коммерции, который был взломан для размещения кода скиммера. Такая подмена является ключевой, поскольку позволяет вредоносному коду выполняться под видом легитимного сервиса

### ✦ Схема процесса

Как только вредоносный скрипт загружается на взломанный веб-сайт, он отслеживает определенные действия, например переход посетителя на страницу оформления заказа. На этом этапе он служит для мошеннического наложения, предназначенного для перехвата данных кредитной карты, введенных жертвой. Затем украденная информация передается на другой взломанный сайт, www.donjuguetes[.]es, что демонстрирует многоуровневый характер этой атаки

### ✦ Последствия

Этот инцидент подчёркивает важность бдительности и надёжных методов обеспечения безопасности для владельцев веб-сайтов, особенно для тех, кто использует платформы электронной коммерции. Использование поддельных скриптов, имитирующих законные сервисы, является хитрой стратегией, которая может легко обмануть даже самых осторожных пользователей. Таким образом, для обнаружения и устранения таких угроз важно применять комплексные меры безопасности, включая использование систем обнаружения вторжений и мониторинг веб-сайтов



## WHAT2LOG

What2Log - блог, посвящённый обсуждению различных аспектов управления журналами и их анализа, где публикуются обновления инструмента What2Log, информация о конкретных функциях ведения журнала и обсуждения проблем, связанных с управлением журналами:

✦ **Раздел обновлений:** В блоге представлены подробные сведения о новых версиях инструмента What2Log.

✦ **EventRecordID:** В одной из записей блога упоминается EventRecordID - скрытый XML-тег в журналах событий Windows, который расширяет информацию журнала.

✦ **Идентификатор события 4672:** В одной из записей блога обсуждается значение идентификатора события 4672 в Windows, который регистрирует специальные привилегии, назначенные новым пользователям для входа в систему.

✦ **Проблемы управления журналами:** В нескольких публикациях из серии блогов рассматриваются различные проблемы управления журналами, включая управление объемом журналов, анализ журналов, корреляцию событий и агрегацию журналов. В этих публикациях рассматриваются сложности и необходимые соображения для эффективного управления журналами и их анализа.

В целом, блог служит ресурсом для людей, интересующихся техническими аспектами ведения журналов, предлагая как образовательный контент, так и обновления по инструменту What2Log на Github

## ATTACKGEN



Проект предоставляет инструмент тестирования реагирования на инциденты в области кибербезопасности, который объединяет большие языковые модели с платформой MITRE ATT&CK для создания индивидуальных сценариев реагирования на инциденты

♦ **Формирование сценариев:** AttackGen может генерировать уникальные сценарии реагирования на инциденты на основе выбранных групп участников угроз

♦ **Настройка:** пользователи могут указывать размер организации и отрасль для сценариев, адаптированных к их конкретному контексту

♦ **Интеграция MITRE ATT&CK:** Инструмент отображает подробный список методов, используемых выбранной группой участников угроз, в соответствии с платформой MITRE ATT&CK

♦ **Пользовательские сценарии:** Есть возможность создавать пользовательские сценарии на основе выбранных методов ATT&CK

♦ **Сбор отзывов:** в AttackGen включена функция сбора отзывов пользователей о качестве создаваемых сценариев

♦ **Контейнер Docker:** Инструмент доступен в виде образа контейнера Docker для упрощения развертывания

♦ **Запуск инструмента:** приведены инструкции по запуску программы AttackGen и переходу к указанному URL-адресу в веб-браузере

♦ **Выбор сценария:** Пользователи могут выбрать отрасль компании, размер и желаемую группу участников угроз для создания сценариев



## ИНТЕГРАЦИЯ EVILGINX С GOPHISH

С очередным обновлением расширяется возможность для целей фишинговых кампаний. Эти обновления Evilginx и его интеграция с GoPhish представляют собой значительный прогресс в технологии фишинговых кампаний, предлагая пользователям более совершенные инструменты для создания попыток фишинга и управления ими с расширенными возможностями настройки и отслеживания.

♦ **Интеграция с GoPhish:** Evilginx теперь официально интегрируется с GoPhish. Это позволяет пользователям создавать фишинговые кампании, которые отправляют электронные письма с URL-адресами Evilginx, используя пользовательский интерфейс GoPhish для мониторинга эффективности кампаний, включая открытие электронной почты, переходы по URL-адресу и успешные перехваты сеансов.

♦ **Усовершенствования API:** В обновлении добавлены дополнительные API в GoPhish, позволяющие изменять статус результатов для каждого отправленного электронного письма. Это улучшение способствует более эффективному управлению кампанией.

♦ **Формирование URL-адреса ("приманки"):** При создании кампании в GoPhish пользователи больше не выбирают "Целевую страницу". Вместо этого они формируют URL-адрес в Evilginx и вводят его в текстовое поле "URL-адрес приманки Evilginx". Этот процесс упрощает создание фишинговых кампаний.

♦ **Пользовательские параметры и персонализация:** GoPhish автоматически формирует зашифрованные пользовательские параметры с персонализированным содержанием для каждой ссылки, встроенной в сгенерированные сообщения электронной почты. Эти параметры включают ФИО и адрес электронной почты получателя. Эта функция позволяет настраивать фишинговые страницы с помощью скриптов js\_inject, повышая эффективность попыток фишинга.

♦ **Расширенная поддержка TLD:** Evilginx расширила поддержку новых доменов верхнего уровня (TLD), чтобы повысить эффективность обнаружения URL-адресов в прокси-пакетах. Обновленный список включает в себя множество доменов верхнего уровня, таких как .aero, .agra, .biz, .cloud, .gov, .info, .net, .org и многие другие, включая все известные двухсимвольные домены верхнего уровня.

\*\* Evilginx и GoPhish — это инструменты, используемые в сфере кибербезопасности, в частности, в контексте моделирования фишинга и платформ для атак типа "человек посередине" (MitM). Они служат разным целям, но могут использоваться вместе для улучшения фишинговых кампаний и тестирования безопасности.

♦ **Evilginx** — это платформа для атак типа "человек посередине", которая может обходить механизмы двухфакторной аутентификации (2FA).

Он работает путём обмана пользователя, заставляя его перейти на прокси-сайт, который выглядит как легитимный сайт, который он намеревается посетить. Когда пользователь входит в систему и передаёт учётные и MFA данные, Evilginx получает эти данные пользователя и токен аутентификации. Этот метод позволяет злоумышленнику повторно использовать токен и получить доступ к целевому сервису в качестве пользователя, эффективно обходя защиту 2FA.

♦ **GoPhish** — это набор инструментов для фишинга с открытым исходным кодом, предназначенный для предприятий и специалистов по безопасности для проведения тренингов по повышению уровня безопасности и моделирования фишинга, который позволяет создавать и отслеживать эффективность фишинговых кампаний, включая открытие электронной почты, переходы по ссылкам и отправку данных на фишинговые страницы.

## SHARPTERMINATOR

Инструмент Terminator является частью класса атак, известного как "Принеси уязвимый драйвер" (BYOVD). Эта стратегия предполагает использование легитимных, но уязвимых драйверов для обхода мер безопасности, прерывания процессов защиты от вирусов и EDR и выполнения вредоносных действий без обнаружения.

### Особенности угрозы эксплуатации инструмента

Инструмент Terminator представляет собой серьёзную угрозу из-за своей способности отключать защитные решения, тем самым способствуя целому ряду вредоносных действий. Эти действия могут варьироваться от развёртывания дополнительных вредоносных программ до масштабной компрометации системы и сбоев в работе.

### Техническая сложность и проблемы с оценкой рисков

Оценить риск, связанный с инструментарием Terminator, сложно по ряду причин. К ним относятся эволюционирующий характер инструмента, разнообразие и масштаб применения, а также диапазон потенциальных целей. Точный процент успеха Terminator в компрометации организаций трудно оценить количественно. Однако его техническая сложность в сочетании с растущей популярностью методов BYOVD среди участников угроз свидетельствует о растущей угрозе.

Кибератака с использованием Terminator может иметь серьёзные последствия для организации. С точки зрения операционной деятельности, финансовые последствия могут включать значительные расходы на реагирование на инциденты, восстановление системы, судебные издержки и возможные штрафы за нарушение нормативных требований. Более того, репутационный ущерб от успешного взлома может привести к потере доверия клиентов, истощению ресурсов и невыгодному положению в конкурентной борьбе, особенно в случае утечки конфиденциальных данных или их фальсификации.

### Эволюция и варианты Terminator

Существуют варианты инструмента Terminator, включая версии с открытым исходным кодом и написанные на разных языках программирования, таких как C# (SharpTerminator) и Nim (Terminator). Эти варианты нацелены на воспроизведение оригинальной технологии или предлагают кроссплатформенную поддержку, что позволяет обойти статические средства обнаружения или эвристические модели.

### Атаки и их последствия

Использование инструмента Terminator и его разновидностей известно, например заметная атака на организацию здравоохранения 15 декабря 2023 года. В ходе этой атаки злоумышленники попытались выполнить команду PowerShell для загрузки текстового файла с сервера C2, который был предназначен для установки XMRig cryptominer в целевой системе.

### Распространённые методы, используемые злоумышленниками для злоупотребления инструментом Terminator:

#### ✦ Использование легитимных, но уязвимых драйверов

Злоумышленники внедряют легитимный драйвер, который является уязвимым, в целевую систему, а затем используют уязвимый драйвер для выполнения вредоносных действий. Это основной принцип атак BYOVD, при которых инструмент Terminator использует уязвимости в таких драйверах, как zam64.sys (Zemana Anti-Logger) или zamguard64.sys (Zemana Anti-Malware), чтобы получить привилегии ядра и выполнить предоставленный злоумышленником код в контексте ядра.

#### ✦ Повышение привилегий на уровне ядра

Успешная эксплуатация позволяет злоумышленникам добиться повышения привилегий на уровне ядра, предоставляя им наивысший уровень доступа и контроля над системными ресурсами. Эти повышенные привилегии используются путём отключения программного обеспечения endpoint security или уклонения от его обнаружения, что позволяет злоумышленникам беспрепятственно выполнять вредоносные действия.

#### ✦ Отключение защитных решений

Как только защита endpoint security взломана, злоумышленники могут отключить антивирус и процессы обнаружения и реагирования на конечные точки (EDR), развернуть дополнительное вредоносное ПО или выполнить другие вредоносные действия без обнаружения. Инструмент нацелен на процессы, связанные с решениями для обеспечения безопасности, и завершает их, эффективно скрывая их от текущих атак.

#### ✦ Использование IOCTL-кодов

Инструмент Terminator и его варианты используют коды IOCTL (управление вводом/выводом) для запроса функциональных возможностей у уязвимого драйвера, таких как попытка завершить целевые процессы. Это включает в себя отправку определённых IOCTL-кодов вместе с параметрами, такими как идентификатор запущенного процесса, чтобы манипулировать поведением драйвера в интересах злоумышленника.

#### ✦ Административные привилегии и обход контроля учётных записей

Чтобы эффективно использовать драйвер, злоумышленнику потребуются административные привилегии и возможность обхода контроля учётных записей пользователей (UAC), или же ему потребуется убедить пользователя принять запрос UAC.

#### ✦ Предотвращение обнаружения

Инструмент пытается эмулировать легитимные заголовки протоколов/файлов, чтобы обойти меры безопасности, хотя это и не увенчалось успехом. Использование легитимных протоколов и служб в качестве серверов управления и контроля (C&C) или каналов связи является ещё одной тактикой для сокрытия своих следов.

#### ✦ Использование общедоступных платформ и протоколов

Злоумышленники также используют общедоступные платформы и протоколы, такие как мессенджеры (IMs) и бесплатные почтовые сервисы, для взаимодействия со взломанными системами и поддержания контроля над своими целями. Этот метод помогает сочетать вредоносный трафик с законной сетевой активностью, что усложняет обнаружение.

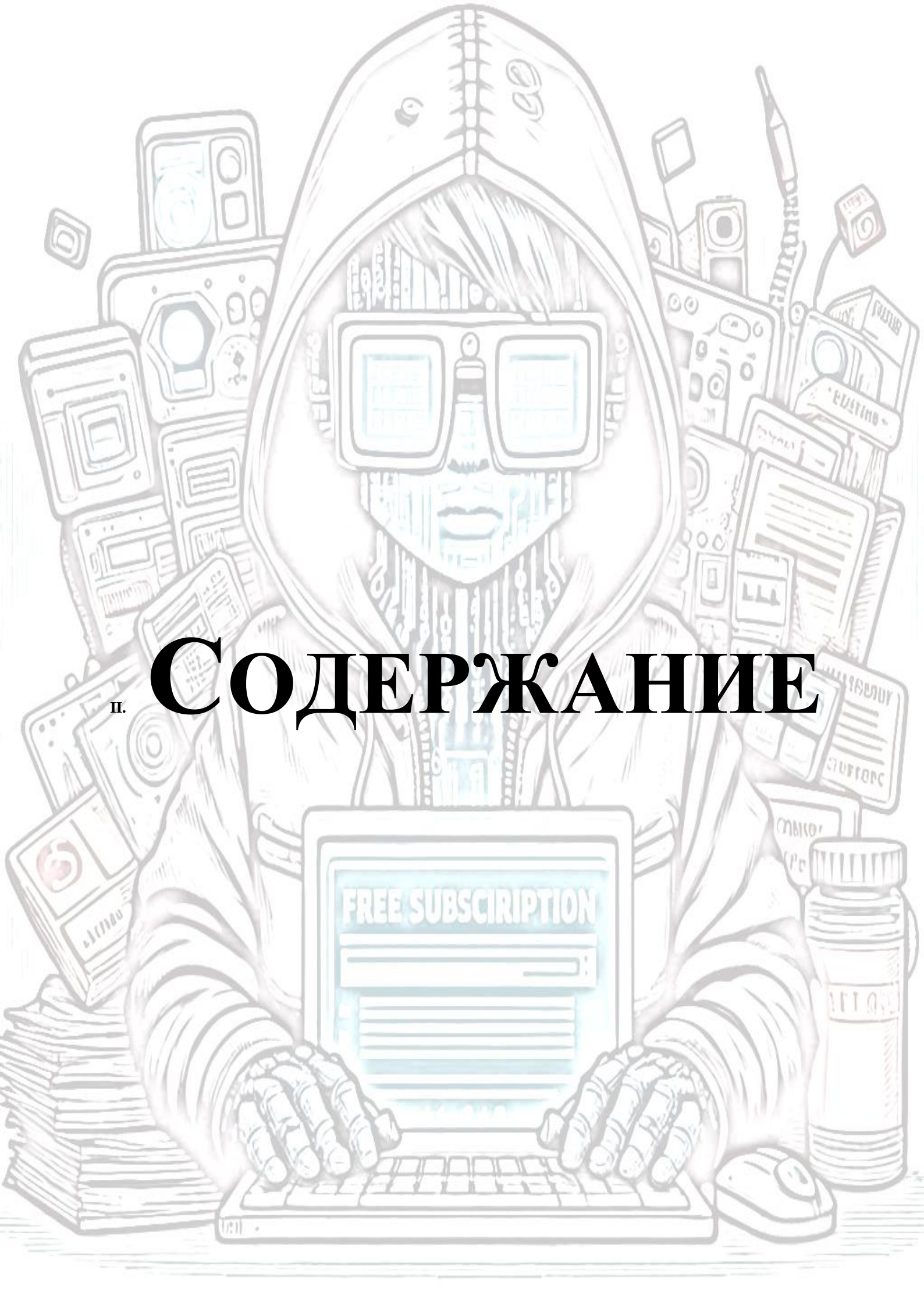


## ViTE - ДИЗАСЕМБЛЕР С ПОДДЕРЖКОЙ RUST

ViTE разработан как кросс-платформенный инструмент анализа исполняемых файлов. Его основная цель - предоставить среду для проверки содержимого двоичных файлов и их отладочной информации. Инструмент предназначен для поддержки различных архитектур, что делает его универсальным для различных исполняемых форматов.

- ◆ **Просмотр списка сборок:** позволяет пользователям просматривать результат разбора двоичного файла вместе с соответствующим исходным кодом.
- ◆ **Интерактивные элементы:** включает заголовок с кнопками и параметрами, просмотр спискаборок и интерактивный терминал.
- ◆ **Исправление байтовых инструкций:** позволяет пользователям напрямую изменять двоичный файл.
- ◆ **Программа просмотра двоичных файлов в hex-формате:** предоставляет шестнадцатеричное представление двоичных файлов для детальной проверки.
- ◆ **Интерфейсы для отладки:** поддерживает front-end интерфейсы для отладки.
- ◆ **Поддерживаемые архитектуры:** Включает поддержку нескольких архитектур, таких как X86-64, AArch64/Armv7, Riscv64gc/Riscv32gc и MIPS-V.
- ◆ **Поддержка целевых систем:** Обеспечивает разборку для различных целевых систем, включая MSVC, Itanium и Rust.
- ◆ **Декодирование структур данных:** Позволяет декодировать структуры данных на основе каждого раздела двоичного файла.
- ◆ **Обновление спискаборок:** Преобразует спискиборок в представление более высокого уровня.
- ◆ **Определение адресов:** помогает в определении адресов в двоичном коде.
- ◆ **Интерпретация данных, не связанных с кодом:** Позволяет интерпретировать данные в двоичном коде, которые не являются исполняемым кодом.
- ◆ **Создание меток для относительных переходов:** Облегчает создание меток для инструкций по относительному переходу в процессе разборки.





II. **СОДЕРЖАНИЕ**

## CVE IN FORTRA'S GOANYWHERE MFT



CVE-2024-0204 как ключ под ковриком, для не прошедших проверку подлинности, и желающих создать своего собственного пользователя-администратора. Эта уязвимость может быть использована удалённо и является классическим примером CVE-425: "Принудительный доступ, когда веб-приложение просто слишком вежливое, чтобы обеспечить надлежащую авторизацию". Уязвимые версии 6.x начиная с 6.0.1 и версии 7.x до 7.4.1, которая была исправлена, а для уязвимых версий необходимо удалить файл /InitialAccountSetup.xhtml или заменить на пустой с перезапуском службы/

### Последствия подобны альбому величайших хитов о кошмарах безопасности:

❖ Создание неавторизованных пользователей-администраторов (акция «избавляемся от складских запасов аутентификационных ключей»)

- ❖ Потенциальная утечка данных (для повышения популярности компании)
- ❖ Внедрение вредоносных программ (вместо традиционных схем распространения)
- ❖ Риск вымогательства (минутка шантажа)
- ❖ Сбои в работе (разнообразие от повелителя хаоса)
- ❖ COMPLIANCE и юридические вопросы (ничто так не оживляет зал заседаний, как старый добрый скандал с COMPLIANCE и потенциальная юридическая драма)

Планка "сложности атаки" установлена так низко, что даже малыш может споткнуться об неё. Отмечается простота, которая заставляет задуматься, не является ли "безопасность" просто модным словом, которым они пользуются, чтобы казаться важными.



## STAR BLIZZARD

Star Blizzard не следует путать с небесным погодным явлением или угрозой ограниченного выпуска из кофейни Dairy Queen. Группа занимается своей деятельностью с ноября 2023 года, оставаясь незамеченной до 12 января 2024 года, ведь вы в это безмятежно смотрели свой любимый сериал в админской.

Представьте, если хотите, финансовую индустрию с её высоким самомнением, получающую (в лицо цифровой пирог) "Ещё один "срочный" запрос на банковский перевод от генерального директора, который в данный момент находится на сафари? Конечно, давайте ускорим это!"

В мире кибербезопасности, где ставки высоки, а все всегда ищут следующее слабое звено, удивительно, что любая отрасль может сохранять невозмутимое выражение лица. Итак, давайте нервно посмеёмся, а затем, возможно, только, возможно, обновим эти пароли и ИТ-политику.



## DARKPINKAPT

Действие очередной кибер-саги разворачивается в мистических землях Азиатско-Тихоокеанского региона, где главные герои (или антагонисты, в зависимости от вашего взгляда на конфиденциальность данных и необходимость доступа к ним) начали свою цифровую деятельность ещё в середине 2021 года и качественно усилили её в 2022 году.

Вооружённый арсеналом инструментов и специально разработанного вредоносного программного обеспечения, предназначенного для кражи данных и шпионажа, Dark Pink был воплощением настойчивости. Их любимое оружие? Фишинговые электронные письма, содержащие сокращённый URL-адрес, который приводил жертв на бесплатный файлообменный сайт, где их ждал ISO-образ, конечно же вредоносный.

Давайте углубимся в цели кибер-художников. Корпоративный шпионаж, кража документов, аудиозапись и утечка данных с платформ обмена сообщениями – все это было делом одного дня для Dark Pink. Их географическая направленность, возможно, начиналась в Азиатско-Тихоокеанском регионе, но их амбиции не знали границ, нацелившись на европейское правительственное министерство в смелом шаге по расширению своего портфолио. Их профиль жертв был таким же разнообразным, как совещание ООН, нацеливаясь на военные организации, правительственные учреждения и даже религиозную организацию. Потому что дискриминация это не модная повестка.

В мире киберпреступности они служат напоминанием о том, что иногда самые серьёзные угрозы приходят в самых непритязательных упаковках с розовым бантиком.



## KILLNET: КИБЕР-ЗВЕЗДА ДРАМКРУЖКА "DDoS"

Кибер-группа, поднялась на вершину таблицы лидеров кибер-активностей, затмив более сотни других групп в прокси-кибервойнах. Их любимое оружие? Очень сложная распределённая атака типа "Отказ в обслуживании" (DDoS), которая бьёт по большому месту: жизненно важной инфраструктуре, правительственным службам, веб-сайтам аэропортов и, почему бы и нет, медиакомпаниям в странах НАТО. У группы есть склонность к драматизму, когда у Европейского парламента хватило наглости начать расследование против них, KillNet пошла ва-банк, нацелившись на бельгийский центр кибербезопасности, потому что, надо больше кибер-истерик. Европа – их любимая игровая площадка, где зарегистрировано более 180 атак, в то время как Северная Америка находится в углу с менее чем 10. Однако они не привередливы: финансовая индустрия, транспорт, правительственные учреждения и бизнес-услуги.



## ФИШИНГ В ВЕЛИКОБРИТАНИИ

Инструментарий атакующих претерпел изменения. Они больше не рассылают письма "Я принц с наследством" и переключились на высокие технологии: мир QR-фишинга (или "квишинга", потому что, по-видимому, с "q" все лучше) и даже подключив ИИ для написания убедительных мошеннических электронных писем. QR-коды — это золотой билет для мошенников в социальных сетях, которые наживаются на ничего не подозревающих массах, пребывающих в поисках билетов на концерт или на следующую крупную распродажу. Между тем, ИИ делает подделку чьей-либо личности проще, чем когда-либо, потому что кому больше нужны настоящие отпечатки пальцев или лица? Если это выглядит как мошенничество и пахнет аферой, то, скорее всего, это просто ещё один день в Интернете. Держите себя в руках и, по возможности, не переходите по этой ссылке от "Секретной службы Ее Величества", обещающей вам возврат налогов в фунткоинах.

## DCRAT (DARK CRYSTAL RAT)



DCRat, швейцарский армейский нож киберпреступного мира, истинное свидетельство предпринимательского духа, процветающего в темных уголках Интернета. С момента своего грандиозного дебюта в 2018 году DCRat стал незаменимым гаджетом для каждого начинающего злодея со склонностью к цифровым проказам. По очень низкой цене в 7 долларов можно приобрести двухмесячную подписку на это чудо современного вредоносного ПО, а для тех, кто действительно предан делу, доступна пожизненная лицензия за внушительную сумму в 40 долларов. DCRat служит напоминанием, что в эпоху цифровых технологий безопасность настолько сильна, насколько сильна способность не переходить по подозрительным ссылкам.

## СИСТЕМА ОЦЕНКИ УЯЗВИМОСТЕЙ CVSS 4.0

Мир кибербезопасности пополнился последней и самой совершенной версией общей системы оценки уязвимостей CVSS версии 4.0. Эта версия обещает произвести революцию в том, как мы оцениваем критичность и влияние уязвимостей ПО, ведь версия 3.1 была всего лишь разминкой.

❖ **Более детализированные базовые показатели.** если есть что-то, что любят профессионалы в области ИБ, так это детализация. Теперь мы не только можем оценить воздействие на уязвимую систему, но и потратить тысячу листов на детализацию, это уже серьёзный уровень профессионализма

❖ **Группа угроз** – критичность уязвимости может быть скорректирована в зависимости от того, мог ли кто-то где-то подумать о их использовании, и теперь паранойя всегда подкрепляется последними данными об угрозах.

❖ **Метрики окружения позволяют адаптировать оценку к нашей конкретной вычислительной среде.** ничто так не говорит о "индивидуальности", как корректировка оценок на основе множества мер по смягчению последствий.

❖ **Показатели угроз были упрощены до уровня зрелости эксплойтов.** если и есть что-то, что легко определить, так это то, насколько зрелым является эксплойт.

❖ **Система подсчёта оценки стала проще и гибче и ... больше.** если и есть какое-то слово, которое ассоциируется с CVSS, так это простота, ведь теперь поддерживается несколько оценок для одной и той же уязвимости

Итак, CVSS версии 4.0 призван спасти положение благодаря своей повышенной ясности, простоте и повышенному вниманию ко всем мелочам и деталям. Потому что, как мы все знаем, единственное, что доставляет больше удовольствия, чем оценка уязвимостей, — это делать это с помощью новой, более сложной системы.



## RANSOMWARE Q3

С 4368 жертвами, пойманными в их цифровые сети, киберпреступникам удалось превзойти самих себя по эффективности на 55,5% по сравнению с предыдущим годом, вот что значит KPI.

Средняя сумма выкупа для предприятия выросла до более чем 100 000 долларов, при этом требования в среднем составляли крутые 5,3 миллиона долларов. 80% организаций придерживаются политики "Не платить", и все же в прошлом году 41% в итоге заплатили выкуп.

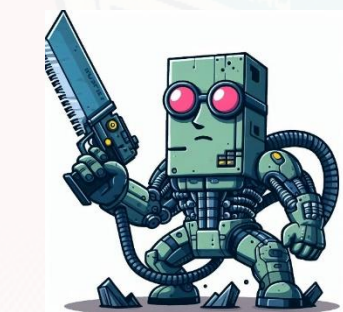
И для тех, кто думает, что страховка может спасти положение, подумайте ещё раз. 77% организаций на собственном горьком опыте убедились, что программы-вымогатели – это далеко не то, за что страховая с лёгкостью заплатит, не проверив, а всё ли вы сделали для защиты.



## RANSOMWARE Q4

LockBit 3.0 завоевал золото на хакерской олимпиаде, за ним последовали отважные новички Clor и ALPHV/BlackCat. По-видимому, 48% организаций почувствовали себя обделёнными вниманием и решили принять участие в кибератаках. Бизнес-сервисы получили награду в номинации "наиболее подверженные цифровому взлому", а образование и розничная торговля последовали за ними.

Хакеры расширили свой репертуар, перейдя от скучного старого шифрования к гораздо более захватывающему миру вымогательства. Не бедные страны США, Великобритания и Канада заняли первое место в категории "страны, которые, скорее всего, заплатят". Биткойны были предпочтительной валютой, хотя некоторые стали поглядывать в сторону Monero. Некоторые организации пытались экономить на выкупе, заплатив только 37%. Тем, кто все-таки раскошелился, пришлось в среднем отдать \$408 643. Кибер-преступность действительно окупается!



## CHISEL SANDSTORM

Ах, этот цифровой век, когда даже у наших вредоносных программ появляется больше возможностей для путешествий и приключений, чем у среднестатистического офисного работника.

Созданная цифровыми мастерами, известными как Sandworm, программа The Chisel — это не просто вредоносная программа; это шедевр в области проникновения. Эта коллекция цифровых инструментов не просто проникает на устройства Android; она настраивает работу, позволяет расслабиться за бокалом мартини и приступить к работе по извлечению всевозможной полезной информации. Информация о системных устройствах, данные о коммерческих приложениях и, о, давайте не будем забывать о важных военных приложениях. Потому что зачем гоняться за скучными повседневными данными, когда можно погрузиться в военные секреты?

Программа Chisel не просто собирает данные, она их систематизирует. Подобно ценителю изысканных вин, она отбирает только самую изысканную информацию для отправки ее создателям. Информация об устройстве системы? Да. Данные о коммерческом применении? Конечно. Военные секреты, которые потенциально могут изменить ход международных отношений? Дайте-два. Это не просто кража, это форма искусства.

В мире, где цифровые угрозы актуальны как никогда Chisel напоминает нам о том, что некоторые вредоносные программы нацелены на доминирование, в особых изощрённых формах. Ура, авторы Chisel, вы действительно подняли планку для всех в мире.



## CYBER TOUFAN AL-AQSA

В мире кибервойн, где ставки столь же высоки, как и самомнение, хакерская группа "Toufan Al-Aqsa" ворвалась на сцену в 2023 году и носилась от одной израильской компании к другой, оставляя за собой шлейф цифрового хаоса. И кто же стоит за этим маскарадом озорства? Что ж, решение присяжных ещё не принято, но все указывают на Иран, потому что если вы собираетесь обвинить кого-то в кибермошенничестве, то это с таким же успехом может быть ваш геополитический враг, верно?

В этом документе представлен анализ хакерской группы Cyber Toufan Al-Aqsa, которая быстро приобрела известность благодаря кибератакам, нацеленным в первую очередь на израильские организации. В анализе рассматриваются различные аспекты деятельности группы, включая её предысторию и возникновение, методы работы, заметные атаки и нарушения, предполагаемое государственное спонсорство и последствия её деятельности для специалистов по кибербезопасности и других специалистов в различных отраслях. Он также направлен на то, чтобы подчеркнуть его значительное влияние на практику кибербезопасности и более широкий геополитический ландшафт.

## MALLOX



Mallox — это цифровой Робин Гуд нашего времени, за исключением того, что они крадут у всех и отдают себе. С середины 2021 года они играли с незащищёнными серверами Microsoft SQL, шифровали данные, а затем любезно предлагали вернуть их за скромное пожертвование в биткоинах. А ещё приобрели новые вредоносные игрушки, добавив в свою коллекцию Remcos RAT, BatCloak и немного Metasploit. Сейчас играют в игру "Поймай обфускацию, если сможешь" с антивирусным ПО.

В этом документе представлен анализ, который посвящён различным аспектам деятельности группы, включая её отличительную практику добавления названий целевых организаций к зашифрованным файлам, эволюцию её алгоритмов шифрования и тактику обеспечения постоянства

и обхода средств защиты.

## ALPHV



Какую драматическую кибер-мыльную оперу мы наблюдали с группой вымогателей Alpha. Это похоже на цифровую игру "ударь крота", когда ФБР и его друзья размахивают молотом правосудия, а мошенники-вымогатели выскакивают с дерзким баннером "unseized". Первоначальный успех ФБР был прерван, когда вновь появился сайт AlphV, на котором теперь таинственным образом отсутствовали какие-либо компрометирующие списки жертв. Сможет ли ФБР наконец поймать Черную кошку за хвост в киберпространстве, или эти цифровые головололки снова ускользнут от нас? Оставайтесь с нами до следующего эпизода "Федералы и Преступники: Кибер-хроники."

# iii. CVE IN FORTRA'S GO ANYWHERE MFT





#### A. Введение

CVE-2024-0204 представляет собой уязвимость для обхода аутентификации в продукте Fortra's GoAnywhere. MFT Эта уязвимость позволяет злоумышленнику, не прошедшему проверку подлинности, создать пользователя с правами администратора для приложения с возможностью удалённой эксплуатации (CWE-425).

Уязвимость затрагивает Fortra GoAnywhere MFT версий 6.x начиная с 6.0.1 и версий 7.x до 7.4.1 и также существует PoC код эксплоита **Error! Reference source not found..** Исправление в версии 7.4.1 было выпущено 7 декабря 2023 года. Что касается ландшафта угроз, то в 2023 году приложения для передачи файлов были главной мишенью злоумышленников, что подчёркивает важность обеспечения безопасности таких приложений.

Из опубликованной рекомендации компании следует, что уязвимость можно устранить, удалив /InitialAccountSetup.xhtml и перезапустив службу. Для экземпляров, развёрнутых в контейнере, файл может быть заменён пустым файлом с последующим перезапуском службы.

#### B. GoAnywhere Managed File Transfer (MFT)

GoAnywhere MFT – это программное решение, которое упрощает для централизации, упрощения и автоматизации перемещения данных, обмена данными между системами, сотрудниками, клиентами и торговыми партнёрами.

GoAnywhere MFT может быть развернут в различных средах, локально, в облаке на таких платформах, как Microsoft Azure и AWS, или в гибридных средах.

GoAnywhere MFT поддерживает широкий спектр протоколов для безопасной передачи файлов, включая SFTP (FTP по SSH), FTPS (FTP по SSL/TLS), SCP (безопасное копирование по SSH), HTTP/s, AS2, AS3, AS4

и другие. Он также предоставляет более 60 различных задач, которые могут быть объединены в рабочие процессы без необходимости программирования или написания сценариев.

В дополнение к своим основным возможностям передачи файлов GoAnywhere MFT также включает функции защиты паролем, двухфакторной аутентификации и интеграции с различными другими системами и приложениями.

#### C. Отраслевое применение решения

GoAnywhere MFT широко используется в различных секторах благодаря функциональности безопасного автоматизировать обмен данными:

- Информационные технологии и услуги
- Программное обеспечение для компьютеров
- Финансовые услуги
- Медицинские услуги и Здоровоохранение
- Обрабатывающая промышленность
- Консалтинг.

В сфере информационных технологий и услуг GoAnywhere MFT используется для интеграции с веб- и облачными приложениями, обеспечивая безопасность данных и автоматизированную передачу файлов с использованием централизованного подхода корпоративного уровня. Его также можно использовать для стандартизации процессов передачи файлов, уменьшая необходимость привлечения групп разработчиков для разработки отдельных решений:

- **Интеграция с веб-и облачными приложениями:** это помогает безопасно интегрировать передачу файлов с веб-и облачными приложениями.
- **Централизация процессов передачи файлов:** GoAnywhere MFT предоставляет централизованную платформу для управления всеми операциями передачи файлов, уменьшая необходимость участия команд разработчиков
- **Автоматизация передачи файлов:** автоматизирует повторяющиеся и сложные задачи по передаче файлов, экономя время и уменьшая количество ошибок.
- **Повышение безопасности:** решение предлагает функции безопасности корпоративного уровня, помогая компаниям, оказывающим ИТ-услуги, защищать конфиденциальные данные во время передачи.

В сфере компьютерного программного обеспечения GoAnywhere MFT может использоваться для автоматизации и обеспечения безопасности передачи файлов, уменьшая потребность «ручного применения» в пользовательских сценариях. Его также можно использовать для создания, редактирования и мониторинга

заданий на передачу файлов, а также для выполнения различных рабочих процессов и переводов данных.

- **Автоматизация распространения программного обеспечения:** Безопасная автоматизация распространения обновлений программного обеспечения и исправлений среди клиентов.
- **Совместная работа:** обеспечение безопасной совместной работы между разработчиками, особенно при работе с исходным кодом и другими конфиденциальными данными.
- **Соответствие нормативным требованиям:** Оказание помощи компаниям-разработчикам ПО в соблюдении требований к разработке программного обеспечения и обработке данных.

В сфере финансовых услуг GoAnywhere MFT используется для защиты конфиденциальных данных клиентов и выполнения требований соответствия. Это помогает контролировать обмен конфиденциальными данными о держателях карт и отслеживать перемещения файлов для упрощения аудита. Например, Sentinel Benefits & Financial Group использует GoAnywhere MFT для создания и редактирования заданий на передачу файлов, мониторинга безопасности, выполнения различных рабочих процессов.

- **Безопасные транзакции:** Автоматизация и защита финансовых транзакций, обеспечение защиты конфиденциальных данных.
- **Соответствие требованиям:** Соблюдение требований, таких как PCI DSS, для защиты данных о держателях карт.
- **Эффективная обработка данных:** оптимизация процесса создания, редактирования и мониторинга заданий на передачу файлов, на примере Sentinel Benefits & Financial Group.

В отрасли здравоохранения GoAnywhere MFT может использоваться для безопасной передачи данных пациентов и другой конфиденциальной информации, помогая организациям здравоохранения соответствовать таким требованиям как HIPAA. Его также можно использовать для автоматизации передачи файлов, уменьшая потребность в ручных процессах с целью повышения эффективности.

- **Соблюдение требований медицинского сектора:** обеспечение соответствия передачи данных медицинским требованиям, таким как HIPAA.
- **Защита данных пациента:** безопасная передача медицинской информации пациента (PHI) при соблюдении правил HIPAA.
- **Безопасный обмен данными о пациентах:** безопасный обмен данными о пациентах между поставщиками медицинских услуг, страховщиками и другими заинтересованными сторонами.

- **Функциональная совместимость:** облегчение обмена медицинскими данными между различными системами и организациями.
- **Автоматизация передачи медицинских данных:** Автоматизация передачи электронных медицинских записей (EHRs), результатов лабораторных исследований и других важных медицинских данных.
- **Автоматизация рабочих процессов в сфере здравоохранения:** автоматизация передачи результатов лабораторных исследований, платёжной информации и других данных, связанных со здравоохранением.

В обрабатывающей промышленности GoAnywhere MFT может использоваться для автоматизации и обеспечения безопасности передачи файлов дизайна, производственных данных и другой конфиденциальной информации. Его также можно использовать для интеграции с другими системами и приложениями, повышая эффективность и уменьшая потребность в ручных процессах.

- **Безопасная передача файлов:** защита передачи конфиденциальных производственных файлов.
- **Интегрированные цепочки поставок:** Интегрированные цепочки поставок для эффективного обмена данными при взаимодействии с партнёрами.
- **Автоматизация производственных процессов:** автоматизация передачи производственных данных, таких как уровень запасов, данные о заказе и отслеживание отгрузки.

В консалтинговой сфере GoAnywhere MFT может использоваться для безопасной передачи конфиденциальных клиентских данных и другой информации. Его также можно использовать для автоматизации передачи файлов, уменьшая потребность в ручных процессах и повышая эффективность.

- **Безопасность клиентских данных:** обеспечение безопасной передачи конфиденциальных клиентских данных во время проведения консультационных мероприятий.
- **Проектное сотрудничество:** Обеспечение безопасной совместной работы над проектами, которые предполагают обмен данными между консультантами и клиентами.
- **Эффективность и автоматизация:** Автоматизация обмена данными и отчётами с клиентами, повышение эффективности и сокращение ручного труда.

#### D. Первопричина CVE

Основная причина CVE-2024-0204 идентифицирована как CWE-425: Forced Browsing. Эта уязвимость возникает, когда веб-приложение некорректно обеспечивает авторизацию скриптов или файлов, позволяя обходить



механизмы аутентификации и получать несанкционированный доступ.

Эксплойт эксплуатирует проблему «path traversal», которая представляет собой тип уязвимости в системе безопасности, позволяющей получить доступ к файлам и каталогам, хранящимся за пределами корневой web-папки. В частности, уязвимость GoAnywhere Fortra позволяет не прошедшему проверку подлинности манипулировать переменными, которые ссылаются на файлы для доступа к произвольным файлам и каталогам, хранящимся в файловой системе». В случае CVE-2024-0204 это позволяет получить доступ к уязвимому файлу /InitialAccountSetup.xhtml и создать пользователя с правами администратора (на чтение и запись и выполнение команд).

Это позволяет эффективно обойти существующие требования к аутентификации и авторизации, поскольку злоумышленнику не нужно предоставлять какие-либо действительные учётные данные для получения административного доступа к системе. Эта уязвимость представляет высокий риск для клиентов, у которых есть доступный через Интернет портал администратора.

#### Е. Воздействие CVE и затронутые системы

Влияние CVE-2024-0204 на пользователей MFT GoAnywhere значительно из-за критического характера уязвимости:

- **Создание неавторизованных пользователей-администраторов:** уязвимость позволяет злоумышленнику, не прошедшему проверку подлинности, создать пользователя-администратора, что может привести к несанкционированному доступу к системе
- **Возможность утечки данных:** Имея административный доступ, злоумышленники могут получить доступ к конфиденциальным данным, что может привести к утечке данных
- **Развёртывание вредоносного ПО:** Злоумышленники с правами администратора могут внедрять вредоносное ПО, в том числе программы-вымогатели, которые могут нарушить работу и привести к финансовым потерям
- **Полный захват системы:** Создание пользователей уровня администратора может позволить злоумышленникам получить полный контроль над уязвимой системой
- **Риск вымогательства:** Учитывая простоту использования, существует риск вымогательства, поскольку злоумышленники потенциально угрожают опубликовать конфиденциальные данные, если они не получают платёж
- **Нарушение работы:** Несанкционированный доступ и потенциальные последующие атаки могут нарушить нормальную работу затронутых организаций

- **Соблюдение требований и юридические проблемы:** Организации, пострадавшие от нарушения, вызванного этой уязвимостью, могут столкнуться с проблемами соблюдения требований и юридическими последствиями

GoAnywhere MFT имеет оценку CVSS 9,8; разница между оценкой CVSS, равной 9,8 и 10,0 в первую очередь заключается в метрике "Score" в системе оценки CVSS. Оценка CVSS, равная 10,0 указывает на то, что уязвимость имеет наиболее серьёзные показатели воздействия и возможности использования, и её воздействие выходит за рамки самого уязвимого компонента, затрагивая также другие компоненты. Оценка CVSS, равная 9,8, также представляет уязвимость с наиболее серьёзными показателями эксплуатируемости и воздействия, но её влияние не распространяется за пределы уязвимого компонента.

Проще говоря, оценка CVSS, равная 10,0, предполагает уязвимость, которая может нанести более масштабный ущерб всей системе, потенциально ставя под угрозу дополнительные системы за пределами начальной точки эксплуатации. Оценка 9,8, хотя и остаётся критической, указывает на уязвимость, которая ограничивается затронутым компонентом и не способна влиять на другие части системы.

#### Ф. Схема атаки и сценарий

Уровень сложности атаки CVE-2024-0204 низкий. Это означает, что условия, необходимые для использования уязвимости, нетрудно достичь, и атака может проводиться без каких-либо особых условий. Низкий уровень сложности в сочетании с критической серьёзностью уязвимости делает её серьёзной проблемой безопасности.

##### 1) Схема атаки

Схема атаки для CVE-2024-0204, уязвимости обхода аутентификации в MFT GoAnywhereFortra, выглядит следующим образом:

- **Первоначальный доступ:** Злоумышленник, не прошедший проверку подлинности, получает доступ к portalу администрирования MFT GoAnywhere. Это возможно из-за проблемы с обходом пути, которую представляет эта уязвимость
- **Эксплуатация:** злоумышленник использует проблему с обходом пути, чтобы получить доступ к /InitialAccountSetup.xhtml
- **Создание пользователя-администратора:** как только злоумышленник получит доступ к InitialAccountSetup.xhtml, он может создать пользователя-администратора со всеми соответствующими права администратора на чтение и запись, а также возможности выполнения команд
- **Возможное дальнейшее использование:** Имея административный доступ, злоумышленник потенциально может получить доступ к конфиденциальным данным, внедрить вредоносное ПО или получить полный контроль над системой

## 2) Сценарий атаки

Возможные сценарии атак для CVE-2024-0204 могут включать:

- **Атаки программ-вымогателей:** Учитывая историю использования продуктов для передачи файлов в качестве шлюзов для атак программ-вымогателей, есть опасения, что CVE-2024-0204 может быть использован аналогичным образом. Злоумышленники могли использовать доступ администратора, полученный благодаря этой уязвимости, для развёртывания программ-вымогателей, шифрующих файлы и требующих выкуп за их расшифровку
- **Эксплуатация данных:** злоумышленники могут использовать доступ администратора для получения конфиденциальных данных. Это могут быть личные данные, финансовая информация или служебные бизнес-данные.
- **Захват системы:** имея доступ администратора, злоумышленники потенциально могут получить полный контроль над системой. Это может быть использовано для нарушения работы, развёртывания дополнительного вредоносного ПО или использования системы в качестве стартовой площадки для дальнейших атак
- **Вымогательство:** Злоумышленники могут угрожать опубликовать конфиденциальные данные, если они не получают оплату. Это может нанести особый ущерб организациям, которые обрабатывают конфиденциальные данные клиентов или несвободную информацию
- **Саботаж:** В более деструктивном сценарии злоумышленники могут использовать доступ администратора для удаления или изменения данных, нарушения операций или иного саботажа организации. Это может привести к значительным последствиям для бизнеса, включая простои и финансовые потери

## G. Последствия

Потенциальные последствия атаки с использованием CVE-2024-0204 на пользователей MFT GoAnywhere:

- **Несанкционированный административный доступ:** злоумышленники могут создать пользователя-администратора через портал администрирования без надлежащей авторизации, что приводит к несанкционированному доступу к системе
- **Утечка данных:** Имея доступ администратора, злоумышленники потенциально могут получить доступ к конфиденциальным данным, отфильтровать их или манипулировать ими, что приведёт к утечке данных
- **Компрометация системы:** Злоумышленники могут использовать доступ администратора для

дальнейшей компрометации системы, потенциально влияя на целостность, доступность и конфиденциальность системы и данных

- **Нарушение работы:** Несанкционированный доступ может быть использован для нарушения работы, что может иметь значительные последствия для бизнеса, включая простои и финансовые потери
- **Вымогательство и программы-вымогатели:** существует риск вымогательства, когда злоумышленники угрожают опубликовать конфиденциальные данные, если они не получат оплату. Уязвимость также может быть использована в качестве шлюза для атак программ-вымогателей, как это было с предыдущими уязвимостями в продуктах для передачи файлов
- **Ущерб репутации:** Успешная атака может нанести ущерб репутации пострадавшей организации, что приведёт к потере доверия клиентов и потенциальным юридическим последствиям
- **Нарушения требований законодательства:** Организации могут грозить штрафы и санкции регулирующих органов, если нарушение приведёт к несоблюдению законов о защите данных и отраслевых нормативных актов

## H. CVE PoC

По GitHub-ссылке <https://github.com/horizon3ai/CVE-2024-0204> размещён PoC-эксплоит. Этот скрипт, разработанный Horizon3.ai, демонстрирует, как можно использовать уязвимость обхода аутентификации в GoAnywhere MFT.

Скрипт работает путём отправки POST-запроса в /InitialAccountSetup.xhtml приложения MFT GoAnywhere. Запрос включает параметры для создания нового пользователя с правами администратора, эффективно минуя механизм аутентификации.

### 1) Параметры скриптов

Параметры включают информацию, необходимую для создания новой учётной записи пользователя:

- **Имя пользователя:** желаемое имя пользователя для новой учётной записи администратора.
- **Пароль:** пароль для новой учётной записи, который должен соответствовать требованиям по сложности GoAnywhere MFT.
- **Адрес электронной почты:** адрес электронной почты, связанный с новой учётной записью администратора.
- **Полное имя:** полное имя физического лица, связанного с новой учётной записью.
- **Разрешения:** Уровень доступа или роли, назначенные новому пользователю, в данном случае права администратора.

Эти параметры отправляются в теле HTTP POST-запроса как часть полезной нагрузки запроса. Сервер обрабатывает эти параметры и создаёт новую учётную запись пользователя с указанными реквизитами.

После запуска скрипта ожидаемым ответом будет указание на то, что сценарий успешно создал нового пользователя с правами администратора в приложении MFT GoAnywhere. Конкретные детали ответа будут зависеть от поведения приложения при создании пользователем:

- **Успешный ответ HTTP:** код состояния, указывающий на успешное выполнение (например, HTTP 200 OK) с веб-сервера, означающий, что запрос POST был успешно обработан.
- **Сообщение с подтверждением:** сообщение или JSON-ответ от приложения, подтверждающий создание нового пользователя с правами администратора.
- **Сообщения об ошибках:** сообщения об ошибках, которые указывали бы на то, что запрос был выполнен неудачно.
- **Административный доступ:** возможность входа в систему с недавно созданными учётными данными администратора, подтверждающими, что пользователь был создан с ожидаемыми разрешениями.

#### 1. Другие уязвимости связанные с CVE

Другие уязвимости, обнаруженные в GoAnywhere MFT, включают:

- CVE-2021-46830
- CVE-2023-0669

CVE-2021-46830 – это проблема «path traversal», которая потенциально может позволить внешнему пользователю, который самостоятельно регистрируется, получить доступ к непреднамеренным областям памяти приложения. Это влияет на версии GoAnywhere MFT, предшествующие версии 6.8.3.

CVE-2023-0669 – это внедрение команды предварительной аутентификации, которая может быть использована произвольным пользователем. Уязвимость связана с десериализацией ненадёжных данных без надлежащей проверки, что влияет на конфиденциальность и целостность.

##### 1) Схема и сценарий атак [CVE-2021-46830]

Исходя из характера уязвимости CVE-2021-46830 процесс атаки для такой уязвимости включает следующие шаги:

- **Обнаружение:** злоумышленник обнаруживает, что веб-приложение уязвимо для обхода пути из-за неадекватной проверки входных данных.
- **Эксплуатация:** злоумышленник создаёт запрос, который включает последовательности обхода

каталогов (например, ../) для перехода из корневого веб-каталога в каталоги, которые должны быть недоступны.

- **Доступ:** созданный запрос позволяет злоумышленнику получить доступ или выполнить файлы, находящиеся за пределами предполагаемых каталогов, доступных через Интернет.
- **Воздействие:** В зависимости от файлов или каталогов, к которым осуществляется доступ, злоумышленник потенциально может прочитать конфиденциальную информацию, выполнить несанкционированные команды или использовать доступ для дальнейшей компрометации системы.

В частности, для CVE-2021-46830 уязвимость позволяла внешнему пользователю, который самостоятельно регистрируется, получать доступ к непреднамеренным областям приложения MFT GoAnywhere, что потенциально могло привести к несанкционированному раскрытию информации или дальнейшим атакам.

Сценарий потенциальной атаки может выглядеть следующим образом:

- **Первоначальный доступ:** злоумышленник идентифицирует приложение MFT GoAnywhere, доступное по сети и позволяющее саморегистрацию пользователей.
- **Использование:** злоумышленник самостоятельно регистрируется, а затем изменяет пути к файлам в приложении для доступа к каталогам и файлам за пределами предполагаемой области действия.
- **Раскрытие информации:** злоумышленник читает файлы, к которым у него не должно быть доступа, потенциально получая доступ к конфиденциальной информации.
- **Дальнейшие атаки:** В зависимости от характера данных, к которым осуществляется доступ, и функциональности приложения злоумышленник потенциально может использовать полученную информацию для проведения дальнейших атак.

##### 2) Схема и сценарий атаки [CVE-2023-0669]

Исходя из характера уязвимости CVE-2021-46830 процесс атаки для такой уязвимости включает следующие шаги:

- **Разведка:** злоумышленник идентифицирует уязвимую целевую систему, которая доступна и имеет конкретную уязвимость, в данном случае CVE-2023-0669.
- **Подготовка атаки:** злоумышленник создаёт вредоносный ввод или полезную нагрузку, предназначенные для использования уязвимости.
- **Доставка:** злоумышленник отправляет обработанную полезную нагрузку в целевую систему. Это может быть связано с сетевыми

запросами, вредоносными файлами или другими способами, в зависимости от характера уязвимости.

- **Эксплуатация:** Полезная нагрузка запускает уязвимость, позволяя злоумышленнику выполнять произвольный код или команды, обходить механизмы безопасности или иным образом компрометировать систему.
- **Пост-эксплуатация:** после успешного использования злоумышленник может выполнять такие действия, как установление постоянного доступа, повышение привилегий, кража данных или распространение на другие системы.

Сценарий потенциальной атаки для уязвимости типа CVE-2023-0669, требующей взаимодействия человека, может включать:

- **Социальная инженерия:** злоумышленник может использовать методы социальной инженерии, чтобы обманом заставить пользователя выполнить определённые действия, которые приведут к срабатыванию уязвимости. Это может быть связано с отправкой вредоносного документа или ссылки пользователю.
- **Вредоносный документ:** Злоумышленник может создать документ, который использует уязвимость при открытии пользователем или взаимодействии с ним. Этот документ может быть замаскирован под легитимный файл, чтобы увеличить шансы пользователя открыть его.
- **Удалённое выполнение кода:** если уязвимость допускает удалённое выполнение кода, злоумышленник потенциально может выполнить произвольный код в системе жертвы после обработки вредоносного документа.
- **Повышение привилегий:** злоумышленник может использовать уязвимость для получения более высоких привилегий в системе, что потенциально может привести к полной её компрометации.
- **Кража или манипулирование данными:** имея возможность выполнять код, злоумышленник может украсть конфиденциальные данные, манипулировать ими или установить в систему дополнительное вредоносное ПО.
- **Закрепление:** злоумышленник может закрепиться в уязвимой системе, обеспечивая постоянный доступ и дальнейшую эксплуатацию.

### 3) *Различия в схеме и сценарии атаки*

С точки зрения воздействия, CVE-2024-0204 позволяет злоумышленнику обойти аутентификацию и создать пользователя с правами администратора, в то время как CVE-2021-46830 позволяет злоумышленнику перемещаться по каталогам и получать доступ к файлам или выполнять их вне предполагаемых каталогов, доступных через Интернет.

С точки зрения воздействия, CVE-2024-0204 связан с проблемой обхода пути в веб-приложении, которая позволяет злоумышленнику обойти аутентификацию и создать пользователя с правами администратора, в то время как CVE-2023-0669 связан с уязвимостью, которая может быть вызвана обработкой специально созданного документа.

С точки зрения сценария, CVE-2024-0204 предполагает получение злоумышленником полного административного доступа к системе, в то время как CVE-2021-46830 предполагает получение злоумышленником несанкционированного доступа к определённым областям приложения. Ключевое различие между ними заключается в том, что CVE-2024-0204 допускает прямой административный доступ без необходимости взаимодействия с пользователем, в то время как CVE-2023-0669 требует, чтобы пользователь взаимодействовал с вредоносным документом для запуска уязвимости. CVE-2024-0204 является уязвимостью веб-приложения, тогда как CVE-2023-0669 связан с обработкой документов, вероятно, в контексте рабочего стола или сервера.

#### 4) *Воздействие [CVE-2021-46830]*

Воздействие CVE-2021-46830 выражается в том, что она позволяет внешнему пользователю, который самостоятельно регистрируется, получать доступ к непреднамеренным областям приложения MFT GoAnywhere, что может привести к несанкционированному раскрытию информации или дальнейшим атакам.

Серьёзность воздействия будет зависеть от конкретных данных и функциональных возможностей, открытых в результате непреднамеренного доступа. Например, если области, к которым осуществляется доступ, содержат конфиденциальные данные, злоумышленник потенциально может украсть эти данные, или в случае если позволяют выполнять определённые команды или функции, злоумышленник потенциально может использовать это для дальнейшей компрометации системы.

#### 5) *Воздействие [CVE-2023-0669]*

Воздействие CVE-2023-0669 можно охарактеризовать следующим образом:

- **Несанкционированный доступ:** злоумышленник потенциально может получить несанкционированный доступ к системе или данным, в зависимости от характера уязвимости и конфигурации системы.
- **Кража данных:** если уязвимость позволяет получить доступ к данным, злоумышленник потенциально может украсть конфиденциальную информацию.
- **Компрометация системы:** в некоторых случаях злоумышленник потенциально может использовать уязвимость для выполнения произвольного кода или команд, что может привести к полной компрометации системы.

- **Отказ в обслуживании:** если уязвимость вызывает сбой системы или перестаёт отвечать на запросы, это потенциально может привести к отказу в обслуживании.

6) *Различия в воздействии*

CVE-2024-0204 оказывает более серьёзное воздействие, поскольку позволяет злоумышленнику получить полный административный доступ к системе, в то время как CVE-2021-46830 потенциально может привести к несанкционированному раскрытию информации или дальнейшим атакам.

CVE-2024-0204 оказывает более серьёзное воздействие, поскольку позволяет злоумышленнику получить полный административный доступ к системе, в то время как влияние CVE-2023-0669 будет зависеть от характера уязвимости и конфигурации системы.

7) *Последствия [CVE-2021-46830]*

Потенциальные последствия атаки, использующей эту уязвимость, могут включать:

- **Несанкционированный доступ:** возможность получить несанкционированный доступ к каталогам и файлам за пределами предполагаемой области действия, что может привести к несанкционированному доступу к конфиденциальной информации или системным ресурсам.
- **Раскрытие информации:** злоумышленник может прочитать файлы, к которым у него не должно быть доступа, что приведёт к раскрытию конфиденциальной информации.
- **Компрометация системы:** В зависимости от характера данных, к которым осуществляется доступ, и функциональности приложения злоумышленник потенциально может использовать полученную информацию для проведения дальнейших атак, что может привести к полной компрометации системы.
- **Манипулирование данными:** если злоумышленник получает доступ на запись к определённым файлам или каталогам, он потенциально может манипулировать данными, что может иметь различные последствия в зависимости от характера данных и функциональности системы.

8) *Последствия [CVE-2023-0669]*

Потенциальные последствия CVE-2023-0669 могут включать:

- **Несанкционированный доступ:** злоумышленник может получить несанкционированный доступ к системе, что потенциально приведёт к дальнейшей эксплуатации.
- **Кража данных:** злоумышленник может украсть конфиденциальные данные из взломанной системы, которые могут включать личную, финансовую или служебную информацию.
- **Компрометация системы:** злоумышленник может выполнить произвольный код, направленный на компрометацию системы, позволяя ему изменять, удалять или шифровать файлы.
- **Развёртывание вредоносного ПО:** Злоумышленник может использовать уязвимость для развёртывания вредоносного ПО, включая программу-вымогатель или бэкдор, для поддержания постоянного доступа к системе.
- **Отказ в обслуживании:** злоумышленник может нарушить работу служб путём сбоя системы или потребления ресурсов, что приведёт к отказу в обслуживании.
- **Повышение привилегий:** если уязвимость позволяет, злоумышленник может повысить свои привилегии в системе, получив более высокий уровень контроля.

9) *Различия последствий*

CVE-2024-0204 может привести к полной компрометации системы из-за несанкционированного административного доступа, в то время как CVE-2021-46830 может привести к несанкционированному доступу к определённым областям приложения и потенциальному раскрытию информации.

И CVE-2024-0204 и CVE-2023-0669 могут привести к полной компрометации системы, но CVE-2024-0204 предполагает несанкционированный административный доступ к веб-приложению, в то время как CVE-2023-0669 предполагает удалённое выполнение кода, возможно, из-за ошибки обхода пути.



# IV. STAR BLIZZARD

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!

FAIKELISARDI!



#### A. Введение

Star Blizzard, также известная как Callisto Group, SEABORGIUM, BlueCharlie, TA446, COLDRIVER и TAG-53 известна атаками на правительственные организации, оборонную промышленность, научные круги, аналитические центры, НПО, политиков и других лиц в США, Великобритании, других странах НАТО и странах, соседних с Россией.

Фишинговые кампании Star Blizzard обычно включают отправку поддельных электронных писем, которые, как представляется, исходят от легитимных частных лиц или организаций. Эти электронные письма предназначены для того, чтобы обманом вынудить жертв предоставить учетные данные своей учетной записи электронной почты, которые затем используются для получения несанкционированного (и постоянного) доступа к учетным записям электронной почты жертв. Известно, что после получения доступа Star Blizzard устанавливает правила пересылки почты, предоставляя им постоянный доступ к переписке и спискам контактов жертвы и используя эту информацию для последующего таргетинга и фишинговых действий.

#### B. Распространенные цели фишинговых атак

Фишинговые кампании обычно нацелены на конкретных лиц или организации с целью кражи конфиденциальной информации, такой как учетные данные для входа в систему, или заражения вредоносным ПО:

- **Высокопоставленные должностные лица в организациях:** Эти лица часто имеют доступ к конфиденциальной информации, что делает их привлекательными объектами для кампаний фишинга

- **Лица, участвующие в конфиденциальных операциях:** Люди, которые обрабатывают конфиденциальные данные или операции внутри компании, часто становятся мишенью из-за ценной информации, которую они могут предоставить
- **Конкретные сотрудники компании:** фишинговые кампании могут быть нацелены на конкретных сотрудников компании, особенно на тех, кто имеет доступ к ценным данным или системам
- **Конкретные организации:** Сами организации могут быть объектами кампаний фишинга, особенно в таких секторах, как правительство, оборона, научные круги и неправительственные организации
- **Пользователи социальных сетей:** Злоумышленники часто используют социальные сети и другие общедоступные источники для сбора информации о потенциальных целях

В последние годы было зафиксировано множество фишинговых атак, некоторые из которых включают:

- **Поддельные веб-сайты:** злоумышленники создают поддельные веб-сайты, имитирующие законные, чтобы обманом заставить людей вводить свою личную информацию
- **Whaling-мошенничество:** это включает в себя выдачу себя за руководителя высокого уровня и отправку электронных писем сотрудникам, часто в финансовый отдел, для авторизации банковских переводов на мошеннические счета
- **Вредоносное ПО:** Электронные письма с вредоносными вложениями или ссылками, которые при открытии устанавливают вредоносное ПО на устройство жертвы
- **Фишинг и вишинг:** это формы скрытого фишинга с помощью SMS (smishing) или голосовых вызовов (vishing), когда злоумышленники выдают себя за законные организации для извлечения личных данных или финансовой информации

В фишинговых кампаниях используются различные тактики для повышения их успешности:

- **Выбор цели:** злоумышленники выбирают отдельных лиц или организации, обладающие потенциальным доступом к ценным данным или финансовой выгоде
- **Разведка:** проводится обширное исследование объекта с целью сбора личной информации, должностных ролей и интересов
- **Персонализация:** Электронные письма создаются с использованием конкретной информации о цели, чтобы казаться заслуживающими доверия и релевантными
- **Срочность и давление:** Сообщения часто передают ощущение срочности или давления, побуждающее к немедленным действиям со стороны цели

- **Общие интересы:** злоумышленники могут использовать известные интересы цели для создания убедительного предложения для отправки электронного письма
- **Известные или авторитетные личности:** выдавать себя за кого-либо, занимающего руководящую должность, или известного контактного лица, чтобы вызвать доверие
- **Скомпрометированные учётные записи электронной почты:** они используются для дополнительной фишинговой активности, что указывает на цикл компрометации и эксплуатации, который может самоподдерживаться и расширять масштабы их кампаний

#### 1) Распространенные темы в электронных письмах Star Blizzard о фишинге

Фишинговые электронные письма Star Blizzard часто касаются тем, представляющих интерес для целевой аудитории, которые они выявляют в ходе обширных исследований с использованием ресурсов с открытым исходным кодом, включая социальные сети и профессиональные сетевые платформы. Они могут выдавать себя за известные контакты своих целей или уважаемых экспертов в области, а также создавать учётные записи электронной почты и поддельные профили в социальных сетях для привлечения своих целей.

#### 2) Распространенные вложения или ссылки, включенные в фишинговые электронные письма Star Blizzard

Фишинговые электронные письма часто содержат вредоносные ссылки или вложения. Они предназначены для того, чтобы обманом вынудить жертву предоставить учётные данные своей учётной записи электронной почты, которые затем группа использует для получения несанкционированного постоянного доступа к учётным записям электронной почты жертв. Они также создают вредоносные домены, которые выглядят как домены существующих и легитимных организаций.

#### 3) Общие индикаторы компрометации (IoC), связанные с фишинговыми кампаниями Star Blizzard

Распространённые IoC (без перечисления конкретного списка), связанные с кампаниями Star Blizzard, покрывают активности:

- Несанкционированный доступ к личным и корпоративным учётным записям электронной почты
- Настройка правил пересылки почты, которые обеспечивают им постоянный доступ к переписке жертвы и спискам контактов
- Доступ к данным списка рассылки и списку контактов жертвы, которые они затем используют для последующего таргетинга
- Использование скомпрометированных учётных записей электронной почты для дальнейшей фишинговой деятельности
- Использование фреймворка с открытым исходным кодом Evilginx в своих фишинговых кампаниях, который позволяет им собирать учётные данные и сеансовые файлы cookie, чтобы обойти использование двухфакторной аутентификации

#### 4) Распространенные типы файлов, включенные в фишинговые электронные письма Star Blizzard

### С. Цели кампаний Star Blizzard

С 2019 года Star Blizzard нацелена на различные сектора и отдельных лиц, в том числе:

- **Академические круги:** Образовательные учреждения и частные лица, связанные с исследованиями или обладающие ценной интеллектуальной собственностью
- **Оборонный сектор:** Организации оборонного сектора, включая подрядчиков и поставщиков для вооружённых сил и оборонной промышленности
- **Правительственные организации:** Различные правительственные учреждения и департаменты, которые имеют доступ к конфиденциальной информации о национальной безопасности
- **Неправительственные организации:** Эти организации могут стать мишенью за их участие в чувствительной политической, социальной или гуманитарной деятельности
- **Аналитические центры:** Организации, которые проводят исследования и пропаганду по таким темам, как социальная политика, политическая стратегия, экономика, военное дело, технологии и культура
- **Известные личности:** Политики и другие лица, которые могут иметь доступ к конфиденциальной информации или влиять на важные решения

Конкретные (технические) цели фишинговых кампаний Star Blizzard:

- **Личные адреса электронной почты:** В основном они отправляли фишинговые электронные письма на личные адреса электронной почты целей, которые могут иметь менее строгий контроль безопасности, чем адреса корпоративной электронной почты.
- **Корпоративные или деловые адреса электронной почты:** они также использовали корпоративные или деловые адреса электронной почты целей, что указывает на комплексный подход к нацеливанию как на личные, так и на профессиональные аспекты жизни своих жертв
- **Данные и контакты списка рассылки:** Получив доступ к учётной записи электронной почты жертвы, они получают доступ к данным списка рассылки и списку контактов жертвы, которые затем используют для последующего таргетинга и дальнейшей фишинговой деятельности



Star Blizzard часто включает вредоносные вложения в свои фишинговые электронные письма. Часто используются такие типы файлов, как PDF-файлы, документы Word, электронные таблицы Excel или другие типы файлов, которые могут содержать встроенные скрипты или макросы

#### 5) Распространенные домены или URL-адреса, используемые в фишинговых кампаниях Star Blizzard

Известно, что Star Blizzard использует URL-адреса, имитирующие законные сервисы обмена файлами. Некоторые из распространённых URL-адресов выглядят следующим образом:

- <https://drive.google.com/file/d/XXXXXXXXXXXXXXXXX/view?usp=sharing>
- <https://onedrive.live.com/?authkey=%XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX&cid=8XXXXXXX9B7>
- [https://www.dropbox.com/s/XXXXXXXXXXXXXXXXX/Star\\_Blizzard\\_Report.pdf?dl=0](https://www.dropbox.com/s/XXXXXXXXXXXXXXXXX/Star_Blizzard_Report.pdf?dl=0)

Эти URL-адреса выглядят обычным образом, но на самом деле они предназначены для того, чтобы обманом заставить жертв ввести свои учётные данные или загрузить вредоносные файлы.

#### D. Применяемые методы кампаний Star Blizzard

##### 1) Конкретные методы, используемые Star Blizzard в своих фишинговых кампаниях

Star Blizzard использует различные методы в своих фишинговых кампаниях в т.ч. для предотвращения обнаружения:

- **Целевые электронные письма:** отправляются фишинговые электронные письма на личные адреса электронной почты целей, хотя они также использовали адреса корпоративной или деловой электронной почты целей
- **Импersonизация:** создаются учётные записи электронной почты, выдавая себя за известные контакты своих целей. Они также создают поддельные профили в социальных сетях, которые выдают себя за уважаемых экспертов
- **Вредоносные домены:** создаются вредоносные домены, напоминающие законные организации
- **Evilginx:** используется фреймворк с открытым исходным кодом Evilginx в своих фишинговых кампаниях, который позволяет им собирать учётные данные и сеансовые файлы cookie, чтобы обойти использование двухфакторной аутентификации
- **Переадресация почты:** компрометации учётных данных цели устанавливаются правила переадресации почты, чтобы обеспечить постоянную видимость переписки жертвы и списков контактов

##### 2) Распространенные методы социальной инженерии, используемые Star Blizzard

Методы социальной инженерии Star Blizzard включают:

- **Исследования и подготовка:** проводятся обширные исследования с использованием социальных сетей и профессиональных сетевых платформ, чтобы определить темы, представляющие интерес для привлечения их целевой аудитории
- **Импersonизация:** создаются учётные записи электронной почты и поддельные профили в социальных сетях, выдавая себя за известных контактов или уважаемых экспертов
- **Установление взаимопонимания:** используя собранную информацию, устанавливаются взаимопонимание с целью сделать свои попытки фишинга более убедительными
- **Доставка по электронной почте:** Электронные письма создаются таким образом, чтобы казаться законными и соответствовать интересам или обязанностям цели, часто содержат вредоносные ссылки или вложения
- **PDF-приманки:** отправляемый PDF-файл, обычно нечитаем, с заметной кнопкой, предназначенной для включения чтения содержимого. Нажатие кнопки приводит к тому, что браузер по умолчанию открывает ссылку, встроенную в PDF-файл, что приводит к краже учётных данных

#### E. Новые тактики, техники и процедуры (TTP) и методы предотвращения обнаружения

С 2022 года Star Blizzard заметно улучшила свою способность избегать обнаружения, сосредоточившись на улучшении своих возможностей. Известно пять новых методов:

- **Использование платформ электронного маркетинга:** используются сервисы электронного маркетинга, такие как Mailerlite и HubSpot, для таргетирования фишинговых кампаний
- **Защищённые паролем документы-приманки в формате PDF:** чтобы обойти фильтры электронной почты используются защищённые паролем документы-приманки в формате PDF
- **Использование скомпрометированных учётных записей электронной почты жертвы:** используются скомпрометированные учётные записи электронной почты жертвы для проведения фишинговой активности против контактов первоначальной жертвы
- **Вредоносные ссылки во вложениях электронной почты:** используются вредоносные ссылки, встроенные во вложения электронной почты, чтобы направлять жертв на свои сайты, похищающие учётные данные
- **Использование скомпрометированных учётных данных:** используются скомпрометированные учётные данные, полученные с поддельных страниц входа, для входа в систему от имени пользователей-жертв

### 1) Backend-скрипты

Серверные скрипты – это скрипты, которые выполняются на сервере, в отличие от клиентских скриптов, которые выполняются в браузере пользователя. Используя серверные скрипты, можно контролировать, какая информация отправляется клиенту, а какая хранится на сервере, что затрудняет обнаружение вредоносной активности средствами автоматического сканирования.

Серверные скрипты разработаны для предотвращения автоматического сканирования своих серверов, контролируемых участниками.

Эта тактика, наряду с другими, такими как использование платформ электронного маркетинга, защищённых паролем PDF-документов-приманок и использование скомпрометированных учётных записей электронной почты жертв, позволяет эффективно выполнять фишинговые кампании с повышенной скрытностью.

Ниже приведены примеры функций в составе этих серверных скриптов:

- **Сбор и отправка пользовательских данных:** В апреле 2023 года было замечено, что Star Blizzard отказывается от использования серверов hCaptcha в качестве единственного первоначального перенаправления. Вместо этого они начали выполнять код JavaScript под названием "Collect and Send User Data" перед перенаправлением пользователя
- **Доработка кода JavaScript:** В мае 2023 года исполнитель угрозы доработал код JavaScript, в результате чего появилась обновлённая версия под названием "Docs", которая все ещё используется сегодня
- **Оценка пользовательского окружения:** Серверный JavaScript-код используется для оценки пользовательского окружения позволяет таргетировать атаку в отношении конкретного пользователя

Функции `pluginsEmpty()`, `isAutomationTool()` и `sendToBackend(data)` являются примерами методов, используемых в этих сценариях.

- **`pluginsEmpty()`:** эта функция проверяет, является ли свойство `plugins` объекта `navigator` пустым. Инструменты автоматического сканирования часто не эмулируют плагины, поэтому эта функция может помочь Star Blizzard идентифицировать и игнорировать такие инструменты.
- **`isAutomationTool()`:** Эта функция проверяет наличие признаков того, что клиент является автоматизированным инструментом, а не пользователем-человеком. Это может включать проверку конкретных строк пользовательского агента, наличия определённых свойств JavaScript или скорости взаимодействия.
- **`sendToBackend(data)`:** эта функция отправляет собранные данные обратно на сервер. Данные могут

включать результаты предыдущих проверок или другую информацию о среде клиента. Эта информация может быть использована для адаптации атаки к конкретному пользователю, повышая шансы на успех.

### 2) Услуги платформы для маркетинга по электронной почте

Star Blizzard начала использовать сервисы электронного маркетинга, такие как Mailerlite и HubSpot, для управления своими фишинговыми кампаниями. Эти платформы позволяют создавать кампании электронной почты с выделенным под-домен в сервисе, который затем используется для создания URL-адресов. Эти URL-адреса служат точкой входа в цепочку перенаправлений, заканчивающуюся на серверах, контролируемых участниками.

Использование этих сервисов даёт ряд преимуществ. Во-первых, электронные письма, отправленные через эти платформы, с меньшей вероятностью будут помечены фильтрами электронной почты как спам или вредоносное ПО, поскольку они поступают от известных сервисов. Во-вторых, эти платформы часто предоставляют возможности отслеживания успешности проведения маркетинговых кампаний, что, в свою очередь, позволяет оценить успешность кибер-кампании.

Большинство электронных кампаний Star Blizzard на HubSpot были нацелены на несколько академических институтов, аналитических центров и других исследовательских организаций, использующих общую тему, с целью получения их учётных данных для портала управления грантами США.

### 3) DNS-провайдер

Star Blizzard использует поставщика услуг доменных имён (DNS) для решения инфраструктурных проблем при реализации и управления атаками. Использование DNS-провайдера даёт несколько преимуществ. Во-первых, это позволяет им быстро и легко создавать новые домены для своих атак. Во-вторых, повышается сложность блокирования или удаления таких доменов, поскольку они управляются сторонним сервисом.

### 4) Рандомизирующее DGA для доменов, зарегистрированных актерами

Star Blizzard использует алгоритмы генерации доменов (DGA) для рандомизации доменных имён для своей инфраструктуры. DGA – это алгоритмы, которые генерируют большое количество доменных имён, которые могут использоваться в т.ч. в качестве C&C-серверов.

Использование DGA затрудняет для служб безопасности и автоматизированных систем прогнозирование и блокировку вредоносных доменов, поскольку домены часто меняются и могут казаться случайными. Этот метод помогает избежать обнаружения с помощью списков блокировки, фильтров сигнатур, систем репутации и других средств контроля безопасности.

Используя DGA, возможно систематически переключаться между доменами во время своих атак, затрудняя отслеживание и удаление этих доменов.

5) *Защищенные паролем PDF-файлы являются приманками или ссылками на облачные платформы обмена файлами*

Star Blizzard использовала защищённые паролем документы-приманки в формате PDF или ссылки на облачные файлообменные платформы в рамках своих фишинговых кампаний. Эта тактика служит нескольким целям:

- **Защищённые паролем PDF-файлы-приманки:** использование защищённых паролем PDF-файлов позволяет обойти некоторые системы автоматического сканирования электронной почты, которые не могут анализировать содержимое зашифрованных документов. Пароли для этих документов обычно предоставляются в том же фишинговом электронном письме или в последующем электронном письме.
- **Ссылки на облачные платформы обмена файлами:** Эти ссылки ведут на облачные платформы, где хранятся защищённые PDF-файлы. Использование известных служб обмена файлами может придать видимость достоверности попытке фишинга, а также может ускользнуть от обнаружения системами безопасности, которые доверяют контенту, размещённому на этих платформах.

PDF-файлы часто содержат призыв к действию, такой как кнопка или ссылка, при нажатии на которые пользователь перенаправляется на вредоносный сайт, предназначенный для кражи учётных данных или другой конфиденциальной информации. Этот метод эффективен, поскольку он использует доверие пользователя к знакомым службам обмена файлами и ожидание получения законных документов.

#### F. Воздействие атак

Атака на Microsoft была обнаружена 12 января 2024 года и началась в конце ноября 2023 года. В рамках общей атаки использовалась «password spray»-атака, чтобы скомпрометировать устаревшую непроизводственную тестовую учётную запись клиента с последующим закреплением в системе. Затем использовались разрешения учётной записи для доступа к учётным записям корпоративной электронной почты Microsoft, включая членов команды высшего руководства и сотрудников, занимающихся кибербезопасностью, юридическими и другими функциями.

Исследование электронных писем и их вложений показывает, что изначально они были нацелены на учётные записи электронной почты для получения информации, связанной с самой Blizzard. Атака не была результатом уязвимости в продуктах или службах Microsoft, и нет никаких доказательств того, что субъект угрозы имел какой-либо доступ к клиентской среде, производственным системам, исходному коду или системам искусственного интеллекта по информации от Microsoft.

1) *Действия, предпринятые Microsoft в ответ на кибератаку Blizzard и Инициатива "Безопасное будущее" (SFI)*

В ответ на кибератаку Blizzard корпорация Майкрософт предприняла немедленные действия по расследованию, пресечению вредоносной активности, смягчению последствий атаки и отказу субъекту угрозы в дальнейшем доступе. Они начали уведомлять сотрудников, чьи учётные записи электронной почты были скомпрометированы во время атаки.

Корпорация Майкрософт заверила, что атака не была вызвана какой-либо конкретной уязвимостью в продуктах или службах Microsoft, и нет никаких доказательств того, что субъект угрозы имел какой-либо доступ к клиентской среде, производственным системам, исходному коду или системам искусственного интеллекта.

Microsoft объявила, что они будут применять свои текущие стандарты безопасности к устаревшим системам, принадлежащим Microsoft, даже если эти изменения могут привести к сбоям в существующих бизнес-процессах. Они также планируют внести существенные изменения в свои методы обеспечения внутренней безопасности.

Ответ Microsoft подчёркивает её приверженность устранению угрозы, исходящей от национальных субъектов, таких как Blizzard, и её приверженность ответственной прозрачности, что недавно подтверждено в их инициативе "Безопасное будущее" (SFI).

Инициатива безопасного будущего (SFI) – это программа, представленная Microsoft в ноябре 2023 года. SFI базируется на ключевых аспектах:

- Разработка киберзащиты на основе искусственного интеллекта.
- Достижения в области фундаментальной разработки программного обеспечения.

#### G. Защита (Рекомендации Microsoft)

##### 1) *Руководство по защите*

В ответ на кибератаку Blizzard корпорация Майкрософт представила рекомендации по защите от подобных атак со стороны национальных государств. Это руководство включает разрешение проблемы с использованием следующих аспектов:

- **Многофакторная аутентификация (MFA):** Корпорация Майкрософт подчеркнула важность включения MFA, поскольку в тестовой учётной записи клиента, скомпрометированной в результате атаки, не была включена функция MFA.
- **Мониторинг приложений OAuth:** Субъекты угроз, такие как Blizzard, часто используют приложения OAuth для сокрытия своих действий. Корпорация Майкрософт рекомендует отслеживать подозрительные приложения OAuth и отзываться все, которые не распознаны или не нужны.
- **Осведомлённость об атаках социальной инженерии:** Microsoft Threat Intelligence выявила

целенаправленные атаки социальной инженерии с использованием фишинговых приманок для кражи учётных данных, отправленных в виде чатов Microsoft Teams компанией Blizzard. Осведомлённость и обучение могут помочь пользователям распознавать эти атаки и избегать их.

- **Анализ сетевого трафика:** Blizzard использовала локальные прокси-сети для запуска своих атак, маршрутизируя трафик через огромное количество IP-адресов, также используемых законными пользователями. Мониторинг и анализ сетевого трафика на предмет подозрительных шаблонов может помочь обнаружить такие действия.
- **Регулярное исправление и обновление:** Поддержание систем и программного обеспечения в актуальном состоянии имеет решающее значение для защиты от атак, использующих известные уязвимости.

Защита от вредоносных приложений OAuth:

- **Проверка уровня привилегий:** использование портала авторизации Microsoft Graph Data Connect для проверки уровня привилегий всех удостоверений, как пользователей, так и участников службы, в клиенте. Также важно проверить привилегии, особенно если они принадлежат неизвестным идентификаторам, привязаны к идентификаторам, которые больше не используются, или являются избыточными.
- **Проверка ApplicationImpersonation привилегий** пользователя ApplicationImpersonation: Проверка удостоверений с помощью привилегий ApplicationImpersonation в Exchange Online, поскольку они позволяют участнику службы выдавать себя за пользователя. Использование команды PowerShell Get-ManagementRoleAssignment -Роль ApplicationImpersonation -GetEffectiveUsers для проверки этих разрешений.
- **Определение вредоносных приложений OAuth:** применение политик обнаружения аномалий для обнаружения вредоносных приложений OAuth, которые выполняют конфиденциальные административные действия Exchange Online.
- **Управление приложениями с условным доступом:** реализовать управление приложениями с условным доступом для пользователей, подключающихся с неуправляемых устройств, для мониторинга и контроля того, как они получают доступ к облачным приложениям.
- **Мониторинг разрешений:** мониторинг всех приложений, содержащих EWS. Доступ к пользователю EWS.full\_access\_as\_app с последующим удалением при отсутствии необходимости в их дальнейшем применении.
- **Управление доступом на основе ролей:** реализация механизмов управления доступом на основе ролей для приложений в Exchange Online, чтобы гарантировать, что им предоставляется

доступ только к определённым требуемым почтовым ящикам.

Защита от атак «password spray»

- Устранение небезопасных паролей
- Обучение пользователей
- Сброс скомпрометированные паролей
- Использование Microsoft Entra ID Protection
- Аудит Microsoft Purview.
- Обеспечение защиты пароля с использованием Microsoft Entra для AD
- Обнаружение рисков при входе пользователя в систему

## 2) *Руководство по обнаружению угроз*

После кибератаки Blizzard корпорация Майкрософт предоставила подробное руководство по обнаружению и поиску таких угроз.

- Поиск признаков компрометации:
- Анализ данных журнала
- Инструменты управления поведением пользователя

Руководство Microsoft по обнаружению и отслеживанию кибератак Blizzard включает проверку активности веб-служб Exchange (EWS) и использование Microsoft Entra ID Protection, которая содержит несколько соответствующих обнаружений, помогающих организациям идентифицировать эти методы или дополнительные действия, которые могут указывать на аномальную активность. Использование инфраструктуры локальной прокси-сети субъектами угроз, как правило, с большей вероятностью генерирует предупреждения Microsoft о защите идентификаторов Entra из-за несоответствий в моделях поведения пользователей по сравнению с законными действиями.

К числу предупреждений о защите идентификатора Microsoft Entra, которые могут помочь указать на активность угрозы, связанную с этой атакой, относятся:

- **Незнакомые свойства входа:** это предупреждение помечает входы из сетей, устройств и местоположений, которые не знакомы пользователю.
- **Password-spray атаки:** это обнаружение риска срабатывает, когда успешно выполнена соответствующая атака.
- **Информация об угрозах:** это предупреждение указывает на необычную для пользователя активность или соответствует известным схемам атак.
- **Подозрительные входы (идентификаторы рабочей нагрузки):** это предупреждение указывает на свойства или шаблоны входа, необычные для соответствующего участника службы.

### 3) Оповещения и защита XDR и SIEM

Microsoft Defender для облачных приложений и Microsoft Defender XDR также предоставляют оповещения, которые могут помочь указать на активность, связанную с угрозой. Эти предупреждения включают указания на значительное увеличение обращений к API веб-служб Exchange, подозрительные метаданные, связанные с деятельностью, связанной с почтой, и создание приложения OAuth, которое обращалось к элементам почтового ящика.

Клиенты Microsoft Defender XDR и Microsoft Sentinel также могут использовать специальные поисковые запросы и аналитические правила для поиска связанных действий в своих сетях. К ним относятся запросы для поиска пользователей, выполняющих вход по помеченному IP-адресу, и правила для их идентификации, предоставление разрешения full\_access\_as\_app приложению OAuth и добавление участника / пользователя служб с повышенными разрешениями

Как только субъект решает использовать приложения OAuth для своей атаки, в предупреждениях могут быть указаны различные последующие действия, которые помогут организациям выявлять и расследовать подозрительную активность.

Следующие предупреждения Microsoft Defender для облачных приложений могут помочь определить активность, связанную с угрозой:

- **Приложение с разрешениями только для приложений для доступа к многопользовательским электронным письмам** – многопользовательское облачное приложение с разрешениями только для приложений показало значительное увеличение обращений к API веб-служб Exchange, специфичному для перечисления и сбора электронных писем. Приложение может быть задействовано в доступе к конфиденциальным данным электронной почты и их извлечении.
- **Увеличение числа обращений API приложения к EWS после обновления учётных данных** – это обнаружение генерирует предупреждения для приложений OAuth, отличных от Microsoft, когда приложение показывает значительное увеличение числа обращений к API веб-служб Exchange в течение нескольких дней после обновления его сертификатов / секретов или добавления новых учётных данных.
- **Увеличение числа обращений API приложений к EWS** – это обнаружение генерирует предупреждения для приложений OAuth, отличных от Microsoft, которые демонстрируют значительное увеличение числа обращений к API веб-служб Exchange. Это приложение может быть задействовано в эксфильтрации данных или других попытках доступа к данным и их извлечения.
- **Метаданные приложения, связанные с подозрительной активностью, связанной с почтой** – при этом обнаружении генерируются предупреждения для приложений OAuth, отличных от Microsoft, с метаданными, такими как имя, URL или издатель, которые ранее наблюдались в

приложениях с подозрительной активностью, связанной с почтой. Это приложение может быть частью кампании атак и может быть вовлечено в утечку конфиденциальной информации.

- **Подозрительный пользователь создал приложение OAuth, которое получало доступ к элементам почтового ящика** – пользователь, который ранее входил в сеанс среднего или высокого риска, создал приложение OAuth, которое использовалось для доступа к почтовому ящику с помощью операции синхронизации или к нескольким сообщениям электронной почты с помощью операции привязки. Злоумышленник мог скомпрометировать учётную запись пользователя, чтобы получить доступ к ресурсам организации для дальнейших атак.

Следующее предупреждение Microsoft Defender XDR может указывать на связанную активность:

- **Подозрительный пользователь создал приложение OAuth, которое получало доступ к элементам почтового ящика.** Пользователь, ранее выполнивший вход в сеанс средней или высокой степени риска, создал приложение OAuth, которое использовалось для доступа к почтовому ящику с помощью операции синхронизации или к нескольким сообщениям электронной почты с помощью операции привязки. Злоумышленник мог скомпрометировать учётную запись пользователя, чтобы получить доступ к ресурсам организации для дальнейших атак

Системы расширенного обнаружения и реагирования (XDR) и управления информацией о безопасности и событиях (SIEM) могут обеспечивать оповещения и защиту от вредоносных действий, подобных тем, которые выполняются группой угроз Blizzard.

Microsoft Defender для облачных приложений может генерировать оповещения о различных подозрительных действиях, в том числе:

- Приложение с разрешениями только на доступ к электронным письмам.
- Увеличение числа вызовов API приложений к веб-службам Exchange (EWS) в т.ч. после обновления учётных данных.
- Метаданные приложения, связанные с подозрительными действиями, связанными с почтой.
- Подозрительный пользователь, создающий приложение OAuth с доступом к элементам почтового ящика.
- Microsoft Defender XDR также может генерировать предупреждение, когда подозрительный пользователь создаёт приложение OAuth, которое обращается к элементам почтового ящика.

Для обнаружения «password-spray» атак службы безопасности могут использовать различные поисковые запросы, которые анализируют данные журнала на наличие признаков таких атак:

- **Неудачные попытки аутентификации в нескольких учётных записях:** внезапные

аномальные значения числа неудачных попыток входа в систему или заблокированных учётных записей, которые могут указывать на password-spray атаки

- **Попытки входа из подозрительных местоположений:** попытки входа из местоположений, которые необычны для пользователя, поскольку злоумышленники могут использовать IP-адреса из разных географических регионов
- **Необычное время входа в систему:** атаки часто происходят в часы, когда меньше пользователей, поэтому мониторинг попыток аутентификации в это время может быть полезен
- **Низкие и медленные показатели атак:** ряд атак ориентирован на попытки оставаться незамеченными, не вызывая блокировок учётных записей или пороговых значений неверного пароля
- **Расширенные поисковые запросы:** использование инструмента поиска угроз на основе запросов, такой как расширенный поиск Microsoft Defender, для проверки событий в сети и сбора дополнительной информации, связанной с предупреждениями о спрее пароля
- **Классификация предупреждений:** проверка пользователя на другие предупреждения до действия по удалению пароля, такие как предупреждения о невозможных поездках, действия из редких стран/регионов или подозрительные действия по удалению электронной почты

Ряд поисковых запросов, рекомендуемых корпорацией Майкрософт:

```
// Find sign-ins by a labeled password spray IP
IdentityLogonEvents
| where Timestamp between (startTime .. endTime)
| where isempty(IPTags) and not(IPTags
has_any('Azure','Internal Network IP','branch office'))
| where IPTags has_any ("Brute force attacker", "Password
spray attacker", "malicious", "Possible Hackers")
```

```
// Find MailItemsAccessed or SaaS actions performed by a
labeled password spray IP
CloudAppEvents
| where Timestamp between (startTime .. endTime)
| where isempty(IPTags) and not(IPTags
has_any('Azure','Internal Network IP','branch office'))
| where IPTags has_any ("Brute force attacker", "Password
spray attacker", "malicious", "Possible Hackers")
```

Анализ сетевого трафика может быть мощным инструментом для обнаружения password-spray атак:

- **Системы обнаружения вторжений (IDS):** инструменты IDS отслеживают сетевой трафик и помечают подозрительные действия при входе в систему. Они анализируют попытки входа в систему, блокировки учётных записей и сбои аутентификации, чтобы выявить потенциальные атаки с использованием паролей

- **Мониторинг безопасности:** непрерывный мониторинг действий пользователя при входе в систему и аномальных шаблонов может помочь выявить потенциальные атаки. Инструменты мониторинга могут отслеживать попытки входа в систему из необычных мест или в необычное время, что может указывать на атаку с использованием пароля.

- **Анализ поведения пользователя:** анализ поведения пользователя может помочь обнаружить подозрительные действия. Отклонения от нормального поведения, такие как попытки входа в систему в нерабочее время или одновременные попытки входа в систему из нескольких мест, могут быть предупреждающими знаками для атак с использованием паролей

- **Настройка параметров пароля безопасности:** если в организации используется платформа ведения журнала безопасности, необходимо убедиться, что она настроена на идентификацию или обнаружение неудачных попыток входа во всех системах. Это поможет вам в будущем обнаруживать характерные признаки атак с использованием паролей

- **Мониторинг и ведение журнала:** это одни из лучших превентивных способов обнаружения атак с использованием паролей. Они помогают обнаруживать неудачные попытки входа в систему и соответствующим образом информировать ИТ-администратора. Например, при 5 неудачных попытках входа в систему политика паролей блокирует учётную запись пользователя, а решение для мониторинга сети подаёт сигнал тревоги ИТ-администратору

- **SIEM:** в случае необычного поведения в организации система SIEM зафиксировала это. Решения SIEM собирают и анализируют данные о событиях в режиме реального времени с сетевых устройств, серверов, контроллеров домена и многого другого, предоставляя аналитические данные о безопасности для анализа в режиме реального времени предупреждений о безопасности, генерируемых приложениями и сетевым оборудованием

Организации могут использовать разрешения приложений OAuth для обнаружения потенциальных уязвимостей безопасности несколькими способами:

- **Расследование и устранение опасных приложений OAuth:** организации могут использовать такие инструменты, как Microsoft Defender для облачных приложений, для расследования и устранения опасных приложений OAuth. Это включает в себя тщательную проверку приложений, которые недавно не обновлялись, приложений с несоответствующими разрешениями и приложений, которые кажутся подозрительными на основе их названия, издателя или URL. Аудит приложения OAuth можно экспортировать для дальнейшего анализа пользователей, авторизовавших приложение

- **Создание политик для управления приложениями OAuth:** организации могут

устанавливать политики разрешений для получения автоматических уведомлений, когда приложение OAuth соответствует определённым критериям. Например, оповещения можно настроить для приложений, которым требуется высокий уровень разрешений. Политики приложений OAuth позволяют организациям отслеживать, какие разрешения запрашивало каждое приложение, и какие пользователи авторизовали эти разрешения

- **Выявление уязвимостей в реализации OAuth:** уязвимости могут возникать в реализации OAuth клиентским приложением, а также в конфигурации самой службы OAuth. Выявление и использование этих уязвимостей может помочь организациям защитить свои собственные приложения от аналогичных атак
- **Мониторинг вредоносных приложений OAuth:** участники угроз могут злоупотреблять приложениями OAuth для автоматизации финансовых атак. Мониторинг такого

злоупотребления может помочь организациям обнаруживать потенциальные уязвимости в системе безопасности и реагировать на них. Например, Microsoft предоставляет запросы, которые можно использовать для идентификации отправителей электронной почты с высоким уровнем исходящей почты и подозрительных событий электронной почты

- **Понимание последствий согласия вредоносного приложения OAuth:** если пользователь предоставляет доступ к вредоносному стороннему приложению, приложение может получить доступ к данным пользователя и выполнять действия от его имени. Понимание последствий таких действий может помочь организациям разработать стратегии обнаружения и устранения потенциальных уязвимостей в системе безопасности



v. **DARKPINKAPT**





#### A. Введение

АРТ-атаки, распространяющиеся по Азиатско-тихоокеанскому региону (АРАС), приписываемые группе, известной как Dark Pink, также называемой Saaiwc Group начались ещё в середине 2021 года, но значительно усилились во второй половине 2022 года. Многие из этих атак, изначально направленные против стран АРАС, были расширены на европейские правительственные учреждения.

Группа использует различные инструменты и специально созданное вредоносное программное обеспечение, предназначенное для кражи данных и шпионажа. Значительную часть успеха Dark Pink можно отнести к фишинговым электронным письмам, используемых для получения первоначального доступа. Эти электронные письма содержат сокращённый URL-адрес, ведущий на бесплатный файлообменный сайт, где жертве предоставляется возможность загрузить ISO-образ, содержащий все файлы, необходимые субъектам угрозы для заражения сети жертвы.

Последствия успешной атаки Dark Pink АРТ могут быть серьёзными для пострадавшей организации. Продвинутые механизмы закрепления в системе группы позволяют им поддерживать доступ к сети жертвы в течение длительного периода времени и продолжать извлекать данные, нанося дальнейший ущерб.

Основными целями Dark Pink АРТ являются корпоративный шпионаж, кража документов и прослушивание звука через микрофоны скомпрометированных устройств. Также было обнаружено, что группа вымогала данные из мессенджеров. В дополнение к этому группа нацелилась на организации в Бельгии, Таиланде и Брунее.

Хронология деятельности Dark Pink АРТ Group

- **Середина 2021 года:** впервые замечена деятельность Dark Pink АРТ group.

- **2022:** Их деятельность активизируется, особенно во второй половине года.
- **Октябрь 2022 года:** предпринята неудачная атака на европейское государственное агентство развития, действующее во Вьетнаме.
- **Январь-апрель 2023 года:** Новые модули загружены в учётную запись GitHub, связанную с группой, что предполагает постоянное развитие их набора инструментов

#### B. Основные задачи Dark Pink АРТ Группы

Основные цели Dark Pink АРТ group включают:

- **Корпоративный шпионаж:** Проведение корпоративного шпионажа, который включает в себя кражу конфиденциальной информации у корпораций с целью получения конкурентного преимущества
- **Кража документов:** Группа активно занимается кражей документов, которые содержат конфиденциальную информацию, принадлежащую частной собственности
- **Видеонаблюдение:** Dark Pink обладает возможностью захвата звука через микрофоны взломанных устройств, которые могут использоваться для подслушивания частных разговоров и встреч
- **Удаление данных с платформ обмена сообщениями:** Группа также занимается удалением данных с различных платформ обмена сообщениями, что указывает на интерес к личной и потенциально конфиденциальной информации, передаваемой по этим каналам
- **Географическая направленность:** хотя большинство атак Dark Pink были направлены против стран Азиатско-Тихоокеанского региона, они также были нацелены на европейское правительственное министерство, демонстрируя расширение их географического охвата
- **Профиль жертвы:** Подтверждённые жертвы включают военные организации на Филиппинах и в Малайзии, правительственные учреждения в Камбодже, Индонезии и Боснии и Герцеговине, а также религиозную организацию, что демонстрирует интерес группы к ценным и разнообразным целям
- **Фишинг-рассылка для первоначального доступа:** Важным фактором успеха операций Dark Pink является использование фишинговых электронных писем, содержащих сокращённый URL. Этот URL-адрес приводит жертв на сайт обмена файлами, где их обманом заставляют загрузить ISO-образ, содержащий вредоносные файлы, необходимые для заражения сети
- **Эволюция методов эксфильтрации:** Компания Dark Pink усовершенствовала свои методы эксфильтрации данных, перейдя от электронной почты и общедоступных облачных сервисов, таких как Dropbox, к использованию протокола HTTP и сервиса Webhook в более поздних атаках

### C. Инструменты Dark Pink APT Group

Ниже приводится информация об инструментах, широко используемых группой Dark Pink для атак, получения доступа и эксфильтрации данных с устройств.

#### 1) Инструменты, используемые Dark Pink APT Group

Группа APT Dark Pink использует в своих атаках набор специализированных вредоносных инструментов, в первую очередь полагаясь на фишинговые электронные письма для получения доступа к сетям своих целей. Примечательным фактом является использование TelePowerBot и KamiKakaBot, которые предназначены для удаления конфиденциальных данных со скомпрометированных хостов. Они были связаны с новой версией вредоносного ПО KamiKakaBot, которая доставляется через фишинговые электронные письма вредоносным ISO-файлом. Этот файл содержит WinWord.exe, который используется для проведения sideload атаки с загрузкой библиотеки динамических ссылок (DLL). Также было обнаружено, что группа использует легитимный MsBuild.exe для запуска вредоносного ПО KamiKakaBot на устройствах жертв. Технология обфускации вредоносного ПО была улучшена с использованием .NET-обфускатора для противодействия антивирусным решениям. Группа также использует специальную утилиту для эксфильтрации мессенджеров под названием ZMsg, которая загружается с GitHub и нужна для кражи сообщений из Viber, Telegram и Zalo.

В дополнение к этому было обнаружено, что Dark Pink использует методы сторонней загрузки DLL и событийного запуска своих полезных нагрузок. Они также используют различные методы и сервисы для передачи данных, включая электронную почту, общедоступные облачные сервисы, такие как Dropbox.

#### 2) Внесены изменения в инструменты, используемые Dark Pink APT Group

У группы есть ссылки на учётную запись GitHub, где они хранят сценарии PowerShell, ZIP-архивы и пользовательские вредоносные программы, разработанные для будущего развёртывания на целевых устройствах. Также было замечено, что они используют уязвимость нулевого дня WinRAR (CVE-2023-38831) в своих атаках для выполнения вредоносного несанкционированного кода. Они использовали эту уязвимость, внедряя вредоносные исполняемые файлы в типы файлов, такие как PDF и JPG, в ZIP-архивы. Эта тактика позволяет злоумышленникам устанавливать вредоносное ПО на устройство пользователя, не вызывая подозрений, поскольку жертва считает, что они взаимодействуют с безвредным файлом. Файл эксплуатации, созданный Dark Pink, включает PDF файл-приманку и папку с таким же именем. Внутри папки находятся два файла: один представляет собой исполняемую программу с тем же именем, что и файл PDF, а другой – файл библиотеки с именем 'twinapi.dll'. Группа также использует такие методы, как заражение через USB и эксплуатация DLL.

#### 3) Новая тактика, применяемая Dark Pink APT Group

Новая тактика, используемая Dark Pink APT, включает в себя использование различных бинарных файлов Living Off the Land (LOLBins) и использование функциональных возможностей надстройки MS Excel для закрепления.

Полезные данные также распределяются через службу TextBin.net, и было замечено, что группа отфильтровывает украденные данные с использованием HTTP-протокола. Эта новая тактика указывает на постоянные усилия группы

по расширению своих возможностей, уклонению от обнаружения и сохранению контроля над скомпрометированными сетями.

### D. Методы извлечения данных

Методы извлечения включают.

- **Разнообразие методов эксфильтрации:** Компания Dark Pink использовала ряд методов и сервисов для эксфильтрации данных от своих целей.
- **Общедоступные сервисы:** общедоступные облачные сервисы, такие как Dropbox, использовались Dark Pink для фильтрации данных
- **Использование электронной почты и облачных сервисов:** В предыдущих атаках группа отправляла украденную информацию по электронной почте или использовала общедоступные облачные сервисы для извлечения данных. Это указывает на то, что они использовали платформы связи и хранения для перемещения данных из скомпрометированных сетей
- **Переход на протокол HTTP и сервис Webhook:** совсем недавно Dark Pink перешла на использование протокола HTTP и сервиса Webhook для удаления украденных данных. Это изменение тактики может быть попыткой избежать обнаружения системами безопасности, которые в большей степени ориентированы на традиционные методы эксфильтрации

Группа Dark Pink APT использует Telegram и сервис Webhook для обмена данными.

**Telegram:** Dark Pink использует telegram как для командования и контроля, так и для передачи данных. Было замечено, что группа использует Telegram-бота для выполнения команд и управления кражей данных. Украденные данные часто отправляются в чат Telegram в zip-архиве. Этот метод обеспечивает безопасный и зашифрованный канал для передачи данных, затрудняя системам безопасности обнаружение и блокировку.

**Webhook:** Webhook.site — это сервис, который позволяет пользователям создавать временные конечные точки для сбора и просмотра входящих HTTP-запросов. Dark Pink использует этот сервис для фильтрации украденных данных по HTTP. Этот метод позволяет группе отправлять данные по определённому URL-адресу, к которому затем могут получить доступ субъекты угрозы. Метод может быть использован для предотвращения обнаружения системами безопасности, которые в большей степени ориентированы на традиционные методы эксфильтрации.

Группа использует частный репозиторий GitHub для размещения дополнительных модулей, загружаемых её вредоносным ПО. Они также разработали новые инструменты для удаления данных, позволяющие избежать обнаружения. Один из методов группы включает использование вредоносной программы KamiKakaBot, которая в первую очередь предназначена для кражи данных, хранящихся в веб-браузерах, таких как Chrome, Edge и Firefox, включая сохранённые учётные данные, историю посещённых страниц и файлы cookie.

Кроме того, они используют специализированный инструмент на базе .NET, известный как Cusky. Этот инструмент умеет извлекать пароли, историю посещённых

страниц, учётные данные для входа и файлы cookie из ряда веб-браузеров, на которые нацелена группа. Украденные данные хранятся локально в каталоге %TEMP%\backu\log, без передачи по сети

#### *Е. Объекты и субъекты атак*

Многие атаки Dark Pink были направлены против стран Азиатско-Тихоокеанского региона, хотя группа расширила сферу своей деятельности, нацелившись на европейское правительство министерство. Это свидетельствует о расширении сферы их деятельности.

##### *1) Отрасли, на которые нацелена Dark Pink APT Group*

Группа Dark Pink APT нацелена на широкий спектр отраслей, включая правительство, вооружённые силы, некоммерческие организации, образовательные учреждения и агентства по развитию в Азиатско-Тихоокеанском регионе и Европе. Конкретные отрасли, упомянутые в контексте их атак, включают розничную торговлю, здравоохранение, игры, технологии, программное обеспечение, фармацевтику, аэрокосмическую промышленность, оборону, автомобилестроение и СМИ.

##### *2) Новые отрасли, нацеленные на Dark Pink APT Group*

Группа компаний Dark Pink APT расширила свои целевые отрасли и географический охват. Ранее считалось, что группа сосредоточена в основном на странах Юго-Восточной Азии, но новые жертвы были выявлены в Бельгии, Таиланде и Брунее. Группа была связана с пятью новыми атаками, направленными против различных организаций в этих странах (Камбоджа, Индонезия, Малайзия, Филиппины, Вьетнам, Босния и Герцеговина)

#### *Ф. Первоначальный доступ и выполнение и Закрепление трояна*

К методам первоначального доступа относятся:

- **Фишинговые электронные письма:** Значительную часть успеха Dark Pink можно отнести к фишинговым электронным письмам, используемым для получения первоначального доступа. Эти электронные письма содержат сокращённый URL-адрес, ведущий на бесплатный сайт для обмена файлами
- **ISO-образ:** Жертвам предоставляется возможность загрузить ISO-образ с сайта обмена файлами. Это изображение содержит все файлы, необходимые субъектам угрозы для заражения сети жертвы
- **Выполнение и закрепление трояна:** как только ISO-образ загружен и открыт, он запускает выполнение трояна на устройстве жертвы. Этот троян предназначен для сохранения работоспособности заражённой системы, позволяя субъектам угрозы сохранять доступ в течение длительного периода

Шпионский фишинг — это разновидность фишинг-атаки, нацеленной на конкретных лиц или группы внутри организации. Это мощный вариант фишинга, вредоносной тактики, которая использует электронную почту, социальные сети, системы мгновенного обмена сообщениями и другие платформы, чтобы заставить пользователей разглашать личную информацию или совершать действия, которые приводят к потере данных или финансовым потерям. Фишинговые атаки в высшей

степени персонализированы и часто требуют предварительного изучения цели. Злоумышленники маскируются под надёжного друга или организацию, чтобы получить конфиденциальную информацию, как правило, по электронной почте или с помощью других онлайн-сообщений. Целью шпионского фишинга является кража конфиденциальной информации, такой как учётные данные для входа в систему, или заражение устройства жертвы вредоносным ПО. При шпионском фишинге киберпреступники рассылают весьма убедительные электронные письма конкретным сотрудникам организации. Эти электронные письма часто содержат вредоносные вложения или ссылки, которые при нажатии на могут доставить троянские программы в систему жертвы. Например, троян Ursnif использует сохранённые электронные письма компании для отправки того, что кажется законными электронными письмами. Эти электронные письма содержат вложение в документ Word с вредоносной макрокомандой, который загружает вредоносное ПО. После выполнения полезной нагрузки компьютер жертвы становится средством доставки для распространения внутри организации

ISO-образы – это файлы, содержащие полную копию CD, DVD или других типов носителей. Они часто используются для распространения программного обеспечения или данных. Киберпреступники начали использовать ISO-файлы для первоначального взлома, поскольку они могут помочь избежать проверок безопасности, предназначенных для поиска архивированных файлов. Вредоносные ISO-файлы использовались для доставки различных типов вредоносных программ, включая трояны IcedID, LokiBot и NanoCore. ISO-файл обычно доставляется как часть кампании malspam, и когда пользователь нажимает на ISO-файл, создается новый виртуальный жёсткий диск. Были замечены киберпреступники, использующие файлы ISO-образов во вредоносных спам-кампаниях для доставки троянов (LokiBot и NanoCore). Файл ISO доставляется в виде ZIP-архива с помощью вредоносной рассылки спама. Когда пользователь нажимает на файл ISO, создаётся новый виртуальный жёсткий диск. ISO-файл содержит вредоносный LNK-файл и скрытый каталог, содержащий полезную нагрузку. Когда жертва нажимает на LNK-файл, это запускает выполнение полезной нагрузки. Этот метод все чаще используется по мере того, как субъекты угроз стремятся обойти контроль, установленный в Сети. Файлы ISO часто пропускаются антивирусным ПО, что повышает вероятность того, что злоумышленники смогут доставить их полезную нагрузку незамеченными.

Выполнение трояна относится к процессу запуска троянской программы-коня в компьютерной системе. Трояны — это вредоносные программы, которые маскируются под законное программное обеспечение. Они могут быть использованы для получения несанкционированного доступа к компьютерной системе и выполнения различных вредоносных действий. Например, вредоносная программа IcedID, содержащаяся в ISO-образе, запускается, когда пользователь нажимает на файл LNK на виртуальном жёстком диске, созданном этим ISO-файлом. Трояны используют различные методы закрепления, чтобы гарантировать, что они продолжают работать в системе даже после её перезагрузки или после запуска программного обеспечения безопасности. Некоторые распространённые методы включают изменение реестра, создание запланированных задач, установку себя как службы или использование руткитов для сокрытия своего

присутствия. Другие методы включают злоупотребление законными процессами операционной системы, такими как добавление записи в ключи запуска в реестре Windows или папке автозагрузки, что гарантирует, что любые программы, на которые ссылаются, будут выполняться при входе пользователя в систему. Некоторые менее распространённые, но более сложные методы включают злоупотребление параметрами выполнения файла.

Закрепление в системе относится к методам, используемым для сохранения доступа к скомпрометированной системе даже после перезагрузки системы или удаления первоначального вектора заражения, включая добавление записей в ключи запуска в реестре Windows или папке автозагрузки, для автозапуска вредоносного кода. Это сохраняет доступ к сети при поиске нужных им данных, и для распространения других вредоносных программ. Решения типа трояна Ursnif, используют методы закрепления с помощью команды внутри раздела реестра и запуск её с помощью командной строки инструментария управления Windows (WMIC).

#### 1) Примеры троянских программ, поставляемых с помощью фишинговых атак

Трояны могут быть доставлены с помощью фишинговых атак, которые носят целенаправленный характер и включают сложные методы социальной инженерии:

- **OutSteel и SaintBot:** трояны использовались при атаках на энергетическую организацию в Украине в рамках более масштабной кампании
- **Ursnif:** банковский троян использует сохранённые электронные письма компании для отправки сообщений, которые кажутся легитимными, с вложением в документ Word, содержащим вредоносный макрос, который загружает вредоносное ПО
- **TrickBot:** троян, распространяемый в основном с помощью фишинговых кампаний с использованием специально подобранных электронных писем с вредоносными вложениями или ссылками
- **IcedID:** Поставляемый в ISO-образе в рамках кампании malspam, этот троян использовался для обхода средств контроля доступа в Интернете.

#### 2) Общие признаки заражения трояном при использовании ISO-образов

После заражения ISO-трояном для доставки вредоносного ПО, может быть несколько признаков:

- **Неожиданная реклама:** Рекламные объявления могут появляться там, где их быть не должно, что может быть признаком разновидности трояна
- **Изменённая домашняя страница:** Домашняя страница веб-браузера может изменяться без разрешения, что указывает на то, что может присутствовать другой тип трояна

- **Подозрительные процессы:** Процессы, связанные с трояном ISO-файлам, могут выполняться в фоновом режиме без ведома пользователя
- **Перенаправленные ссылки:** Ссылки могут перенаправлять на сайты, отличные от ожидаемых, что может быть признаком трояна, манипулирующего веб-трафиком
- **Повреждённые файлы:** Открытие файла и обнаружение его повреждения может свидетельствовать о проникновении вредоносного ПО
- **Странные всплывающие окна:** Некоторые формы вредоносного ПО могут маскироваться под законные программы, и неожиданные всплывающие окна могут быть признаком такой тактики
- **Новые или изменённые файлы:** Некоторые типы вредоносных программ могут создавать копии файлов или вводить в систему новые файлы, часто с общими названиями, чтобы избежать обнаружения

#### G. IoCs

Показатели компрометации IoCs включают:

IP-адреса:

- 185.141.63[.]128
- 185.141.63[.]129
- 185.141.63[.]130
- 185.141.63[.]131

Домены:

- hxxp://185.141.63[.]128/office/update/
- hxxp://185.141.63[.]129/office/update/
- hxxp://185.141.63[.]130/office/update/
- hxxp://185.141.63[.]131/office/update/
- hxxp://185.141.63[.]128/office365/update/
- hxxp://185.141.63[.]129/office365/update/
- hxxp://185.141.63[.]130/office365/update/
- hxxp://185.141.63[.]131/office365/update/

Хэши файлов:

- 5f4dcc3b5aa765d61d8327deb882cf99
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6

THE KIRNGS OF BRUTE-ORECE  
THE OF DFTRR-FORCE AND IND DDDOS,

VI. **KILLNET: КИБЕР-  
ЗВЕЗДА  
ДРАМКРУЖКА  
"DDOS"**





#### А. Введение

KillNet – кибер-группа, которая стала лидером среди более чем сотни подобных групп, возникших в результате прокси-кибервойн. Основные стратегии KillNet вращаются вокруг проведения низкоуровневых распределённых атак типа "Отказ в обслуживании" (DDoS) против критической инфраструктуры, государственных служб, веб-сайтов аэропортов и медиапредприятий в странах НАТО.

KillNet также известен своими активными и конфронтационными усилиями по дезинформации, нацеленными на 90 000 подписчиков Telegram. Эти кампании включают в себя буллинг над жертвами их DDoS-атак и распространение угроз. Например, атака KillNet'a на веб-сайте Европарламента привело к его временной недоступности. В ответ на расследование, начатое против KillNet в связи с нападением на Европейский парламент, группа атаковала бельгийский центр кибербезопасности.

Группа Anonymous Sudan, очевидно, расширила возможности KillNet, и стала самым продуктивным филиалом коллектива в 2023 году, проведя большинство заявленных DDoS-атак. KillNet также заявила, что насчитывает 280 членов в США, приписывая атаку на Boeing своим американским "коллегам".

Виктимология KillNet обширна и включает в себя различные сектора и страны:

- **География (атак):** Большинство жертв KillNet находятся в Европе; зарегистрировано более 180 атак, из них не менее 10 – в Северной Америке атак
- **Целевые отрасли:** Общие цели включают финансовую отрасль, транспорт, правительственные учреждения и бизнес-услуги
- **Сектор здравоохранения:** таргетирование отрасли здравоохранения США также вызывает опасения из-

за потенциального воздействия на важнейшие службы здравоохранения

- **Государственные службы:** сообщалось об атаках на правительственные веб-сайты в нескольких странах, включая Румынию, Молдову, Латвию и Соединённые Штаты
- **Транспорт:** Аэропорты и другие транспортные системы США подверглись DDoS-атакам
- **Предприятия средств массовой информации:** также пострадали медиакомпании в странах НАТО

Со временем KillNet разработала полуофициальную организационную структуру со значительным присутствием в Telegram и начала расширять свою деятельность. Группа начала создавать глобальную команду операторов из даркнета, предлагая такие услуги, как дезинформация, воздействие на сетевую инфраструктуру, репутационные атаки, эксфильтрация данных и утечки данных, наряду с DDoS атаками. Они также разработали свои собственные инструменты и ботнеты после первоначального использования инструментов с открытым исходным кодом.

#### В. Тактика

Основные стратегии KillNet основаны на DDoS-атаках и bruteforce-атаках.

##### 1) DDoS-атаки

KillNet в основном использует низкоуровневые DDoS-атаки. Группа обычно не использует сложных инструментов или стратегий, и, хотя их DDoS-атаки могут вызвать перебой в обслуживании, они обычно не приводят к серьёзному ущербу. KillNet проводит DDoS-атаки на уровень 4 модели OSI (SYN flood-атаки) и уровень 7 (массовые запросы POST/GET). Целью этих атак является истощение ресурсов путём заполнения целевой службы вредоносными запросами на подключение.

##### 2) bruteforce-атаки

KillNet также использует bruteforce-атаки против различных сервисов. В этих атаках используются предопределённые списки слов для поиска незащищённых сервисов, которые пытаются использовать учётные данные по умолчанию или слабые учётные данные. Группа в первую очередь нацелена на такие сервисы, как FTP (порт 21), HTTP (порт 80), HTTPS (порт 443) и SSH (порт 22), а также на серверы Minecraft и TeamSpeak.

##### 3) Цели DDoS-атак

DDoS-атаки в первую очередь были нацелены на критически важную инфраструктуру, правительственные службы и медиа-компании в странах НАТО, включая США, Канаду, Австралию, Италию. Не исключением стали и международные институты, партнёры НАТО, и страны, включая Германию, Данию, Швецию, Францию, Польшу, Словакию, Украину, Израиль, Объединённые Арабские Эмираты (ОАЭ) и другие страны-союзники и партнёры НАТО, такие как Япония.

Группа также нацелена на организации в секторах здравоохранения, финансовой индустрии, транспортной и секторах бизнес-услуг. Отдельные цели KillNet включают военные объекты, морские терминалы и объекты материально-технического обеспечения, другие виды транспорта и системы онлайн-торговли.

Важно отметить, что, хотя DDoS-атаки KillNet могут вызывать перебои в обслуживании на несколько часов или даже дней, они обычно не наносят серьёзного ущерба. Однако они могут нарушать работу основных служб и представлять серьёзную угрозу для организаций, особенно в таких критически важных секторах, как здравоохранение.

#### 4) Методы атак

Основным вектором атаки KillNet является DDoS, который включает в себя «заполнение» целевой службы вредоносными запросами на подключение, что приводит к истощению ресурсов. Известно также, что группа занималась извлечением данных из целевых сетей, включая почтовые ящики высокопоставленных чиновников и банковские данные.

Что касается инструментов, KillNet использовала множество методов, включая сценарии DDoS и вербовку ботнетов и использование поддельных источников атак для маскирования, а в октябре 2023 года KillNet начала продавать новый инструмент для DDoS-атак с арендой (на день, неделю, месяц). Всё это ожидаемо должно увеличить количество новых атак.

Группа использует несколько известных DDoS-инструментов, включая "Aura-DDoS", "Blood", "DDoS Ripper", "Golden Eye", "Hasoki" и "MHDDoS". Они также используют инструмент под названием "CC-Attack", который автоматизирует использование открытых прокси-серверов и включает методы рандомизации, позволяющие избежать обнаружения на основе сигнатур. Кроме того, было замечено, что KillNet использует slow-POST DDoS атаки и ICMP-флуд, атаки с IP-фрагментацией, TCP SYN flood, TCP RST flood, TCP SYN / ACK, NTP flood, DNS amplification и CLAP-атаки (LDAP connectionless).

#### 5) Подбор персонала

Деятельность KillNet не ограничивалась кибератаками. Группа занималась вербовкой, сбором средств и продвижением своих идей по различным каналам, включая социальные сети, для расширения своей базы поддержки, ориентируясь на людей с различными наборами навыков, включая программистов, сетевых инженеров, тестировщиков на проникновение, системных администраторов и социальных инженеров. Несмотря на заявления лидера группы KillNet об уходе из группы в середине 2022 года, он продолжает оставаться центральным координатором коллектива KillNet.

В 2023 году группа объявила о запуске своей Dark School, школы по борьбе с киберпреступностью, целью которой является обучение следующей когорты и пополнение рядов коллектива. KillNet набирает новых участников, активно подыскивая подходящих кандидатов среди сторонников своего дела, используя различные каналы социальных сетей, такие как Telegram и VK. У них

есть подробная форма, которую потенциальные новобранцы должны заполнить, прежде чем их будут рассматривать для вступления. KillNet работает с военной структурой, с чёткой иерархией сверху вниз и множеством небольших отрядов, которые они называют своим "Легионом" которые действуют в соответствии с инструкциями, раздаваемыми в их Telegram-каналах.

#### С. Цели, воздействие и последствия атак

Последствия атак KillNet могут варьироваться от временных перебоев в обслуживании до потенциальных финансовых потерь и ущерба репутации. Правительственные меры реагирования включали классификацию KillNet как террористической организации и рассылку предупреждений через агентства кибербезопасности.

##### 1) Индустрия здравоохранения

KillNet нацелен на сектор здравоохранения США (HPI) с декабря 2022 года. Их фирменные DDoS-атаки на критически важные секторы инфраструктуры обычно приводят к перебоям в обслуживании, длящимся несколько часов или даже дней. Эти атаки имеют серьёзные последствия, поскольку они могут прервать уход за пациентами, привести к потере данных о них и нарушить связь между поставщиками медицинских услуг. В январе 2023 года KillNet и ее филиалы провели многочисленные скоординированные DDoS-атаки на организации здравоохранения в США, что привело к перебоям в обслуживании и значительным нарушениям рутинных и важнейших повседневных операций, длящимся несколько часов или даже дней. В некоторых случаях группа также краля данные из ряда больниц. Эти атаки в первую очередь были нацелены на системы здравоохранения как многопрофильные больницы, также и одиночные в том числе с травматологическими центрами первого уровня.

Роль правоохранительных органов в противодействии атакам KillNet включает расследование инцидентов, координацию с международными правоохранительными группами и принятие мер по пресечению деятельности группы. Например, ФБР в координации с международными правоохранительными органами и Европоллом ранее проникало в инфраструктуру других групп, представляющих киберугрозу.

Агентство по кибербезопасности и инфраструктурной безопасности (CISA) также играет важную роль в оказании помощи организациям в реагировании на такие атаки. CISA предоставляет ресурсы и рекомендации, помогающие организациям защищаться от киберугроз, и работает с пострадавшими организациями над смягчением последствий атак.

##### 2) Энергетическая и финансовая промышленность

В энергетическом секторе атаки могут нарушить работу промышленных систем управления, поддерживающих энергетическую инфраструктуру США. Хотя влияние на способность энергетического сектора предоставлять локализованные услуги пока было минимальным, угроза сохраняется. В случае успеха эти атаки потенциально могут нарушить энергоснабжение, что приведёт к перебоям в

подаче электроэнергии и повлияет на критически важную инфраструктуру.

В финансовом секторе DDoS-атаки становятся все более серьёзной проблемой. Эти атаки могут вызывать периодические простои, вынуждая сотрудников службы безопасности отражать атаки, потенциально нарушая финансовые транзакции. KillNet даже пригрозил неминуемыми атаками на банковскую систему SWIFT и другие финансовые учреждения. Хотя фактическое воздействие этих угроз является неопределённым, в случае успеха они потенциально могут нарушить глобальные финансовые транзакции.

Важно отметить, что, хотя KillNet использует DDoS в качестве своего основного инструмента, этот метод обычно используется скорее для привлечения внимания, чем для нанесения серьёзного ущерба. Тем не менее, группа наращивает свои возможности и демонстрирует готовность атаковать критически важные объекты инфраструктуры. Таким образом, хотя фактический ущерб, причинённый атаками KillNet, до сих пор был минимальным, существует потенциал для более значительных сбоев.

### 3) *Авиационная промышленность*

Эти атаки в первую очередь были нацелены на общедоступные веб-сайты аэропортов, в результате чего они замедлили работу или стали полностью недоступны. Группа атаковала более 30 европейских аэропортов и несколько крупных аэропортов США, включая международный аэропорт Атланты Хартсфилд-Джексон, международный аэропорт Лос-Анджелеса, международный аэропорт Чикаго О'Хара, международный аэропорт Орlando, международный аэропорт Денвера, международный аэропорт Феникс Скай Харбор и другие.

DDoS-атаки привели к сбоям в работе веб-сайтов аэропортов, что повлияло на взаимодействие клиентов с авиакомпаниями. Однако теракты не повлияли на важнейшие операции аэропорта и не сорвали полёты. Европейское агентство по управлению воздушным движением Eurocontrol, подтвердило, что DDoS-атака KillNet затронула его веб-сайт, но не нарушила полеты и не создала какой-либо угрозы воздушному движению.

Эксперты предупреждают о возможности более серьёзных атак в будущем. Группировка продемонстрировала готовность атаковать критически важные объекты инфраструктуры и призвала другие группировки начать аналогичные атаки против гражданской инфраструктуры США, включая морские

терминалы, объекты логистики, центры мониторинга погоды и системы здравоохранения. Таким образом, хотя фактический ущерб, нанесённый авиационной отрасли атаками KillNet, пока был минимальным, существует потенциал для более значительных сбоев.

Авиакомпании, пострадавшие от атак KillNet, не раскрываются. Однако атаки были нацелены на веб-сайты нескольких крупных аэропортов США, что может косвенно повлиять на авиакомпании, работающие в этих аэропортах, нарушив взаимодействие клиентов с ними.

Проводимые группой распределённые атаки типа "Отказ в обслуживании" (DDoS) были нацелены на веб-сайты нескольких крупных аэропортов США, в результате чего они замедлили работу или стали полностью недоступны. Однако эти атаки не повлияли на важнейшие операции аэропорта и не нарушили полёты.


Воздействие на авиакомпании, работающие в этих аэропортах, в первую очередь будет проявляться в виде нарушения взаимодействия с клиентами. Например, пассажиры могли испытывать трудности с доступом к информации о рейсе, бронированием или сменой рейсов, а также с онлайн-регистрацией, пока веб-сайты аэропортов не работали. Однако фактический масштаб этого сбоя не обнародован публично.

### 4) *Другие отрасли*

Помимо секторов здравоохранения и энергетики, KillNet нацелился на множество других секторов и отраслей. К ним относятся:

- **Правительственные службы:** в прошлом году KillNet атаковал правительственные веб-сайты в нескольких странах, включая по меньшей мере три штата в США
- **Транспорт:** веб-сайты аэропортов США стали жертвами DDoS-атак KillNet
- **СМИ и новостные агентства:** деятельность KillNet также затронула медиакомпания
- **Рынки темной сети:** KillNet участвовал в атаках на рынки темной сети
- **Финансовый сектор:** Группа угрожает финансовому сектору, включая банковскую систему SWIFT и другие финансовые учреждения





**вн. ФИШИНГ В  
ВЕЛИКОБРИТАНИИ**



#### *А. Введение*

Фишинговые атаки в Великобритании находятся на подъёме, киберпреступники используют все более изощренные методы для обмана отдельных лиц и организаций с целью получения конфиденциальной информации. Национальный центр кибербезопасности (NCSC) и другие организации, активно работают над борьбой с этими угрозами, предоставляя отдельным лицам ресурсы для сообщений о подозрительных действиях и предлагая рекомендации о том, как не стать жертвой. По данным за 2023 год 74% нарушений связаны с человеческим фактором, который включает атаки социальной инженерии, ошибки или неправильное использование.

Новый вид мошенничества включают QR-фишинг, при котором преступники скрывают вредоносные ссылки в QR-кодах и размещают их в социальных сетях в рамках активностей для фанатов, поиска билетов и т.п..

Искусственный интеллект (ИИ) также используется киберпреступниками для усиления своих фишинговых атак. С его помощью создаются убедительные персонализированные фишинговые электронные письма, и дипфейки, используемых для имитации биометрической аутентификации с использованием лиц и голоса

#### *В. Борьба с фишингом в Великобритании*

Борьба с фишингом в Великобритании предполагает комплексный подход, который включает правительственные инициативы, сотрудничество с технологическими компаниями, действия правоохранительных органов, а также образовательные программы.

Правительство Великобритании предприняло несколько шагов по борьбе с фишингом и другими формами киберпреступности. Национальный центр

кибербезопасности (NCSC), организация правительства Великобритании, имеет полномочия расследовать и удалять мошеннические адреса электронной почты и веб-сайты. Правительство подписало соглашение с некоторыми крупнейшими технологическими компаниями, которая обязывает блокировать и удалять мошеннический контент со своих платформ. Также правительство запустило новую стратегию борьбы с мошенничеством, в которую входит Национальное подразделение по борьбе с мошенничеством, возглавляемое Национальным агентством по борьбе с преступностью и полицией Лондон-Сити. Национальное агентство по борьбе с преступностью (NCA) стремится повысить устойчивость Великобритании к кибератакам и улучшить реакцию правоохранительных органов на угрозу киберпреступности.

Повышение образования и осведомлённости рассматривается как ключ к предотвращению фишинговых атак. Различные организации предлагают учебные курсы по повышению осведомлённости о фишинге, которые обучают отдельных лиц и сотрудников тому, как распознавать такие атаки и предотвращать их. NCSC предоставляет рекомендации по защите от фишинговых атак, а также по выявлению мошеннических электронных писем, текстовых сообщений, веб-сайтов и звонков и сообщению о них.

Сотрудничество с международными партнёрами также имеет решающее значение в борьбе с фишингом, особенно учитывая, что многие киберугрозы исходят из-за рубежа. NCSC Великобритании объединила усилия с Агентством национальной безопасности (АНБ) США и другими международными партнёрами, чтобы публиковать обновления о текущих угрозах и предоставлять рекомендации по защите от них.

#### *С. Важность последствий фишинга*

Фишинг в Великобритании представляет собой значительную и растущую угрозу для частных лиц, предприятий и критически важной инфраструктуры страны. Фишинговые атаки, которые часто включают обман людей с целью получения конфиденциальной информации или установки вредоносного ПО, становятся все более изощренными и распространёнными. Национальный центр кибербезопасности (NCSC) предупредил о целенаправленных фишинговых кампаниях против организаций и частных лиц Великобритании, подчеркнув сохраняющуюся и значительную угрозу критически важной инфраструктуре страны.

Финансовые последствия фишинга существенны, компании сообщают о больших убытках (...лишь бы не платить). Например, в 2021 году фишинговые атаки привели к убыткам на общую сумму 44,2 миллиона долларов по всему миру, а средние затраты организации на восстановление после утечки данных в Великобритании превышают 3,4 миллиона фунтов стерлингов.

Фишинг также оказывает значительное влияние на общественность. Примерно девять из десяти пользователей Интернета в Великобритании сталкивались с контентом, который, как они подозревали, является мошенничеством.

Кроме того, фишинг подрывает безопасность информационных систем и может привести к утечке данных, краже личных данных и финансовому мошенничеству. Использование уязвимости «человека» делает его критически важным для стратегий кибербезопасности.

#### D. Недавние фишинговые атаки в Великобритании

Фишинговые атаки остаются серьёзной угрозой кибербезопасности в Великобритании, и различные недавние примеры демонстрируют разнообразие тактик, используемых киберпреступниками.

- **Вишинг-атаки:** В ноябре 2023 года международная операция сорвала фишинговую кампанию, в результате которой жертвы были обмануты на десятки миллионов евро. Преступники осуществляли вишинговые (голосовой фишинг) атаки из колл-центров Украины и Чехии, выдавая себя за банковских служащих с целью перевода (вымогательства) денег
- **Фишинговая кампания для сотрудников отелей:** В том же месяце фишинговые кампании были нацелены на сотрудников отелей. Злоумышленники отправляли электронные письма сотрудникам, обманом заставляя их переходить по ссылке, по которой загружалась вредоносная infostealer-программа. После заражения злоумышленники удаляли данные клиентов
- **Поддельные электронные письма USPS:** В мае 2023 года USPS и Служба почтовой инспекции сообщили о распространении поддельных электронных писем, якобы, от должностных лиц USPS. В этих электронных письмах получателям предлагалось подтвердить свои личные данные о доставке, нажав кнопку, которая при открытии могла активировать вирус и украсть информацию
- **Фишинговая атака транспортного бизнеса Великобритании:** В первом квартале 2021 года транспортное предприятие Великобритании подверглось кибератаке, в результате которой сотрудникам организации было отправлено электронное письмо с документом, содержащим ссылку на поддельный портал. Поддельный портал требовал от получателя входа в систему с использованием учётных данных для проверки подлинности Office 365 / G-Suite. Когда получатели входили в систему, их учётные данные и парольные фразы собирались и затем использовались для доступа к почтовым ящикам жертв
- **QR-фишинг:** В 2024 году появилась новая форма фишинга под названием "квишинг", при которой преступники скрывают вредоносные ссылки в QR-кодах чтобы украсть личную информацию или загрузить вредоносное ПО. Этот тип фишинга может проявляться в виде электронных писем, в которых утверждается, что посылка не была доставлена или что возникла проблема
- **Фишинговая атака на юридическую фирму:** Сотрудники юридической фирмы не смогли

распознать фишинговую атаку. Они получили электронное письмо, нажали на ссылку для загрузки документа, затем непреднамеренно ввели учётные данные для входа на то, что, по их мнению, было законным веб-сайтом, но привело к утечке данных.

#### E. Недавние фишинговые атаки, нацеленные бизнес в Великобритании.

Фишинговые атаки по-прежнему представляют серьёзную угрозу для бизнеса в Великобритании, и за последние годы произошло несколько заметных инцидентов.

- **Кибератака на библиотеку (январь 2024 г.):** британская библиотека подверглась кибератаке, в результате которой её ИТ-системы вышли из строя. Группа вымогателей Rhysida взяла на себя ответственность за атаку и слила внутренние данные о персонале, включая сканы паспортов сотрудников и трудовых договоров, в даркнет
- **Мошенничество с предложениями работы в WhatsApp (ноябрь 2023 г.):** Тысячи соискателей стали мишенью мошенников в WhatsApp, которые использовали поддельные предложения о работе, чтобы заманить жертв в свою схему
- **Фишинговые атаки на малый бизнес (2023):** Исследование показало, что мошенничество и фишинг составляли 82% онлайн-угроз для малого бизнеса в Великобритании в 2023 году. Только в первой половине 2023 года число фишинговых атак по электронной почте выросло на 464% по сравнению с 2022 годом
- **Фишинговые атаки на организации Великобритании (2022–2023 гг.):** 83% британских предприятий и благотворительных организаций, подвергшихся кибератаке идентифицировали фишинг как тип атаки

#### F. Недавние фишинговые атаки, нацеленные на частных лиц из Великобритании

Фишинговые атаки остаются серьёзной угрозой кибербезопасности в Великобритании, а различные недавние инциденты подчёркивают эволюцию тактики киберпреступников.

- **Фишинговая атака на Booking.com:** В ноябре 2023 года фишинговая атака была нацелена на Booking.com. Преступники осуществляли вишинговые (голосовой фишинг) атаки из колл-центров в Украине, выдавая себя за банковских служащих, чтобы оказать давление на жертв с целью перевода денег
- **Фишинговые атаки на парламентариев Великобритании:** В декабре 2023 года были совершены фишинговые атаки, направленные против парламентариев Великобритании из нескольких политических партий
- **Фишинговые атаки с мимикрией под правительственные электронные письма:** В 2022 году Национальный центр кибербезопасности (NCSC) сообщил о мошенничестве – фишинговые

атаки проводились с применением поддельных писем, выглядящих как настоящие правительственные электронные письма

#### G. Фишинговые мошенничества, нацеленные на сотрудников

Фишинговые мошенничества, нацеленные на сотрудников, также известные как мошенничество с компрометацией деловой электронной почты (BEC), часто нацелены на руководителей или специалистов по персоналу, то есть должности, которые имеют доступ к конфиденциальной информации. Эти атаки обычно связаны с отправкой электронных писем, которые, как представляется, от старшего руководителя или CEO, с запросом банковского перевода или информации о заработной плате. К числу распространённых фишинговых мошенничеств, нацеленных на сотрудников, относятся:

- **Атаки на топ-представителей:** это целенаправленные попытки украсть конфиденциальную информацию у компании путём выдвигая себя за топ-менеджеров, таких как генеральные директора или CFO
- **Фишинговые атаки с формой W-2:** в этом случае злоумышленник выдаёт себя за руководителя организации и отправляет сообщение сотруднику отдела заработной платы или отдела кадров с запросом W-2 информации
- **Фишинг новых сотрудников:** Новые сотрудники часто становятся мишенью, потому что они стремятся произвести впечатление и могут не замечать признаков фишинговой атаки

#### H. Фишинговые мошенничества, нацеленные на потребителей (обычных пользователей)

Фишинговые мошенники, нацеленные на потребителей, часто выдают себя за хорошо известные компании или организации, такие как банки или правительственные учреждения, чтобы завоевать доверие целевых лиц. Эти мошенничества обычно включают отправку электронных писем или текстовых сообщений, которые, как представляется, исходят от этих организаций, с просьбой предоставить потребителям личную идентификационную информацию. Затем мошенники используют эту информацию для открытия новых учётных записей на имя потребителя или вторжения в его существующие учётные записи. Некоторые распространённые фишинговые программы, ориентированные на потребителей, включают:

- **Мошенничество с обналичиванием чеков:** Мошенники нацелены на людей, продающих товары онлайн. Они переплачивают сумму с использованием расчёта чеком и просят перевести излишек обратно только для того, чтобы вернуть первоначальную сумму
- **Мошенничество с продажами:** Онлайн-покупатели, ищущие выгодную сделку, становятся мишенью для сайтов аукционов электроники высокого класса. Даже если потребитель не выиграет товар, ему все равно придётся заплатить

- **Мошенничество с трудоустройством:** Предполагаемый работодатель проводит собеседование по телефону и сообщает соискателю, что он получил работу. Затем соискателя работы просят заполнить онлайн-кредитную форму, которая используется для кражи его личности

#### I. Упреждающие стратегии

Фишинг является серьёзной угрозой кибербезопасности, и раннее обнаружение имеет решающее значение для предотвращения того, чтобы жертвы не стали жертвами этих атак.

- **Обнаружение фишинга на раннем этапе:** Раннее обнаружение фишинговых атак важно, так как 50% жертв становятся таковыми в течение 24 часов. Использование технологий и автоматизации может помочь выявлять фишинговые страницы раньше.
- **Использование DMARC:** DMARC – это глобальный стандарт аутентификации электронной почты, который помогает проверять происхождение электронных писем и блокировать поддельные из них. Это позволяет отправителям убедиться, что электронное письмо действительно исходит от того, от кого оно, по их утверждению, оно должно исходить
- **Мониторинг регистраций доменов:** Мониторинг регистраций доменов может помочь обнаружить мошеннические веб-сайты, созданные для кражи учётных данных, перенаправления веб-трафика или продажи контрафактной продукции. Такие сервисы, как PhishLabs и Red Points, предлагают услуги мониторинга доменов, которые могут автоматизировать процесс поиска и удаления поддельных учётных записей, приложений, веб-сайтов и доменов
- **Автоматизация обнаружения фишинга:** Машинное обучение может помочь обнаружить фишинговые атаки путём изучения шаблонов и создания моделей, которые могут автоматически отличать законные веб-сайты от вредоносных или другие формы коммуникации. Существуют также различные антифишинговые инструменты и сервисы, которые могут помочь компаниям защититься от атак
- **Сотрудничество между командами:** Сотрудничество между командами имеет важное значение для борьбы с фишингом. Регулярные тренинги по повышению осведомлённости персонала могут гарантировать, что сотрудники будут знать, как распознать фишинговое электронное письмо, даже по мере того, как методы мошенников становятся все более продвинутыми

##### 1) Обнаружение фишинга на раннем этапе

Раннее обнаружение фишинга имеет решающее значение, поскольку жертвы наиболее уязвимы в первые 24 часа и для этого организации могут использовать различные технологии:

- **Автоматическое сканирование:** Использование инструменты автоматического сканирования для регулярного поиска фишинговых веб-сайтов и электронных писем. Эти инструменты могут сканировать и анализировать веб-страницы, электронные письма и другой цифровой контент на предмет признаков фишинга.
- **Машинное обучение:** Внедрение алгоритмов машинного обучения, которые могут извлекать уроки из моделей известных фишинговых атак и прогнозировать новые. Эти алгоритмы могут обрабатывать большие объёмы данных для выявления потенциальных угроз быстрее, чем люди.
- **Сообщения о пользователях:** поощрение пользователей сообщать о предполагаемых попытках фишинга. Быстрое создание отчётов может привести к более быстрому удалению фишинговых сайтов и предотвратить дальнейший ущерб.

### 2) Использование DMARC

DMARC используется как система проверки подлинности электронной почты, разработанная для защиты доменных имён от использования в фишинговых мошенничествах, подделке электронной почты и других киберпреступлениях:

- **Аутентификация электронной почты:** DMARC работает, гарантируя, что законная электронная почта должным образом аутентифицируется в соответствии с установленными стандартами DKIM (почта, идентифицируемая ключами домена) и SPF (структура политики отправителя).
- **Отчётность:** DMARC также предоставляет получателям электронной почты возможность сообщать отправителям о сообщениях, которые прошли или не прошли проверку.
- **Применение политики:** отправители могут устанавливать политики для того, как получатели должны обрабатывать почту, которая не проходит проверки подлинности, что потенциально предотвращает доставку мошеннических писем.

### 3) Мониторинг регистраций доменов

Мониторинг регистраций доменов может помочь выявить потенциальные фишинговые сайты до того, как они станут активными:

- **Службы наблюдения за доменами:** использование службы, которые отслеживают регистрацию доменных имён, похожих на бренд или товарные знаки.
- **Автоматические оповещения:** настройка автоматические оповещения для уведомления вашей службы безопасности о регистрации потенциально мошеннического домена.
- **Службы удаления:** использование служб, которые могут помочь удалить фишинговые сайты после их выявления.

### 4) Автоматизировать обнаружение фишинга

Автоматизация обнаружения фишинга предполагает использование программного обеспечения для выявления фишинговых угроз и реагирования на них:

- **Фишинговые базы данных:** использование базы данных известных фишинговых сайтов для блокирования доступа к ним.
- **Анализ в режиме реального времени:** внедрение системы, которые выполняют анализ веб-страниц и электронных писем в режиме реального времени для обнаружения фишингового контента.
- **Интеграция:** интеграция обнаружения фишинга в инфраструктуру безопасности, такую как брандмауэры, шлюзы электронной почты и endpoint решения, для комплексной защиты.

### 5) Совместная работа в разных командах

Сотрудничество является ключом к успешной стратегии борьбы с фишингом:

- **Межведомственное обучение:** проведение регулярных тренингов во всех подразделениях для ознакомления сотрудников с новейшими тактиками фишинга и способами их распознавания.
- **Обмен данными:** обмен данными о новых фишинговых угрозах между группами безопасности, ИТ-отделами и другими заинтересованными сторонами.
- **Планирование реагирования на инциденты:** разработка и применение на практике плана реагирования на инциденты с участием нескольких команд для обеспечения скоординированного реагирования на фишинговые атаки.

### 1. Программное обеспечение для обнаружения фишинга и реагирования на него

Программное обеспечение для обнаружения фишинга и реагирования на него представляет собой набор инструментов кибербезопасности, которые позволяют организациям выявлять фишинговые угрозы и устранять их. Несколько инструментов, которые можно использовать для автоматизации обнаружения фишинга:

- **Agari:** Этот сервис представляет собой систему реагирования на фишинговые инциденты, разработанную для ускорения сортировки фишинговых сообщений, судебной экспертизы, исправления и локализации взломов
- **IRONSCALES:** Эта самообучающаяся платформа безопасности электронной почты предназначена для активной борьбы с фишингом. Она сочетает в себе взаимодействие с человеком и идентификацию, ориентированную на искусственный интеллект, для предотвращения попыток фишинга, включая компрометацию деловой электронной почты (BEC)
- **Avanan:** Это антифишинговое программное обеспечение для электронной почты, размещённое в облаке, подключается к вашему почтовому провайдеру с помощью API для обучения его

искусственного интеллекта на основе данных электронной почты. Служба анализирует не только содержимое сообщений, форматирование и информацию в заголовке, но и оценивает существующие отношения между отправителями и получателями, чтобы установить уровень доверия

- **Barracuda Sentinel:** Этот инструмент использует API почтового провайдера для защиты от фишинга, а также искусственный интеллект для изучения уникальных коммуникационных моделей вашей организации, чтобы выявлять и блокировать фишинг атаки и кибермошенничество в режиме реального времени
- **Proofpoint Targeted Attack Protection (TAP):** Этот инструмент помогает организациям эффективно обнаруживать, смягчать и блокировать продвинутые целевые атаки, которые поступают по электронной почте
- **RSA FraudAction:** Этот инструмент специализируется на обнаружении и предотвращении попыток фишинга, троянов и мошеннических веб-сайтов
- **PhishER:** Эта облегчённая платформа управления безопасностью, автоматизации и реагирования (SOAR) помогает организовывать реагирование на угрозы и управлять большим объёмом фишинговых угроз
- **Zphisher:** Это инструмент для начинающих, который включает в себя несколько автоматических тестов на фишинг
- **Evilginx2:** Этот фишинговый инструмент описывает себя как платформу для атак типа "человек посередине", используемую для фишинга учётных данных для входа в систему вместе с сессионными файлами cookie, позволяющими обойти двухфакторную аутентификацию
- **DTonomy AIR Enterprise:** Этот инструмент на основе искусственного интеллекта включает в себя анализ фишинговых электронных писем в пакетном режиме, автоматизацию управления задачами и обращениями, а также сотни сборников игр

#### 1) Основные функции программного обеспечения для обнаружения фишинга и реагирования на него

При выборе программного обеспечения для обнаружения фишинга и реагирования на него необходимо учитывать следующие ключевые особенности:

- **Идентификация домена:** возможность идентифицировать и проверять подлинность домена, с которого отправляется электронное письмо, помогая предотвратить подмену домена
- **Анализ Analysis:** анализ заголовков электронных писем на предмет несоответствий или признаков подделки, которые могут указывать на попытку фишинга
- **Анализ ссылок:** проверка ссылок в электронных письмах или веб-контенте, чтобы определить, ведут

ли они на известные фишинговые сайты или вредоносный контент

- **Анализ атак имперсонации:** обнаружение попытки выдать себя за законного юридического или физического лица. Это является типичным приёмом фишинг-атак
- **Аналитика искусственного интеллекта:** использование искусственного интеллекта для упреждающего выявления подозрительных моделей поведения и прогнозирования новых фишинговых угроз
- **Анализ с БД известных ссылок:** сравнение с базами данных известных угроз, которые часто обновляются вручную экспертами по безопасности, для выявления попыток фишинга
- **Отчётность для конечных пользователей:** позволяет пользователям сообщать о предполагаемых попытках фишинга, что может привести к более быстрому удалению сайтов мошенников и предотвращению дальнейшего ущерба

#### 2) Как работают инструменты моделирования и тестирования фишинга

Инструменты моделирования и тестирования фишинга предназначены для того, чтобы предоставить пользователям реальный опыт борьбы с фишинговыми атаками:

- **Реалистичные симуляции:** распространение ряда реалистичных сценариев фишинга, имитирующих новейшие методы атак, включая вишинг (голосовой фишинг), для обучения пользователей
- **Регулярно обновляемые шаблоны:** использование шаблонов, которые часто обновляются, чтобы отражать новейшие тактики фишинга, гарантирует, что обучение остаётся актуальным
- **Частота автоматического тестирования:** автоматизирование частоты тестов на имитацию фишинга обеспечивает последовательное обучение, а не спорадические, разовые сеансы
- **Тестирование в активной среде:** увидев фишинговое электронное письмо в активной среде, пользователи должны применить свои знания, чтобы не стать жертвой, усилив своё обучение
- **Идеи администратора:** с точки зрения администратора, внедрение симуляций и тренингов даёт представление об эффективности тренинга и состоянии безопасности организации

#### 3) Внедрение программного обеспечения для обнаружения фишинга и реагирования на него

Эффективное внедрение программного обеспечения для обнаружения фишинга и реагирования на него требует сочетания технических решений, обучения пользователей и организационной политики. Связанные рекомендации:

- **Регулярное обучение сотрудников навыкам кибербезопасности:** Непрерывное обучение

гарантирует, что сотрудники смогут распознавать попытки фишинга и реагировать на них.

- **Внедрение передовые методы обеспечения безопасности электронной почты:** использование протоколов, такие как DMARC, для проверки подлинности электронных писем и предотвращения подмены. Этот протокол основан на стандартах SPF и DKIM для проверки происхождения электронных писем и блокирования поддельных писем
- **Использование искусственный интеллект и автоматизацию:** ПО на базе ИИ может с высокой точностью сканировать входящие сообщения на наличие признаков фишинга. Алгоритмы машинного обучения также могут предсказывать новые фишинговые угрозы, изучая шаблоны известных атак
- **Отслеживание результатов фишинга:** использование инструментов моделирования фишинга для отслеживания реакции сотрудников на имитируемые атаки. Это может помочь выявить уязвимости и измерить эффективность обучающих программ
- **Фильтрация DNS-трафик:** Решения для фильтрации DNS могут предотвращать доступ пользователей к вредоносным веб-сайтам, блокируя запросы к доменам, внесённым в черный список. Некоторые фильтры могут предварительно проверять веб-сайты на наличие вредоносного кода и добавлять их в черный список
- **Использование технические решения:** применение надёжные пароли, DNS-фильтрацию, антивирусных решений, политик безопасного просмотра веб-страниц и использование службы безопасной электронной почты для предотвращения фишинговых компрометаций
- **Внедрение мер реагирования на инциденты и отчётности:** разработка плана реагирования на выявленную фишинговую активность. Это включает в себя шаги по исправлению положения и механизмы отчётности для устранения и смягчения последствий успешных атак
- **Использование шлюза безопасной электронной почты:** Развёртывание фильтров электронной почты, которые проверяют заголовки и вредоносный контент, классифицируют электронную почту и проверяют URL-адреса на соответствие репутации каналов
- **Защита пользовательских конечных точек:** Обеспечение безопасности пользовательских конечных точек путём внедрения средств защиты этих точек и обучения пользователей методам безопасного просмотра веб-страниц и электронной почты.

#### 4) Ошибки реализации

При внедрении программного обеспечения для обнаружения фишинга и реагирования на него следует избегать нескольких распространённых ошибок:

- **Нерегулярное обновление программного обеспечения:** Регулярные обновления нужны, чтобы программное обеспечение могло эффективно обнаруживать новейшие фишинговые угрозы и реагировать на них
- **Чрезмерная зависимость от ИТ-отделов:** Хотя ИТ-отделы играют решающую роль в управлении и обслуживании программного обеспечения для обнаружения фишинга, важно, чтобы все сотрудники понимали, как выявлять попытки фишинга и реагировать на них
- **Вера в антивирусное программное обеспечение:** хотя антивирусное программное обеспечение может помочь обнаружить и предотвратить некоторые попытки фишинга, само по себе этого недостаточно. Решения для обнаружения и реагирования на конечные точки (EDR) и расширенного обнаружения и реагирования (XDR) могут обеспечить более комплексную защиту
- **Отсутствие продуманного моделирования фишинга:** Моделирование фишинга может быть полезным инструментом для обучения сотрудников распознавать попытки фишинга и реагировать на них. Однако важно проводить эти симуляции вдумчиво и чётко взаимодействовать со всеми соответствующими заинтересованными сторонами
- **Отсутствие продуманной стратегии защиты:** полагаться исключительно на антифишинговую программу может быть рискованно, поскольку злоумышленнику достаточно одной ошибки, чтобы добиться успеха. Стратегия комплексной защиты, включающая несколько уровней безопасности, обеспечит более надёжную защиту

При выборе программного обеспечения для обнаружения фишинга и реагирования стоит опираться на следующие критерии:

- **Интеграция с другими инструментами:** Программное обеспечение должно быть способно интегрироваться с другими средствами обеспечения безопасности для комплексного подхода к безопасности
- **Возможности машинного обучения:** Многие современные инструменты используют машинное обучение для анализа действий конечных точек и сети и обнаружения потенциальных угроз
- **Определение приоритетности угроз:** ПО должно иметь возможность определять приоритетность предупреждений об угрозах, чтобы помочь вашей команде сосредоточиться на наиболее серьёзных угрозах в первую очередь
- **Агентный мониторинг против безагентного:** как агентный, так и безагентный мониторинг имеют свои плюсы и минусы, и может потребоваться их сочетание для оптимальной безопасности
- **Возможности мониторинга и анализа:** ПО должно быть способно отслеживать поведение

конечной точки и обнаруживать, расставлять приоритеты, и оповещать о признаках компрометации (IoC) и признаках атаки (IOA)

- **Обнаружение против предотвращения:** Некоторые решения больше ориентированы на обнаружение попыток фишинга, в то время как другие – на предотвращение них
- **Автоматическое обнаружение угроз в режиме реального времени:** Эта функция может помочь вашей службе безопасности быстро выявлять угрозы и реагировать на них

#### К. Риски фишинга в праздничные дни

##### 1) Почему мошенники любят праздники

Мошенники любят сезон отпусков по нескольким причинам:

- **Повышенная онлайн-активность:** во время праздников люди более активны в Интернете, совершают покупки подарков, бронируют поездки и делают пожертвования благотворительным организациям. Эта возросшая активность предоставляет мошенникам больше возможностей обманом заставить людей раскрыть конфиденциальную информацию
- **Отвлекающий фактор:** Сезон отпусков – напряженное время, люди часто отвлекаются и могут быть не такими бдительными, как обычно. Мошенники пользуются этим, отправляя фишинговые электронные письма, которые, как представляется, исходят из авторитетных источников, таких как банки или популярные розничные продавцы
- **Эмоциональная манипуляция:** Мошенники часто используют эмоциональную манипуляцию во время сезона отпусков. Они могут выдавать себя за благотворительные организации или членов семьи, чтобы обманом вынудить людей отправлять деньги или раскрывать личную информацию
- **Сезонные темы:** Мошенники используют электронные письма, сообщения и веб-сайты праздничной тематики, чтобы обмануть жертв. Они могут отправлять поддельные электронные письма с заказами и отслеживанием, благотворительные электронные письма и сообщения, связанные с праздничными мероприятиями или расписаниями
- **Оппортунистическое поведение:** мошенники пользуются тем фактом, что многие компании предлагают бонусы или сезонные рабочие места во время праздников. Они создают фишинговые кампании, нацеленные на сотрудников с помощью поддельных предложений бонусов или на соискателей с помощью мошеннических объявлений о работе
- **Социальная инженерия:** мошенники используют тактику социальной инженерии, чтобы создать ощущение срочности или страха, например, заявляя, что посылка была пропущена или что учётная запись получателя была взломана. Это может

побудить к поспешным действиям, таким как переход по вредоносным ссылкам

- **Поддельные интернет-магазины или “Магазины-двойники”:** мошенники создают мошеннические веб-сайты, имитирующие деятельность законных интернет-магазинов, чтобы обманом заставить потребителей вводить свою личную и финансовую информацию
- **Уведомление о пропущенной доставке / недоставке:** жертвы получают уведомления о том, что доставка была пропущена или посылка не была доставлена, с предложением перейти по ссылке, которая может привести на фишинговый сайт или установить вредоносное ПО
- **Мошенничество с подарочными картами:** мошенники рассылают поддельные электронные письма или текстовые сообщения с просьбой к жертвам приобрести несколько подарочных карт по личным или деловым причинам, часто выдавая себя за кого-то, кого знает жертва
- **Фальшивые благотворительные организации:** преступники создают фиктивные благотворительные организации и запрашивают пожертвования у людей, которые считают, что они вносят свой вклад в законное дело
- **Мошенничество в социальных сетях:** мошенники используют платформы социальных сетей для предложения праздничных акций, ваучеров или подарочных карт, требующих заполнения опросов, направленных на кражу личной информации
- **Мошеннические сезонные вакансии:** в Интернете размещаются поддельные объявления о вакансиях, предлагающие хорошие деньги за очень небольшую работу, ориентированные на людей, стремящихся подзаработать во время праздников
- **Фишинговые электронные письма:** они особенно распространены в сезон отпусков и могут принимать форму поддельных запросов на подтверждение доставки или других сообщений с целью получения личной информации
- **Кража данных:** Мошенники могут выдавать себя за службы доставки и отправлять мошеннические уведомления о краже посылки или проблемах с доставкой, чтобы обманом вынудить получателей предоставить личные данные
- **Мошенничество с отпуском:** предложения поддельных отпускных или туристических сделок, цель которых - украсть деньги или личную информацию у ничего не подозревающих жертв
- **Борьба с мошенничеством:** частным лицам отправляются нежелательные сообщения, которые могут показаться безобидными, но могут быть признаком того, что мошенник имеет доступ к личной информации получателя





viii. **DCRAT (DARK  
CRYSTAL RAT)**



#### A. Введение

DCRat (Dark Crystal Rat) является бэкдором коммерческого типа, который продаётся преимущественно на подпольных форумах. Он существует с 2018 года и работает как модульный троянец удалённого доступа (RAT), предлагаемый как вредоносное ПО как услуга (MaaS). Вредоносная программа предназначена для предоставления несанкционированного доступа к системам в обход мер безопасности.

Что касается цен, DCRat продаётся примерно за 7 долларов за двухмесячную подписку. Лицензия на один месяц стоит всего 5 долларов, в то время как пожизненное использование лицензии стоит 40 долларов.

В 2022 году разработчик из DCRat объявил на своей странице в GitHub, что выпуск будет прекращён, а также дал ссылку на его преемника и заявил, что новый исходный код останется закрытым и не будет продаваться.

#### B. Функциональные возможности DCRat

DCRat – модульный вредоносный код с функцией удалённого доступа (RAT) с рядом функций, которые делают его универсальным инструментом.

Сам продукт DCRat состоит из трех компонентов: исполняемого файла stealer / client, отдельной PHP-страницы, служащей конечной точкой / интерфейсом C2, и инструмента администратора. Он использует модульную структуру, которая развёртывает отдельные исполняемые файлы для каждого модуля, большинство из которых представляют собой скомпилированные двоичные файлы .net, запрограммированные на C #.

DCRat может использоваться весьма широко, включая мониторинг, разведку, кражу информации, проведение распределённых атак типа "Отказ в обслуживании" (DDoS) и выполнение кода. Он также позволяет выполнять кражу

учётные данные, используемые для входа в учётные записи социальных сетей, в частности Telegram и Discord.

По состоянию на 2023 год DCRat был дополнен несколькими новыми возможностями:

- **Модуль CryptoStealer:** модуль позволяет получить доступ к крипто-кошелькам пользователей
- **Динамическое выполнение кода:** DCRat может выполнять код на нескольких языках программирования
- **Крипто-майнинг:** были задокументированы случаи, когда DCRat развёртывал программное обеспечение для крипто-майнинга на подконтрольных устройствах
- **Способы доставки:** DCRat распространяется с помощью заманчивых приманок на тему контента для взрослых, заражённых файлов и в т.ч. путём распространения по сети
- **Методы предотвращения обнаружения:** DCRat избегает изолированных сред, которые имитируют интернет-соединения для анализа вредоносных программ
- **Закрепление:** DCRat использует уязвимость нулевого дня в диагностическом средстве поддержки Microsoft (MSDT), CVE-2022-30190 (Follina), для закрепления на заражённом компьютере

По состоянию на 2023 год DCRat имеет следующие ключевые функции (**полный список**):

- Кража информации
- Мониторинг и контроль
- Деструктивные атаки
- Модульность и индивидуальная настройка
- Взаимодействие с системой
- Администрирование и контроль
- Развёртывание и распространение
- Скрытность и предотвращение обнаружения

#### 1) Кража информации

- **Кража данных:** DCRat может красть конфиденциальные данные из систем-жертв, включая создание скриншотов, сбор данных из буфера обмена
- **Кейлоггинг:** он может регистрировать нажатия клавиш для сбора конфиденциальной информации, такой как пароли
- **Кража данных браузера:** DCRat может извлекать файлы cookie сеанса, учётные данные для автоматического заполнения, личную информацию и данные кредитной карты из браузеров

- **Сбор данных из буфера обмена:** может копировать и красть содержимое буфера обмена пользователя
  - **Кража учётных данных:** может красть учётные данные из популярных FTP-приложений и учётных записей в социальных сетях, особенно для Telegram и Discord
- 2) *Мониторинг и контроль*
- **Скриншоты:** может делать скриншоты для мониторинга активности пользователя
  - **Сбор системной информации:** DCRat собирает системную информацию, такую как статистика процессора и графических процессоров, имя хоста, имена пользователей, языковые настройки и установленные приложения
- 3) *Возможности деструктивных атак*
- **DDoS-атаки:** DCRat может запускать DDoS-атаки в отношении выбранных целей
  - **Динамическое выполнение кода:** предоставляет возможность динамического выполнения кода на нескольких языках программирования
- 4) *Модульность и индивидуальная настройка*
- **Модульная архитектура:** DCRat использует модульную структуру, развёртывая отдельные исполняемые файлы для каждого модуля, большинство из которых представляют собой скомпилированные двоичные файлы .NET, запрограммированные на C #
  - **Платформа для плагинов:** у него есть платформа для разработки плагинов, которая позволяет создавать новые модули, расширяя его возможности
- 5) *Системное взаимодействие*
- **Закрепление:** DCRat может закрепляться на скомпрометированных хостах с использованием таких методов, как создание запланированных задач, ключей запуска реестра и ключей автозапуска Winlogon Registry Keys
  - **Крипто-майнинг:** были случаи, когда DCRat развёртывал программное обеспечение для крипто-майнинга на конечных точках жертв
- 6) *Администрирование и контроль*
- **Администрирование C2:** вредоносная программа включает интерфейс администрирования командования и контроля (C2), который позволяет злоумышленникам загружать модули, выполнять команды удалённо и извлекать данные
  - **Исполняемый файл Stealer / Client:** Он состоит из исполняемого файла .NET, предназначенного для использования систем Windows
- 7) *Развёртывание и распространение*
- **Вредоносное ПО как услуга (MaaS):** DCRat работает как MaaS, позволяя приобретать его и использовать различным потребителям
  - **Недорогие лицензии:** двухмесячная подписка стоит примерно 7 долларов, для более длительного использования доступны другие варианты ценообразования
- 8) *Скрытность и предотвращения обнаружения*
- **Маскировка:** DCRat использует методы, сокрытия своего присутствия и маскировку сетевого трафика
  - **Функции защиты от обнаружения:** плагины могут препятствовать запуску на виртуальной машине, отключать защитника Windows и подсветку веб-камер на определённых моделях
  - **Механизмы закрепления:** Он может использовать такие методы, как создание запланированных задач, ключи запуска реестра и Winlogon автозапуск разделов реестра, чтобы закрепиться в системе
- 9) *Развёртывание DCRat*
- DCRat работает как вредоносное ПО как услуга (MaaS). DCRat развёртывается с помощью атак, использующих широкий спектр тактик, включая вредоносный спам, фишинг и пиратское (или “взломанное”) коммерческое программное обеспечение (мошеннические программы обновления и антивирусные продукты).
- После установки администрация DCRat C2 позволяет злоумышленникам загружать модули на заражённый хост, удалённо выполнять команды и извлекать данные. DCRat использует модульную платформу, которая развёртывает отдельные исполняемые файлы для каждого модуля, большинство из которых представляют собой скомпилированные двоичные файлы .net, запрограммированные на C#. Вредоносная программа способна красть информацию из браузеров, такую как сеансовые файлы cookie, учётные данные для автоматического заполнения, личную информацию и данные кредитной карты. Он также может отслеживать заражённый хост, регистрируя и эксфильтрируя нажатия клавиш и снимки экрана.
- DCRat устанавливает соединение между устройством жертвы и устройством злоумышленника через командно-контрольный сервер (C2). Как только вредоносная программа устанавливается на устройство жертвы, она снова подключается к серверу C2, контролируемому злоумышленником. Этот сервер может отправлять команды на скомпрометированное устройство, позволяя злоумышленнику получать доступ к данным и изменять их, красть конфиденциальную информацию и обеспечивать закрепление путём повторного подключения к серверу C2 даже после перезагрузки или попыток удалить вредоносное ПО.

Наиболее распространённые «приманки» DCRat:

- **Контент для взрослых в т.ч. поддельный:** DCRat распространяется с использованием приманок, явно относящихся к страницам OnlyFans и другому контенту для взрослых. Жертв обманом заставляют загружать вредоносные файлы, часто ZIP-архивы, которые содержат вредоносное ПО

- **Фишинг и вредоносный спам:** DCRat также распространяется через фишинговые электронные письма и кампании вредоносного ПО, когда жертвы получают электронные письма с вредоносными вложениями или ссылками, которые при открытии устанавливают вредоносное ПО
- **Распространение по сети:** вредоносное ПО может распространяться по сети, используя уязвимости или другие методы для заражения нескольких устройств

#### 10) Предотвращение обнаружения

Злоумышленники, использующие DCRat, используют несколько методов, чтобы избежать обнаружения:

- **Проникновение в процесс:** DCRat редко приводит к вредоносной активности в текущем процессе. Вместо этого он предпочитает создавать большие деревья процессов и внедрять безвредный процесс в какой-то момент
- **Закрепление в системе:** DCRat способствует закреплению в системе через копирования себя в случайно запущенный процесс и в корневой каталог. Он также может создавать ярлыки для этих копий в папке автозагрузки и реестре пользователя
- **Задержка выполнения:** DCRat может задерживать выполнение на некоторое время после заражения, чтобы избежать немедленного обнаружения
- **Обфускация:** полезная нагрузка DCRat была защищена с помощью Enigma Protector, чтобы усложнить анализ кода
- **Использование сертификатов SSL / TLS:** DCRat, как и многие другие семейства вредоносных программ, использует самоподписанные сертификаты SSL / TLS, которые могут помочь ему «сливаться с обычным зашифрованным трафиком»

#### 11) Относительная эффективность

DCRat известен своей экономичностью, универсальностью и регулярными обновлениями, что делает его серьёзной угрозой. DCRat позволяет получить контроль над заражённым компьютером и украсть конфиденциальную информацию, такую как содержимое буфера обмена и личные учётные данные, из приложений. DCRat разрабатывается и поддерживается одним пользователем, который активно продвигает свой продукт на нескольких подпольных форумах, а также на канале Telegram. Это не похоже на большинство других RATs, которые обычно являются работой сложных и хорошо обеспеченных киберпреступных групп.

DCRat отличается от других RAT решений и способен функционировать как загрузчик, удаляя другие типы вредоносных программ на заражённый компьютер. DCRat использует три различных метода сохранения данных на скомпрометированном хосте: создание запланированной задачи, создание раздела запуска реестра и создание раздела реестра автозапуска. Он также использует команду W32tm

“stripchart” в качестве тактики задержки для её выполнения и управления событиями, что не характерно для других RATs.

С точки зрения эффективности, DCRat удивительно эффективен, несмотря на свою низкую стоимость. Вредоносная программа находится в активной разработке, новые возможности добавляются регулярно. Он также способен предотвращать обнаружение программным обеспечением безопасности, что делает его мощной угрозой кибербезопасности.

Наиболее распространённые функции других троянов удалённого доступа включают способность устанавливать полный или частичный контроль над заражёнными компьютерами, возможность запускать дочерний процесс и использование планировщика задач для обеспечения закрепления в скомпрометированной системе. Они также могут передавать конфиденциальную информацию, устанавливая соединения с серверами командования и управления (C2). Некоторые RAT-решения, такие как nJ RAT на базе .NET framework и позволяют хакерам удалённо управлять устройством жертвы, предоставляя им доступ к веб-камере, нажатиям клавиш и паролям, хранящимся в веб-браузерах и настольных приложениях.

#### 12) Обнаружение DCRat

##### a) Общие характеристики IoC

Наиболее распространённые индикаторы компрометации (IoC) для DCRat attacks связаны со следующими характеристиками:

- Мониторинг заражённого хоста путём протоколирования и эксфильтрации нажатий клавиш и скриншотов, которые можно использовать для отслеживания их активности
- Кража информации из браузеров, например сеансовые файлы cookie, учётные данные для автозаполнения, личная информация и данные кредитной карты, и популярных FTP-приложений
- Возможность записывать нажатия клавиш жертвой, которые могут быть использованы для кражи паролей и другой конфиденциальной информации
- Возможность сбора информации о системе (статистика процессора и графических процессоров и т.д.)

##### b) Особенности IoC

Наиболее распространённые IoC для DCRat связаны с:

- **Сетевой трафик:** DCRat взаимодействует со своим сервером управления (C2) для фильтрации данных и приёма команд. Это сообщение может быть обнаружено как необычный сетевой трафик
- **Сбор данных:** DCRat собирает конфиденциальную информацию со скомпрометированных хостов, такую как тип сервера, имя пользователя и сведения о графическом процессоре, которые могут быть обнаружены путём мониторинга необычного доступа к данным или перемещения

- **Механизмы закрепления:** DCRat использует несколько методов закрепления, включая создание запланированной задачи, создание раздела запуска реестра и создание раздела реестра автозапуска. Эти записи могут быть обнаружены путём мониторинга изменений в запланированных задачах, реестре и процессах запуска
- **DDoS-атаки:** DCRat может организовывать DDoS-атаки против целевых веб-сайтов. Это может быть обнаружено путём мониторинга необычных схем сетевого трафика или увеличения запросов к определённому веб-сайту
- **Динамическое выполнение кода:** DCRat имеет возможность выполнять код на нескольких языках программирования. Это может быть обнаружено путём мониторинга необычного выполнения кода или поведения процесса
- **Кража информации:** DCRat может облегчить кражу конфиденциальных данных с устройств жертв, включая создание скриншотов и сбор учётных данных. Это может быть обнаружено путём мониторинга необычного доступа к данным
- **Крипто-майнинг:** были задокументированы случаи, когда DCRat развёртывал программное обеспечение для крипто-майнинга на конечных точках жертв. Это можно обнаружить путём мониторинга необычной загрузки процессора или сетевого трафика

*c) Имена файлов и процессов, связанных с атаками DCRat*

Полезная нагрузка DCRat часто защищена с помощью Enigma Protector, чтобы скрыть её содержимое и предотвратить анализ. Вредоносная программа состоит из

нескольких компонентов, каждый из которых отвечает за определённый тип вредоносной активности. Авторы DCRat опубликовали специальное программное обеспечение под названием DCRat Studio, которое служит инструментом для разработки новых модулей для вредоносного ПО.

В некоторых наблюдаемых атаках было замечено, что вредоносная программа создаёт экземпляр процесса svchost.exe и внедряет код, используя методы удаления содержимого из процесса. Другие имена файлов, ассоциированные с атаками DCRat, включают 8c8bc051a42578631ab04380a0daef57e67abd8cf1a272e75213285929a74c5e.exe и 0xNax.exe.

*d) Информация о криптовалютном кошельке*

DCRat способен красть широкий спектр конфиденциальной информации, включая информацию о криптовалютном кошельке. Отдельный модуль вредоносного ПО CryptoStealer позволяет злоумышленникам получать доступ к крипто-кошелькам пользователей. Это могут быть закрытые ключи, необходимые для доступа к кошелькам и контроля над ними, а также история транзакций и информация о балансе.

*e) Скриншоты, которые может сделать DCRat*

DCRat имеет возможность делать скриншоты компьютера жертвы. Это может быть использовано для мониторинга их активности, включая веб-сайты, которые они посещают, приложения, которые они используют, и информацию, которую они вводят в эти приложения. Это может включать конфиденциальную информацию, такую как учётные данные для входа в систему, данные кредитной карты и другую личную информацию. Вредоносная программа может запустить поток, чтобы начать делать скриншоты с компьютера жертвы и сохранять их в формате JPEG, затем загружать файлы на C2

IX.

# СИСТЕМА ОЦЕНКИ УЯЗВИМОСТЕЙ CVSS 4.0





#### A. Введение

Общая система оценки уязвимостей (CVSS) версии 4.0 представляет собой последнюю итерацию стандартной отраслевой системы количественной оценки критичности и воздействия уязвимостей программного обеспечения.

CVSS v4.0 вносит несколько существенных изменений и улучшений по сравнению с предыдущей версией (v3.1), чтобы обеспечить более детальную, точную и всестороннюю оценку уязвимостей.

В анализе ниже будут рассмотрены различные аспекты CVSS версии 4.0, включая улучшенные показатели, введение новых категорий и последствия, которые эти изменения имеют для специалистов по кибербезопасности и организаций. Анализируя спецификацию CVSS версии 4.0, будет представлено качественное резюме, в котором собраны основные улучшения и модификации по сравнению с её предшественником, CVSS версии 3.1, что позволит читателям лучше понять её влияние на процессы управления уязвимостями. Благодаря тщательному изучению платформы CVSS версии 4.0 наряду с выводами экспертов по кибербезопасности, этот анализ направлен на то, чтобы предоставить чёткое руководство по эффективному использованию CVSS версии 4.0 для повышения уровня безопасности организации.

#### B. Ключевые изменения

Основные обновления в CVSS версии 4.0:

- **Новые базовые метрики и значения:** вводятся новые базовые метрики, которые отражают дополнительные аспекты риска, такие как потенциальные последствия успешной атаки, включая оценку воздействия на уязвимую систему (VC, VI, VA) и последующие системы (SC, SI, SA)

- **Упрощённые метрики угроз:** Временная оценка была переименована в Threat Metric Group и теперь включает только один показатель – зрелость
- **Новая дополнительная группа метрик:** группа введена для улучшения внешних атрибутов, дающих дополнительное представление о характеристиках уязвимости
- **Изменения в векторной строке:** Векторная строка была обновлена и теперь начинается с CVSS: 4.0, а не с CVSS: 3.1. Хотя в векторную строку не вносились никакие другие изменения, CVSS версии 4.0 содержит изменения в определении некоторых значений метрик и в формулах
- **Улучшенное руководство:** CVSS v4.0 предоставляет улучшенные рекомендации аналитикам для получения согласованных оценок, рекомендации по оценке уязвимостей в библиотеках ПО и поддерживает несколько оценок CVSS для одной и той же уязвимости, которая затрагивает разные платформы или операционные системы
- **Повышенная ясность и простота:** CVSS 4.0 нацелен на обеспечение более упорядоченного процесса расчёта, и снижения субъективности за счёт более конкретизации по метрикам
- **Акцент на отказоустойчивость:** CVSS 4.0 вновь уделяет внимание отказоустойчивости, особенно на ранних стадиях эксплойта, решая растущие проблемы, связанные с безопасностью операционных технологий (OT), промышленных систем управления (ICS) и Интернета вещей (IoT)
- **Переименование ключевых метрик:** Временные метрики в CVSS 3.1 были переименованы в метрики угроз в CVSS 4.0
- **Взаимодействие с пользователем:** CVSS 4.0 сделала показатель взаимодействия с пользователем более детализированным. В то время как в CVSS 3.1 для этого метрики были заданы значения None (N) или Required (R), в CVSS 4.0 параметры были расширены до Active, Passive и None
- **Новые базовые метрики и значения:** CVSS 4.0 вводит новые базовые метрики и значения, обеспечивая более детальную и точную оценку уязвимостей
- **Оценка воздействия на уязвимые и последующие системы:** CVSS 4.0 обеспечивает более точное представление о воздействии уязвимостей как на уязвимую систему, так и на последующие системы
- **Упрощение метрик угроз:** Метрики угроз были упрощены, чтобы сфокусироваться только на зрелости эксплойтов
- **Новая дополнительная группа метрик:** CVSS 4.0 представляет новую дополнительную группу метрик

- **Требования к атаке:** CVSS 4.0 вводит новую базовую метрику "Требования к атаке", которая получает значение "Присутствует", если есть условие предварительной атаки
- **Изменения области применения:** Функция "Области применения" из CVSS версии v3.1 была удалена и заменена понятием "Уязвимая система"
- **Поддержка нескольких оценок:** CVSS 4.0 предназначен для поддержки нескольких оценок CVSS для одной и той же уязвимости, которая затрагивает разные платформы, операционные системы и т.д.
- **Рекомендации для других секторов:** CVSS 4.0 Расширение рамок CVSS в отношении других отраслей, например, автомобилестроение.

#### *C. Преимущества использования cvss версии 4.0 по сравнению с предыдущими версиями*

CVSS v4.0 улучшает оценку уязвимостей за счёт внедрения детального и точного представления рисков, связанных с уязвимостями программного обеспечения:

- **Более детализированные базовые метрики** – CVSS версии 4.0 включает новые базовые метрики и значения, которые отражают дополнительные аспекты риска, такие как потенциальные последствия успешной атаки. Это включает в себя чёткую оценку воздействия на Уязвимую систему (VC, VI, VA) и Последующие системы (SC, SI, SA), что позволяет получить более подробное представление о воздействии уязвимости
- **Интеграция анализа угроз** – Группа метрик угроз в CVSS версии 4.0 регулирует критичность уязвимости на основе факторов реального времени, таких как доступность кода, подтверждающего концепцию, или активное использование. Такая интеграция анализа угроз гарантирует, что оценка отражает текущий ландшафт угроз и вероятность атаки
- **Метрики окружения** – уточняют оценку критичности для конкретной вычислительной среды. Учитываются такие факторы, как наличие мер по смягчению последствий и критичность затронутой системы в среде пользователя для проведения более индивидуальной оценки рисков
- **Упрощённые метрики угроз** – Группа метрик угроз, ранее известная как Временные метрики, была упрощена, чтобы сосредоточиться на наиболее важном аспекте оценки уязвимостей в режиме реального времени - зрелости эксплойтов. Это упрощение помогает пользователям лучше понимать риск уязвимостей
- **Повышенная ясность и простота** – CVSS 4.0 направлена на уменьшение двусмысленностей и несоответствий в оценках уязвимостей, которые были распространены в предыдущих версиях. Новая

версия содержит более конкретные рекомендации и определения метрик, которые должны привести к более точному подсчёту рейтинга

- **Поддержка нескольких оценок** – Новая платформа предназначена для поддержки нескольких оценок CVSS для одной и той же уязвимости, когда она затрагивает разные платформы или операционные системы, обеспечивая более полную оценку
- **Акцент на отказоустойчивость** – уделяется внимание отказоустойчивости, особенно на ранних стадиях эксплойта, что становится все более важным для безопасности операционных технологий (OT), промышленных систем управления (ICS) и Интернета вещей (IoT)
- **Предоставляемая поставщиком оценка критичности и воздействия** – теперь интегрируется предоставляемую поставщиком оценку критичности и воздействия, учитывая более широкий спектр точек зрения и более точно согласовывая процесс оценки с реальными сценариями
- **Повышенная точность оценки уязвимостей** – The Целью CVSS версии 4.0 является обеспечение повышенной точности оценки уязвимостей для отрасли и общественности, включая различные усовершенствования для повышения точности оценки уязвимостей

#### *D. Детализированные метрики и процесс подсчёта рейтинга*

CVSS v4.0 вводит несколько более детализированных метрик для обеспечения более детального понимания технических характеристик уязвимостей. Одним из ключевых изменений является более детальная разбивка базовых метрик, которая включает новые значения для взаимодействия с пользователем, классифицируемые как Пассивные или Активные. Метрика взаимодействия с пользователем (UI) в CVSS версии 4.0 обеспечивает большую детализацию требуемого объёма взаимодействия. Кроме того, CVSS версии 4.0 вводит новую метрику требований к атаке, которая обеспечивает большую детализацию при описании предварительных условий, позволяющих атаковать.

CVSS версии 4.0 упрощает процесс оценки несколькими способами. Метрики угроз, ранее известные как временные метрики, были упрощены и переименованы, чтобы подчеркнуть важность оценки уязвимостей в режиме реального времени. Уровень исправления (RL) и достоверность отчёта (RC) были удалены, а срок действия "Кода" эксплойта был переименован в срок действия эксплойта (E). Временные метрики были упрощены, чтобы помочь потребителям лучше понять риск уязвимостей. Система оценки в CVSS версии 4.0 проще и гибче по сравнению с предыдущими версиями, цель которой - обеспечить универсальную основу для оценки различных уязвимостей.



## Е. Список метрик

Общая система оценки уязвимостей (CVSS) версии 4.0 состоит из четырёх групп метрик: базовые, метрики угрозы, окружения и дополнительные.

**Базовая группа метрик** представляет собой внутренние характеристики уязвимости, которые остаются постоянными с течением времени и в разных пользовательских средах. Базовый балл рассчитывается по специальной формуле, которая учитывает такие факторы, как влияние уязвимости на целостность, конфиденциальность, доступность, возможность использования и масштаб.

**Группа метрик угроз**, ранее известная как группа временных метрик, предоставляет дополнительный контекст для базовых метрик. Однако метрики угроз не оказывают существенного влияния на итоговую оценку CVSS.

**Группа метрик окружения** представляет характеристики уязвимости, которые являются уникальными для среды пользователя. Эти метрики позволяют организациям настраивать метрики CVSS на основе их конкретной среды. Однако метрики состояния окружения определяются пользователями и напрямую не влияют на общедоступные оценки CVSS, которые основаны исключительно на Базовой оценке.

**Дополнительная группа метрик** — это новое дополнение в CVSS версии 4.0. В неё входят метрики, обеспечивающие дополнительный контекст, такие как автоматизируемость, восстановление, срочность для поставщика и усилия по устранению уязвимостей. Однако дополнительные метрики являются необязательными и не оказывают никакого влияния на окончательный расчётный балл CVSS.

### 1) Базовые метрики

Базовые метрики представляют собой неотъемлемые качества уязвимости:

- Вектор атаки (AV)
- Сложность атаки (AC)
- Требуемые привилегии (PR)
- Взаимодействие с пользователем (UI)
- Область применения
- Метрики воздействия: Конфиденциальность уязвимой системы (VC), Целостность (VI), Доступность (VA) и Системные Конфиденциальность (SC), Целостность (SI), Доступность (SA)

#### а) Цель

Базовая группа метрик представляет собой внутренние качества уязвимости, которые остаются постоянными с течением времени. Она состоит из двух наборов метрик: метрик возможности использования и метрик воздействия. Метрики эксплуатируемости отражают простоту и технические средства, с помощью которых уязвимость

может быть использована, в то время как метрики воздействия отражают прямые последствия успешного эксплойта. Базовые метрики помогают определить начальную оценку критичности уязвимости. В CVSS версии v3.1 базовая группа метрик состояла из четырёх основных метрик: вектор атаки (AV), Сложность атаки (AC), Требуемые привилегии (PR) и взаимодействие с пользователем (UI). В CVSS 4.0 введён показатель, называемый Требованиями к атаке (AT), для повышения детализации системы подсчёта рейтинга

#### б) Влияние на оценку

Базовые метрики дают оценку в диапазоне от 0 до 10, которую затем можно изменить, оценив метрики угрозы и окружения. Базовая оценка отражает техническую критичность уязвимости только при рассмотрении ее отдельно. Важно отметить, что базовый балл является лишь отправной точкой для построения полной картины риска, связанного с уязвимостью.

#### с) Использование

Базовая группа метрик используется для оценки фундаментальных качеств уязвимости, которые сохраняют своё постоянство с течением времени. Он используется для оценки критичности уязвимостей и их влияния на организации без учёта временных метрик или окружения

#### д) Расчёт

Базовые метрики делятся на метрики эксплуатируемости и метрики воздействия. Когда аналитик присваивает этим базовым метрикам значения, они дают оценку в диапазоне от 0.0 до 10.0.

Калькулятор CVSS версии 4.0, который является эталонной реализацией стандарта CVSS, может использоваться для генерации оценок на основе значений этих метрик. Калькулятор применяет формулу, указанную в стандарте CVSS версии 4.0, для получения базового балла

#### е) Распределение приоритетов уязвимостей

Базовые метрики представляют собой внутренние характеристики уязвимости, которые остаются постоянными с течением времени и в разных пользовательских средах. Они включают метрики возможности использования (такие как вектор атаки, сложность атаки, требования к атаке, требуемые привилегии и взаимодействие с пользователем) и метрики воздействия на уязвимую систему (такие как конфиденциальность, целостность и доступность) и последующие метрики воздействия на систему. Базовые метрики дают оценку в диапазоне от 0 до 10, которая отражает техническую критичность уязвимости, если рассматривать ее изолированно. Этот показатель важен при анализе уязвимости и помогает определить приоритеты уязвимостей на основе присущих им характеристик

### 2) Метрики угроз

Метрики угроз, ранее известные как Временные метрики, корректируют критичность уязвимости на основе факторов реального времени. К ним относятся:

- Зрелость использования (E)

- Уровень восстановления (RL)
- Достоверность отчета (RC)

*a) Цель*

Цель группы метрик угроз – скорректировать критичность уязвимости на основе таких факторов, как доступность кода, подтверждающего концепцию, или активное использование. Эта группа отражает характеристики уязвимостей, связанные с угрозой, которые могут меняться с течением времени.

Например, он включать такую информацию, использовалась ли уязвимость или существует ли какой-либо подтверждающий концепцию эксплойт. Значения, найденные в этой группе метрик, могут меняться с течением времени, отражая меняющийся ландшафт угроз.

*b) Влияние на оценку*

Группа метрик угроз влияет на итоговую оценку CVSS, корректируя критичность уязвимости в зависимости от ландшафта угроз. Отсутствие явных выбранных метрик угрозы все равно приведёт к получению балла, но включение “Т” в номенклатуру уместно, если какие-либо метрики угрозы используются для корректировки балла

*c) Использование*

Группа метрик угроз используется для уточнения оценки критичности уязвимости на основе применимого анализа угроз. Он используется в сочетании с группой базовых метрик, которая представляет внутренние качества уязвимости, которые остаются постоянными с течением времени, и группой метрик среды, которая представляет характеристики уязвимости, уникальные для конкретной вычислительной среды.

*d) Расчёт*

Метрики угроз в Общей системе оценки уязвимостей (CVSS) версии 4.0 корректируют критичность уязвимости на основе таких факторов, как доступность кода, подтверждающего концепцию, или активное использование. Эти метрики отражают характеристики уязвимости, связанные с угрозой, которые могут меняться с течением времени.

В CVSS версии 4.0 метрики угроз заменили временные метрики из предыдущих версий, что привело к более конкретным и упрощённым метрикам. Метрики уровня исправления (RL) и достоверности отчёта (RC), которые были частью временных метрик в предыдущих версиях, были удалены в CVSS версии 4.0.

Значения, присвоенные метрикам угрозы, используются при расчёте окончательной оценки наряду с базовыми метриками и метриками окружения. Если явные значения метрик угрозы не предоставлены, используются значения по умолчанию, которые предполагают наибольшую критичность.

Калькулятор CVSS версии 4.0, который является эталонной реализацией стандарта CVSS, может использоваться для генерации оценок на основе значений этих метрик. Калькулятор применяет формулу, указанную

в стандарте CVSS версии 4.0, для получения окончательной оценки, которая включает метрики угрозы.

*e) Определение приоритетов уязвимостей*

Метрики угроз, ранее известные как временные метрики, корректируют критичность уязвимости на основе таких факторов, как доступность кода, подтверждающего концепцию, или активное использование. Эти метрики отражают характеристики уязвимости, которые меняются с течением времени, например, использовалась ли уязвимость или существует ли какой-либо подтверждающий концепцию эксплойт. Значения в этой группе метрик могут меняться с течением времени, и они помогают в оценке уязвимости в режиме реального времени. Принимая во внимание вероятность использования и потенциальное воздействие успешной атаки, CVSS версии 4.0 стремится предложить более целостную и точную оценку уязвимостей.

*3) Метрики окружения*

Метрики окружения позволяют организациям настраивать метрики CVSS на основе их конкретной среды. Они включают:

- Изменённые Базовые метрики
- Потенциальный сопутствующий ущерб (CDP)
- Метрики требований к безопасности: Требования к конфиденциальности уязвимой системы (CR), Требования к целостности уязвимой системы (IR) и требования к доступности уязвимой системы (AR)

*a) Цель*

Группа метрик среды в CVSS версии 4.0 представляет характеристики уязвимости, уникальные для среды пользователя. Это позволяет организациям корректировать Базовую оценку уязвимости, чтобы отразить ее влияние в их конкретном контексте. Эта группа объясняет наличие средств контроля безопасности, которые могут смягчить некоторые или все последствия уязвимости, и относительную важность уязвимой системы в технологической инфраструктуре.

*b) Влияние на оценку*

Метрики окружения позволяют аналитикам настраивать оценку CVSS с учётом исходных данных, касающихся важности ИТ-активов и наличия мер по смягчению последствий, которые могут увеличить или уменьшить критичность уязвимости. Эти метрики являются модификаторами базовой группы метрик и предназначены для учёта аспектов деятельности предприятия, которые могут влиять на критичность уязвимости. Группа метрик окружения влияет на итоговую оценку CVSS, позволяя вносить коррективы в зависимости от конкретной среды, в которой существует уязвимость.

*c) Использование*

Группа метрик окружения используется для адаптации метрики CVSS к уникальной среде организации с учётом таких факторов, как важность затронутого ИТ-актива и эффективность существующих средств контроля

безопасности. Эти метрики являются модифицированным эквивалентом Базовых метрик и задаются пользователями для обеспечения более точной оценки риска, связанного с уязвимостью, в их конкретном операционном контексте.

#### *d) Расчёт*

Метрики окружения в Общей системе оценки уязвимостей (CVSS) версии 4.0 предназначены для корректировки базовой оценки уязвимости с учётом воздействия в конкретном организационном контексте. Эти метрики учитывают цели защиты уязвимой системы и наличие средств контроля безопасности, которые уменьшают уязвимость.

Метрики рассчитываются путём предварительного определения Модифицированных базовых метрик, которые представляют собой Базовые метрики, скорректированные с учётом наличия мер по смягчению последствий или компенсирующих средств управления. Требования безопасности используются для указания важности затронутого ИТ-ресурса для организации, что может усилить или уменьшить критичность в зависимости от критичности актива. Показатель потенциального сопутствующего ущерба отражает потенциальный непрямо́й ущерб, выходящим за рамки ИТ-активов.

Окончательная оценка окружения рассчитывается путём объединения модифицированных базовых метрик с требованиями безопасности и потенциальным сопутствующим ущербом с использованием формулы из спецификации CVSS v4.0. Этот показатель обеспечивает индивидуальную оценку критичности уязвимости в конкретной среде организации

#### *e) Определение приоритетов уязвимостей*

Метрики окружения дополнительно уточняют результирующий показатель критичности для конкретной вычислительной среды. Они учитывают такие факторы, как наличие мер по смягчению последствий в этой среде и критичность систем. Эти метрики задаются пользователями и могут привести к расхождению между оценкой и фактическим риском в реальном мире из-за их субъективного характера. Однако они имеют решающее значение для обеспечения более точной оценки уязвимостей в конкретной среде, тем самым улучшая определение приоритетов уязвимости и управление рисками.

#### *4) Дополнительные метрики*

Дополнительные метрики предоставляют дополнительный контекст и описывают аспекты уязвимости, которые выходят за рамки основного стандарта CVSS. К ним относятся:

- Автоматизируемость (A)
- Контроль над ресурсами (VD)
- Восстановление ®
- Срочность устранения (PU)
- Усилия по реагированию на уязвимости (VRE)

#### *a) Цель*

Цель Дополнительной группы метрик - предоставить пользователям контекстуальную информацию, позволяющую более детально разобраться в уязвимостях. Эти метрики дают ценную информацию о внешних аспектах уязвимостей, позволяя потребителям глубже вникать в конкретные контекстуальные соображения. Они предназначены для обеспечения более полного понимания уязвимостей путём описания и измерения дополнительных внешних атрибутов

#### *b) Влияние на оценку*

В отличие от основных метрик CVSS, Дополнительные метрики не участвуют в расчёте рейтинга CVSS. Они не оказывают никакого влияния на окончательный расчётный балл CVSS. Вместо этого они служат дополнительной информацией для более детальной оценки уязвимости. Затем организации могут присвоить важность и /или эффективное влияние каждой метрике или набору / комбинации метрик, оказывая им большее, меньшее или абсолютно нулевое влияние на конечный анализ рисков

#### *c) Использование*

Использование каждой метрики в группе дополнительных метрик определяется потребителем оценки. Эта контекстуальная информация может использоваться по-разному в среде каждого потребителя. Затем потребитель информации может использовать значения этих Дополнительных метрик для выполнения дополнительных действий, если он того пожелает, придавая метрикам и значениям локальную значимость.

#### *d) Расчёт*

Дополнительные метрики в Общей системе оценки уязвимостей (CVSS) версии 4.0 являются новым дополнением, разработанным для предоставления дополнительного контекста и описания внешних атрибутов уязвимости. Эти метрики необязательны и не участвуют в расчёте окончательной оценки CVSS. Вместо этого они служат дополнительной информацией для более детальной оценки уязвимости.

План использования и реагирования на каждую метрику в группе дополнительных метрик определяется пользователем, проводящим оценку. Эта контекстуальная информация может использоваться по-разному в среде каждого пользователя. Затем организации могут присвоить важность и /или эффективное влияние каждой метрике или набору / комбинации метрик, оказывая им большее, меньшее или абсолютно нулевое влияние на окончательный анализ рисков.

#### *e) Распределение приоритетов уязвимостей*

Дополнительные метрики являются новым дополнением в CVSS версии 4.0. Они измеряют внешние атрибуты уязвимости и предоставляют контекстуальную информацию. Эти метрики не влияют на оценку уязвимости, но могут быть использованы для информирования компаний, приобретающих продукты для обеспечения дополнительного контекста для групп по уязвимости и устранению последствий

### 5) *Различия*

Дополнительная группа метрик используется для предоставления дополнительного контекста и не влияет на оценку CVSS, в то время как группы метрик базы, угрозы и окружения вносят непосредственный вклад в процесс оценки и необходимы для расчёта критичности уязвимости. Группа дополнительных метрик в CVSS версии 4.0 отличается от групп базовых метрик, метрик угроз и метрик окружения несколькими способами:

#### **Дополнительная группа метрик:**

- **Назначение:** предоставляет дополнительный контекст и описывает внешние атрибуты уязвимости, которые выходят за рамки основного стандарта CVSS
- **Влияние на оценку:** Метрики в этой группе не влияют на окончательный расчётный балл CVSS. Они являются необязательными и используются для передачи дополнительной информации, которая может повлиять на анализ рисков организации и план реагирования
- **Использование:** Использование и план реагирования для каждой метрики в группе дополнительных метрик определяются пользователем, проводящим оценку, и эта контекстуальная информация может использоваться по-разному в среде каждого потребителя

#### **Базовые группы метрик, угрозы и окружения:**

- **Назначение:** Эти группы содержат метрики, которые непосредственно вносят вклад в расчёт метрики CVSS, отражающего внутренние характеристики уязвимости (Базовый уровень), ландшафт угроз в реальном времени (Угроза) и конкретное воздействие в контексте организации (окружение)
- **Влияние на оценку:** Метрики в этих группах напрямую влияют на итоговую оценку CVSS, причём каждая группа по-разному оценивает критичность и влияние уязвимости
- **Использование:** Базовые метрики предоставляются организацией, обслуживающей уязвимую систему, или третьей стороной, в то время как метрики угроз и окружение предназначены для конечных потребителей, чтобы дополнить базовые метрики дополнительным контекстом

### F. *Метрики воздействия различных технологий*

В CVSS версии 4.0 были введены новые метрики для учёта выявления уязвимостей в операционных технологиях (OT) и их воздействия. Эти метрики особенно актуальны в связи с растущей озабоченностью по поводу безопасности OT, промышленных систем управления (ИС) и Интернета вещей (IoT). Обновления направлены на обеспечение более точной оценки рисков, связанных с уязвимостями в этих средах

#### 1) *Метрики безопасности*

Метрики безопасности были добавлены как в группы дополнительных метрик, так и в группы метрик окружения в CVSS версии 4.0. Эти метрики оценивают потенциальное влияние использования уязвимости на безопасность, что особенно важно в таких секторах, как здравоохранение или промышленные системы управления, где безопасность является критической проблемой

#### 2) *Особые соображения, связанные с OT*

Новые метрики воздействия эксплуатационных технологий включают в себя соображения о том, соответствуют «и "последствия уязвимости определению ИЕС 61»08", который является стандартом функциональной безопасности систем, связанных с электрической / электронной / программируемой электроникой. Это включение отражает растущую озабоченность по поводу кибер-рисков OT и потребность в системе оценки, которая может адекватно отражать уникальные риски, связанные с средами OT

#### 3) *Воздействие на Уязвимые и Последующие системы*

В CVSS версии 4.0 также особое внимание уделяется оценке воздействия эксплуатации уязвимости как на уязвимую систему, так и на последующие системы. Это особенно актуально для операционных сред, где уязвимость в одном компоненте потенциально может оказывать каскадное воздействие на другие взаимосвязанные системы

#### 4) *Использование дополнительных метрик и метрик окружения*

Хотя Дополнительные метрики напрямую не влияют на итоговую оценку CVSS, они предоставляют ценную контекстуальную информацию, которая может быть использована организациями для обоснования своего анализа рисков и планов реагирования. Метрики окружения позволяют настраивать оценки CVSS на основе конкретной среды, которая может включать в себя другие настройки

A stylized illustration of a hacker wearing a red hood and goggles, typing on a laptop in a digital environment. The background is filled with glowing blue and green lines representing data and code. The text "RANSOMWARE Q3" is prominently displayed in the center, with a small "x." to its left.

x. **RANSOMWARE Q3**



## A. Введение

Ниже подробно проанализируем публичные материалы о программах-вымогателях за третий квартал 2023, углубляясь в различные аспекты текущей ситуации, меняющиеся тенденции в атаках, отрасли и географию явления. Материалы позволяют оценить как количественные факторы инцидентов, так и качественный синтез данных применяемых тактик, и последствия для стратегий кибербезопасности в будущем. Цель анализа – предоставить читателям полезную информацию и более глубокое понимание феномена программ-вымогателей в его нынешнем виде и прогнозов на 2024.

## B. Отличительные особенности за 2023 год

- **Рост количества атак программ-вымогателей:** Количество известных атак, при которых жертва не платила выкуп, составило 457 только в ноябре; общее количество зарегистрированных атак составило 1900, а нераскрытых массовых атак было 1815 за первые полгода. Количество сообщений, связанных с программами-вымогателями, составило 4082, в среднем 371,1 сообщения в месяц.
- **Атаки программ-вымогателей на сектор здравоохранения:** за последние четыре года количество атак на сектор здравоохранения увеличилось на 278%. Крупные нарушения, о которых сообщалось, затронули более 88 миллионов человек (на 60% больше чем в 2022).
- **Успех программ-вымогателей:** 2023 год отмечен как самый успешный год для групп программ-вымогателей за всю историю: в общей сложности 4368 жертв, что на 55,5% больше, чем в предыдущем году. Только за второй и третий кварталы 2023 года общее число жертв превысило 2022 год и составило 2903 человека.
- **Всплеск числа программ-вымогателей:** Во втором квартале 2023 года количество случаев вымогательства увеличилось на 67% по сравнению

с предыдущим кварталом, жертвами стали 1386 человек по всему миру. Ведущими группами программ-вымогателей в этот период были LockBit3.0, ALPHV и Cl0p.

- **Кампания MOVEit:** Кампания MOVEit была признана самой успешной в этом году, что подчёркивает важность chain-атак и необходимость надёжного контроля версий и понимания поверхности атаки. Основной мишенью были США, где было зарегистрировано примерно 64% случаев.
- **Рекордный третий квартал:** Третий квартал 2023 года стал самым успешным кварталом в истории программ-вымогателей, поскольку на отрасль сильно повлияла эксплуатация критических уязвимостей и появление новых групп и семейств программ-вымогателей.
- **Рост отрасли в целом:** несмотря на глобальные усилия правоохранительных органов по борьбе с программами-вымогателями, отрасль быстро расширяется.
- **Новые программы-вымогатели:** было ликвидировано множество программ-вымогателей, включая Hive, RansomedVC и ALPHV. Однако появились и новые игроки, такие как Hunters International, Dragon Force и WereWolves.
- **Выкупы вымогателям:** Средний размер корпоративного выкупа превысил 100 000 долларов при среднем требовании в размере 5,3 миллиона долларов. 80% организаций придерживаются политики "Не платить", и только 41% организаций заплатили выкуп.
- **Страхование от программ-вымогателей:** 77% организаций обнаружили, что программы-вымогатели специально исключены из их страхования безопасности.
- **Цели:** в США промышленный сектор подвергся атакам 48 различных групп программ-вымогателей.
- **Атаки на крупные компании:** Toyota, Boeing и другие компании с использованием уязвимости Citrix Bleed (CVE-2023-4966).
- **Программа-вымогатель как услуга (RaaS):** Распространение RaaS стало заметной тенденцией, упростив киберпреступникам выполнение атак.

## C. Особенности кампании MOVEit

Кампания MOVEit относится к инциденту 2023 года, связанному с использованием уязвимости нулевого дня в программном обеспечении для передачи файлов MOVEit, разработанном Progress Software. Кампания была организована группой программ-вымогателей Cl0p, которая использовала уязвимость для кражи данных многочисленных организаций в различных секторах, включая правительство, финансы и здравоохранение.

- **Уязвимость и эксплуатация:** уязвимость CVE-2023-34362 затронула как локальные, так и облачные версии MOVEit и связана с SQL-

инъекциями для манипулирования данными и получения доступа к базе данных.

- **Исполнители:** ответственность за атаки несла группа Clop, которая в том же году была связана с инцидентами GoAnywhere и PaperCut.
- **Влияние:** Кампания оказала значительное влияние, затронув более 1062 организаций и примерно 65 435 641 человека к концу августа 2023 года. Жертвы охватывали целый ряд отраслей и включали как частные организации, так и организации государственного сектора.
- **Реакция:** Progress Software оперативно отреагировала на обнаружение уязвимости, выпустив исправление. Однако спустя месяцы число жертв продолжало расти, что наводит на мысль о том, что многие организации, вероятно, подверглись взлому в первые несколько дней и недель кампании.
- **Последствия:** Кампания MOVEit подчеркнула важность упреждающей безопасности и управления уязвимостями. Потенциальный ущерб может быть нанесён, поскольку многие организации были скомпрометированы потому, что наняли сторонних подрядчиков или субподрядчиков.

#### D. География

- **Глобальное распространение:** расширение географии присутствия на новые страны и регионы.
- **Наиболее пострадавшие страны:** США были наиболее пострадавшей страной с большим количеством взломанных учётных записей, далее Великобритания, Канада, Мозамбик, Ангола и Гана.
- **Сектора:** сектора образования, строительный и недвижимость, центральное и федеральное правительство, средства массовой информации, развлечения, а также местные органы власти.
- **Тенденции в области программ-вымогателей:** появились новые группы программ-вымогателей, такие как Rhysida, BianLian, IceFire, Sparta и B100dy, что подчёркивает развивающийся характер отрасли.

#### E. Результаты третьего квартала 2023 года

- **Рекордная активность:** наблюдался значительный всплеск активности программ-вымогателей: частота глобальных атак вымогателей выросла на 11% по сравнению со вторым кварталом и на 95% в годовом исчислении (г/г).
- **Жертвы:** Количество жертв программ-вымогателей в 2023 году уже превысило то, что наблюдалось в 2021 и 2022 годах.
- **Новые игроки:** такие программы-вымогатели как MalasLocker, 8base и NokoYawa, привлекли внимание, так как за первый квартал своей деятельности эти группы в совокупности заявили о 305 жертвах.

- **Отрасли:** Атаки затронули производство, правительственные учреждения, нефтегазовый сектор, транспорт, логистику и складирование.
- **Тенденции на будущее:** Исходя из активности в конце 3-го и начале 4-го квартала, ожидается, что цифры превзойдут все, что наблюдалось в предыдущие годы

#### F. Прогноз на 2024 год

- **Chain-атаки:** используются преимуществами инфраструктуры ориентированной на подрядчиков и субподрядчиков, вкпе с традиционными методами, таких как использование учётных данных и использование методов социальной инженерии
- **Тенденции:** индустрия программ-вымогателей развивается с появлением новых групп и тактик.
- **Страхование от программ-вымогателей:** по мере роста числа атак программ-вымогателей роль страхования в кибербезопасности будет становиться все более важной, поскольку организациям необходимо ориентироваться в сложностях покрытия инцидентов с вымогателями
- **Технологические разработки:** кибербезопасность будет продолжать развиваться с переходом к более комплексным стратегиям защиты, которые включают предотвращение, обнаружение, устранение последствий
- **Глобальное воздействие:** ожидается, что географическое влияние программ-вымогателей останется значительным, поскольку киберпреступники по-прежнему нацелены на широкий круг стран и отраслей

#### G. Заключение

- **Атаки:** 2023 наиболее целевым сектором был сектор деловых услуг, за которым следовали секторы розничной торговли и производства.
- **Рост индустрии программ-вымогателей:** несмотря на усилия правоохранительных органов, индустрия программ-вымогателей продолжала быстро расти. Появились новые группы, а существующие, такие как LockBit3.0, ALPHV и Cl0p, нанесли ущерб организациям по всему миру
- **Усилия правоохранительных органов:** правоохранительные органы по всему миру работают над тем, чтобы остановить рост индустрии программ-вымогателей. Они добились определённого успеха в закрытии нескольких крупных киберпреступных группировок, таких как N1VE
- **Прогноз на 2024 год:** индустрия программ-вымогателей продолжит расти, при этом новые и существующие группы будут представлять серьёзную угрозу для организаций по всему миру



XI. **RANSOMWARE Q4**





*Аннотация – Анализ тенденций в области программ-вымогателей за 4 квартал 2023 года направлен на понимание многогранного ландшафта угроз, связанных с программами-вымогателями и произошедших изменений.*

*С учётом специфики можно определить особенности операций, совершаемых с использованием программ-вымогателей, включая идентификацию доминирующих групп программ-вымогателей, их целевых секторов и географического распределения атак.*

*Кроме того, анализ выявит важные тенденции, такие как рост числа инцидентов с программами-вымогателями, эволюция тактики вымогательства и последствия этих изменений для стратегий кибербезопасности.*

*Эти знания будут полезны как для специалистов в области технической, так и стратегической безопасности, предлагая информацию, которая может направлять разработку надёжных механизмов защиты, информировать о решениях по управлению рисками и, в конечном счёте, повышать устойчивость организаций к постоянно присутствующей угрозе программ-вымогателей.*

#### *А. Введение*

2023 год стал самым успешным годом для групп программ-вымогателей в истории: в общей сложности 4368 жертв, что на 55,5% больше, чем в предыдущем году. Только в четвёртом квартале число жертв составило 1386 человек, что указывает на постоянное влияние программ-вымогателей на отрасль.

В 4 квартале 2023 года наиболее распространённые типы атак программ-вымогателей в основном осуществлялись тремя группами: LockBit 3.0, Clor Ransomware и ALPHV / BlackCat ransomware. LockBit 3.0 оставалась самой активной группой программ-вымогателей, заявляя в среднем о 23 жертвах в неделю.

В ежеквартальном отчёте Air IT об угрозах подчёркивается, что атаки программ-вымогателей, фишинг и инсайдерские угрозы по-прежнему представляют значительные риски, при этом резкий рост объёма данных и расширение уязвимостей глобальной сети. В отчёте ISACA о состоянии кибербезопасности за 2023 год указано, что 48% организаций столкнулись с ростом кибератак в 4 квартале 2023 года.

В отчёте TechTarget о тенденциях в области программ-вымогателей на период до 2024 года говорится, что атаки на цепочки поставок и использование облачной и VPN-инфраструктуры по-прежнему будут оставаться ключевыми тенденциями. В отчёте также упоминается, что с 2020 года было обнаружено более 130 различных штаммов программ-вымогателей, причём наиболее распространённым является семейство GandCrab family being the most prevalent.

Отчёт Trend Micro о программах-вымогателях за первую половину 2023 года показал, что LockBit, BlackCat и Clor были ведущими группами RaaS, при этом число организаций-жертв значительно увеличилось по сравнению со второй половиной 2022 года.

Исследование Check Point Research описало 2023 год как год масштабных атак программ-вымогателей с переходом от тактики шифрования к использованию украденных данных для вымогательства. Сектор образования и исследований в наибольшей степени пострадал от атак программ-вымогателей в 2023 году.

#### *В. Воздействие на отрасли*

В 4 квартале 2023 года отраслями, наиболее пострадавшими от атак программ-вымогателей, были сектор бизнес-услуг, сектор образования / исследований и сектор розничной / оптовой торговли.

Сектор бизнес-услуг США был наиболее уязвимым сектором по данным Cyberint.

Сектор образования и исследований также сильно пострадал от атак программ-вымогателей, на долю которых, по данным Check Point Research, пришлось 22% всех атак в 2023 году.

По данным Check Point Research, еженедельный рост числа атак в секторе розничной и оптовой торговли составил 22% по сравнению с 2022 годом.

Другие отрасли, которые были заметно затронуты, включают ИТ, здравоохранение и производственный сектор, которые, по данным Trend Micro, были наиболее уязвимыми с точки зрения обнаружения файлов-вымогателей в первой половине 2023 года. В отчёте TechTarget также перечислены несколько отраслей в качестве приоритетных целей, включая строительство и недвижимость, правительственные учреждения, СМИ, развлечения и досуг, местные и федеральные органы власти, энергетическую и коммунальную инфраструктуру, транспорт, финансовые услуги, а также профессиональные и отдельно юридические услуги.

### С. Ключевые моменты Q4

- **Рекордное количество жертв:** 2023 год стал самым успешным годом для групп программ-вымогателей в истории: в общей сложности 4368 жертв, что на 55,5% больше, чем годом ранее. Только в четвёртом квартале было зафиксировано 1386 жертв
- **Доминирующие группы программ-вымогателей:** LockBit 3.0 оставалась самой активной группой программ-вымогателей, заявляя в среднем о 23 жертвах в неделю. Также были заметны программы-вымогатели Clor и ALPHV / BlackCat, жертвами которых стали 104 и 81 человек соответственно
- **Громкие инциденты:** Известные инциденты включали атаку LockBit на Royal Mail и отключение программы-вымогателя Hive
- **Влияние на отрасль:** Сектор бизнес-услуг, сектор образования / исследований и сектор розничной / оптовой торговли были одними из наиболее пострадавших от атак программ-вымогателей
- **Географический фокус:** главной мишенью стали США, за ними следуют Великобритания и Канада
- **Тенденции в методах атак:** произошёл сдвиг в тактике от шифрования к использованию украденных данных для вымогательства, при этом злоумышленники больше внимания уделяли краже данных и кампаниям по вымогательству, которые не обязательно включали шифрование данных
- **Программа-вымогатель как услуга (RaaS):** RaaS остаётся ключевым фактором атак, и такие группы, как LockBit, работают по этой модели
- **Тактика вымогательства:** Двойные и тройные атаки с целью вымогательства становятся все более распространёнными и потенциально более результативными, и дорогостоящими для пострадавших компаний
- **Chain-Атаки:** chain-атаки стали неотъемлемой частью ландшафта угроз, связанных с программами-вымогателями, распространяя воздействие атак не только на отдельных жертв

### D. Платёжные инструменты программ-вымогателей

В 4 квартале 2023 года наиболее распространёнными способами оплаты, используемыми при атаках программ-вымогателей, по-прежнему оставались криптовалюты, причём наиболее распространённым был биткойн. На биткойн приходилось примерно 98% платежей программ-вымогателей из-за его предполагаемой анонимности и простоты использования. Однако появились первые признаки того, что цифровые валюты, более ориентированные на конфиденциальность, такие как Monero, набирают популярность в качестве предпочтительного способа оплаты для киберпреступников. Этот сдвиг произошёл из-за возрастающей простоты обнаружения потока и источников биткойна.

Несмотря на распространённость выплат с целью получения выкупа, доля жертв, которые платили выкупы, снижалась. Только 37% жертв программ-вымогателей заплатили выкуп в 4 квартале 2023 года, что является рекордно низким показателем. Снижение было связано с улучшением мер безопасности и инвестициями в непрерывность резервного копирования, что позволило большому количеству организаций восстанавливаться после атак без выплаты выкупов.

Средний платёж за выкуп в 4 квартале 2023 года был значительно высоким: средний платёж составил 408 643 доллара, что на 58% больше, чем в 3 квартале 2022 года, а средний платёж составил 185 972 доллара, что на 342% больше, чем в 3 квартале 2022 года. Увеличение сумм платежей было расценено киберпреступниками как тактика компенсации сокращающегося числа жертв, готовых платить выкупы.

### E. Точки входа программ-вымогателей

- **Фишинговые атаки:** Фишинговые атаки были основным методом доставки программ-вымогателей, при этом 62% успешных атак программ-вымогателей использовали фишинг в качестве точки входа в систему жертвы. Число фишинговых атак выросло на 173% в третьем квартале 2023 года. Злоумышленники использовали все более изощренные методы социальной инженерии, чтобы обманом вынудить сотрудников предоставлять конфиденциальную информацию
- **Использование уязвимостей:** Уязвимости в программном обеспечении и системах были ещё одной распространённой точкой входа. Например, группа программ-вымогателей CLOP использовала программное обеспечение для передачи файлов GoAnywhere. Два новых вида программ-вымогателей, SACTUS и 3AM, появились в четвёртом квартале 2023 года, причём SACTUS использовал известные уязвимости в устройствах VPN
- **Кража учётных данных и атаки методом грубой силы:** Кража учётных данных использовалась в 44% успешных атак программ-вымогателей, а учётные данные методом грубой силы, такие как подбор пароля, использовались в 17% атак
- **Атаки на цепочки поставок:** Злоумышленники нацеливались на сторонних поставщиков, чтобы получить доступ к сети организации.
- **Инсайдерские угрозы:** Инсайдерские угрозы продолжали представлять значительные риски для организаций
- **Атаки социальной инженерии:** Атаки социальной инженерии, включая компрометацию деловой электронной почты (BEC), также были распространёнными

### F. Методы шифрования программ-вымогателей

Методы шифрования, используемые в этих атаках, эволюционировали с течением времени, и

злоумышленники используют сочетание симметричных и асимметричных методов шифрования для повышения эффективности своих атак. При таком подходе программа-вымогатель генерирует два набора ключей, и для повышения эффективности атаки используется цепочка шифрования.

В дополнение к этим методам шифрования произошёл заметный сдвиг в стратегиях выполнения атак программ-вымогателей: первичная цель — это кража данных, за которыми следуют кампании по вымогательству, которые не обязательно включают шифрование данных.

#### G. Способы Доставки программ-вымогателей

Наиболее распространёнными методами доставки были chain-атаки по, методы двойного вымогательства и воздействия "Программа-вымогатель как услуга" (RaaS).

Атаки на цепочки поставок стали надёжным методом для зрелых и опытных групп программ-вымогателей. В этих атаках вместо прямого нападения на единственную жертву злоумышленники нацеливаются на сторонних поставщиков, чтобы получить доступ к сети организации.

Двойное вымогательство было ещё одним распространённым методом. С помощью этого метода злоумышленники не только шифруют данные жертвы, но и угрожают утечкой украденных данных, если выкуп не будет выплачен.

Операции с программами-вымогателями как услугой (RaaS) также сыграли значительную роль. В RaaS разработчики создают программное обеспечение-вымогатель и продают доступ к этому инструменту преступникам, которые затем распространяют его среди потенциальных целей. Доступ осуществляется на основе подписки, поэтому он называется RaaS.

Фишинг с вредоносными вложениями и эксплуатация уязвимостей, также использовались в качестве методов начального доступа к целевой системе

#### H. Уязвимости, используемые при атаках программ-вымогателей

В четвёртом квартале 2023 года злоумышленники-вымогатели продолжали использовать ряд уязвимостей для компрометации организаций. Одной из наиболее заметных эксплуатируемых уязвимостей была уязвимость двухлетней давности, для которой примерно в то же время было доступно исправление. Это подчёркивает важность своевременного управления исправлениями и контроля версий в организациях.

Кроме того, использовались уязвимости в ПО MagicLine4NX, и MOVEit, составляя значительный процент жертв в предыдущих кварталах, и вполне вероятно, что такие уязвимости оставались мишенью для групп программ-вымогателей.

В 2023 году также произошёл всплеск использования эксплойтов нулевого дня при атаках программ-

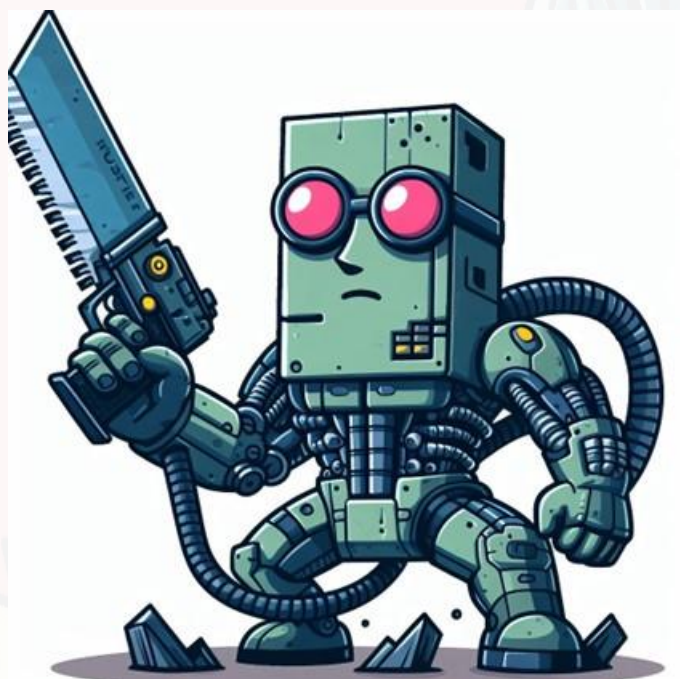
вымогателей, которые представляют собой уязвимости, неизвестные поставщику ПО или не имеющие доступного исправления на момент атаки. Тенденция использования 0-day уязвимостей подчёркивает адаптивность атакующих и необходимость для организаций укреплять свою защиту от таких возникающих угроз.

#### I. Способы предотвращения атак программ-вымогателей

- **Резервное копирование данных:** Регулярное резервное копирование данных является важным шагом в смягчении последствий атаки. Решение для резервного копирования данных может гарантировать, что даже если данные зашифрованы, организация сможет восстановить свои системы без необходимости платить выкуп
- **Обучение кибератакам:** Обучение сотрудников распознавать потенциальные угрозы вымогателей и избегать их, такие как фишинговые электронные письма и вредоносные вложения, может значительно снизить риск успешных атак
- **Управление исправлениями:** Регулярное обновление и исправление ПО может устранить известные уязвимости, которые могут использовать программы-вымогатели
- **Расширенное предотвращение угроз:** Автоматизированные системы обнаружения и предотвращения угроз могут выявлять и устранять большинство атак программ-вымогателей до того, как они нанесут значительный ущерб
- **Защита конечных устройств:** обеспечение безопасности конечных устройств, в т.ч антивирус, могут обнаруживать и блокировать угрозы, связанные с программами-вымогателями
- **Сегментация сети:** Разделение сети на отдельные сегменты может предотвратить распространение программ-вымогателей по всей системе
- **Модель безопасности с нулевым доверием:** Внедрение модели с нулевым доверием, при которой доступ к ресурсам предоставляется только после успешной проверки пользователем своей личности, может снизить вероятность атаки программ-вымогателей
- **Многофакторная аутентификация (MFA):** Внедрение MFA повышает уровень безопасности, затрудняя злоумышленникам доступ к системам
- **Доступ с наименьшими привилегиями:** Обеспечение пользователям минимальных уровней доступа, необходимых для выполнения их задач, ограничивает ущерб от атаки
- **Белый список приложений:** Разрешение запускать в системе только одобренные приложения может предотвратить выполнение программ-вымогателей.

A blue, blocky robot with a square head and large, circular eyes. It is holding a large, blue sword in its right hand. The robot has a mechanical body with various pipes and joints. The background is a light blue gradient.

xii. **CHISEL**  
**SANDSTORM**



*Аннотация – В этом документе представлен анализ вредоносного ПО "Infamous Chisel", приписываемого группе Sandworm. В анализе рассматриваются различные аспекты вредоносного ПО, включая его возможности, компоненты и последствия его развёртывания против конкретных целей, в частности устройств Android.*

*Анализируя компоненты и тактику вредоносного ПО, документ проливает свет на сложную природу киберугроз и их потенциал для компрометации конфиденциальной информации и нарушения операций. Выводы подчёркивают острую необходимость в упреждающих мерах защиты.*

*Для специалистов по кибербезопасности и других направлений этот анализ служит ценным ресурсом для понимания механизма и последствий продвинутых вредоносных угроз. Материалы документа могут послужить основой для разработки более эффективных стратегий и технологий защиты, повышения уровня безопасности организаций ввиду постоянно меняющегося ландшафта киберугроз.*

#### A. Введение

Вредоносная программа Chisel нацелена на устройства Android, обеспечивая удалённый доступ и кражу информации. Sandworm использовал это вредоносное ПО в кампании, направленной на устройства Android, используемых в военном секторе. Вредоносное ПО представляет собой набор компонентов, которые обеспечивают постоянный доступ к заражённому устройству Android через сеть Tor, а также периодически сопоставляют и извлекают информацию о жертве со скомпрометированных устройств. Украденная информация включает в себя информацию о системных устройствах, информацию о коммерческих приложениях и приложениях, специфичных для военного сектора.

#### B. Компоненты печально известного долота

Infamous Chisel — это набор компонентов, связанных с Sandworm, предназначенных для обеспечения удалённого доступа и сбора информации с телефонов Android.

В состав Infamous Chisel входят:

- **netd**: компонент используется для автоматического сбора и фильтрации информации об устройстве. Он также ищет в нескольких каталогах файлы, соответствующие заранее определённому набору расширений, которые затем удаляются.
- **killer**: компонент убивает процесс netd.
- **blob**: компонент выполняется netd и отвечает за настройку и выполнение утилиты Tor td.
- **td**: утилита представляет собой Tor без очевидных модификаций.
- **tcpdump**: утилита представляет собой tcpdump без очевидных модификаций.
- **ndbr\_armv7l** и **ndbr\_i686**: эти утилиты содержат: dropbear, dropbearkey, ssh, scp, nmap, dbclient, watchdog, rmflag, mkflag.
- **db**: утилита содержит: dropbear, dropbearkey, ssh, scp, nmap, dbclient, watchdog, rmflag, mkflag.

#### C. Сетевые и другие возможности

Infamous Chisel предназначен для закрепления в системе путём замены штатного системного двоичного файла netd по пути /system/bin/netd. Когда вредоносный netd запускается, он проверяет, является ли init родительским процессом, который его выполнил. Этот родительский процесс отвечает за создание процессов, перечисленных в скрипте init.rc. Вредоносная замена netd при таком выполнении разветвится и выполнит штатный процесс, резервную копию которого зарезервировали по пути /system/bin/netd\_, передав параметры командной строки. Это сохраняет нормальную функциональность netd, в то же время позволяя вредоносному netd выполняться от имени пользователя root.

Компонент netd предоставляет большую часть пользовательских функций. Основная его цель — сбор и извлечение информации со скомпрометированного устройства через определённые промежутки времени. Он использует комбинацию сценариев оболочки и команд для сбора информации об устройстве и также выполняет поиск в нескольких каталогах, в которые попадают файлы согласно определённому набору критериев.

Infamous Chisel имеет несколько других возможностей:

- **Мониторинг сети и сбор трафика**: может отслеживать сетевую активность и собирать данные о сетевом трафике. Это позволяет собирать информацию о сетевой среде и перехватывать конфиденциальные данные, передаваемые по сети.
- **Доступ по SSH**: может устанавливать соединения SSH, которые можно использовать для удалённого выполнения команд и передачи данных.
- **Сканирование сети**. может сканировать локальную сеть, собирая информацию об активных хостах, открытых портах и баннерах для идентификации другие потенциальные цели в сети.

- **Передача файлов SCP:** может использовать протокол безопасного копирования (SCP) для передачи файлов. Это может быть использовано для кражи данных с заражённого устройства или для переноса вредоносных файлов на устройство.
- **Эксfiltrация информации:** выполняет периодическое сканирование файлов и сетевой информации на предмет кражи. Файлы конфигурации системы и приложений удалены с заражённого устройства.
- **Сбор информации об устройствах:** собирает различную информацию о системных устройствах, информацию о коммерческих приложениях и приложениях, специфичных для военного сектора.
- **Автоматическая эксfiltrация:** удаляет файлы через определённые промежутки времени.
- **Остановка службы:** может остановить штатную службу netd.

#### D. Эксплуатируемые уязвимости

Chisel использует различные уязвимости и методы для обеспечения несанкционированного доступа и контроля над целевыми устройствами Android, например комбинацию уязвимостей системы, небезопасных конфигураций и сетевых протоколов для достижения своих целей. К ним относятся закрепление и повышение привилегий, предотвращения обнаружения, доступ к учётным данным, сбор конфиденциальной информации, создание скрытых каналов управления и контроля и потенциальное перемещение внутри сети.

- **Закрепление и повышение привилегий:** закрепление обеспечивается на заражённом устройстве путём замены штатного системного двоичного файла netd. Эта замена позволяет вредоносному netd выполняться от имени пользователя root, тем самым получая повышенные привилегии.
- **Предотвращение обнаружения.** используется несколько методов предотвращения обнаружения. Например, проверяется, выполняется ли Chisel с помощью init и по пути к штатному netd, что снижает вероятность обнаружения его вредоносных действий. Кроме того, компонент blob распаковывает исполняемые файлы из архивов bzip, чтобы избежать обнаружения путём распаковки его полезных данных только после того, как они прошли первоначальные проверки безопасности.
- **Учётные данные:** используется утилита tcpdump для анализа сетевых интерфейсов и мониторинга сетевого трафика, перехвата учётных данных. Извлекается информация из файлов, содержащих учётные данные и ключевую информацию с использованием системным механизмов доступа.
- **Обнаружение и сбор:** выполняются действия по обнаружению и сбору, такие как перебор каталогов данных для обнаружения интересных файлов, сбор информации GPS, составление списка установленных пакетов и сбор различной системной

информации. Это указывает на то, что Chisel использует отсутствие применения безопасного хранилища и неправильные настройки разрешений на устройстве для доступа и сбора конфиденциальной информации.

- **C2C и эксfiltrация:** настраивает и запускает Tor со скрытым сервисом Drogbear для обеспечения SSH-соединения. Такая настройка позволяет вредоносному ПО установить скрытый канал связи с заражённым устройством, используя сетевые протоколы и службы для сохранения контроля над устройством и кражи собранных данных.
- **Сетевое сканирование и распространение.** содержит функции сканирования локальной сети, сбора информации об активных хостах, открытых портах и баннерах. Эта возможность предполагает, что Chisel использует сетевое окружение заражённого устройства для выявления других потенциальных целей в сети для горизонтального перемещения или дальнейшего использования.

#### E. Эксfiltrация данных

Chisel собирает информацию с заражённых Android-устройств посредством ряда автоматических и ручных процессов. Вредоносное ПО выполняет периодическое сканирование файлов и сетевой информации на предмет кражи файлов, соответствующих заранее определённому набору параметров, и удаляет файлы конфигурации системы и приложений с заражённого устройства.

- **Предотвращение дублирования.** Когда файл выбран для эксfiltrации, он хешируется с использованием MD5 и перекрёстно ссылается на список ранее отправленных хэшей файлов. Это гарантирует, что один и тот же файл не будет отправлен несколько раз.
- **Эксfiltrация файлов из каталогов данных.** программа ищет в указанных каталогах файлы с определёнными расширениями и удаляет их.
- **Эксfiltrация файлов конфигурации и резервных копий конфигурации.** Вредоносная программа ищет файлы.json или.json.bak в указанных каталогах и удаляет их.
- **Эксfiltrация файлов.** программа удаляет файлы с помощью POST-запроса. Ожидается, что ответ сервера будет HTTP, и эксfiltrация считается завершённой, когда сервер отправляет сообщение «Успех» в любом месте своего ответа.
- **Сбор и эксfiltrация информации:** собирает различную информацию о конфигурации оборудования устройства и записывает эту информацию в файлы в каталоге /data/local, которые затем удаляются. Сюда входит идентификатор Android, сетевая информация, список установленных приложений и различная информация об оборудовании устройства.
- **Сканирование локальной сети.** включает в себя встроенный сетевой сканер, который выполняет сканирование IP-адресов локальной сети для

обнаружения других устройств. Результаты этого сканирования немедленно передаются, предоставляя злоумышленникам информацию, которая может облегчить горизонтальное перемещение внутри сети.

- **Частота эксфильтрации.** ПО предназначено для автоматического удаления файлов через регулярные промежутки времени, при этом определённые интервалы устанавливаются для различных типов сбора данных. Например, сбор информации о файлах и устройствах происходит каждые 23 часа 53 минуты, а конфиденциальная информация перекачивается каждые 10 минут.
- **Использование Tor и SSH:** Chisel использует Tor и SSH для C2C-связи, обеспечивая зашифрованный канал, который может быть трудно обнаружить и перехватить. Такая настройка позволяет ПО поддерживать скрытый канал связи с заражённым устройством, что усложняет обнаружение и устранение последствий.

Когда файл выбирается для эксфильтрации, он хешируется по MD5 и перекрёстно ссылается на список ранее отправленных хэшей файлов, хранящихся в файле в одном из трёх мест, поддерживающих разные версии Android. Будет использоваться первый существующий путь к каталогу: `/sdcard/Android/data/.google.index`, `/storage/emulated/0/Android/data/.google.index` или `storage/emulated/1/Android/data/.google.index`.

Эксфильтрация файла считается завершённой, когда сервер отправляет сообщение «Успех» в любом месте своего ответа. Для этой эксфильтрации используется POST протокола передачи гипертекста (HTTP), и ожидается, что ответ сервера также будет HTTP, но это явно не проверяется. 16 необработанных байтов MD5 добавляются в конец файла `google.index`, гарантируя, что один и тот же файл не будет отправлен несколько раз. Поскольку файл `google.index` содержит необработанные байты, без предварительного уведомления может показаться, что он содержит случайные данные. Начальный размер составляет 256 КБ, заполненный значениями NULL, что обеспечивает пространство для максимум 16 384 хэшей файлов. Все записи хэша будут проверены для каждого файла перед эксфильтрацией. Когда достигается конец файла `google.index`, позиция сбрасывается на начало, перезаписывая предыдущие хэши. Это означает, что, если количество файлов, подлежащих удалению с устройства, превысит 16 384, файлы будут отправлены несколько раз.

Компонент `netd` запускает таймеры о выполнении различных задач, включая утечку информации о файлах и устройствах. Этот процесс происходит каждые 86 000 секунд (приблизительно 23 часа, 53 минуты и 20 секунд), в течение которых вредоносная программа ищет в указанных каталогах файлы, соответствующие списку расширений, и собирает различную информацию о конфигурации оборудования устройства. Собранная информация хранится в каталоге `/data/local`, а затем удаляется.

#### F. Влияние и географический охват

Влияние Infamous Chisel на устройства Android значительно и приводит к потере конфиденциальной информации, нарушению конфиденциальности и потенциальному использованию устройства для дальнейших вредоносных действий.

Chisel в первую очередь нацелен на устройства Android, используемые военным сектором. Кампания была выявлена, когда о ней сообщили несколько организаций, в том числе Национальный центр кибербезопасности Великобритании (NCSC), Агентство национальной безопасности США (NSA), Агентство по кибербезопасности и инфраструктурной безопасности США (CISA), Федеральное бюро расследований США (ФБР), Национальный центр кибербезопасности Новой Зеландии (NCSC-NZ), Канадский центр кибербезопасности и Австралийское управление связи (ASD).

#### G. Пути заражения

Основываясь на возможностях и методах работы, описанных в документе, можно сделать вывод о некоторых потенциальных векторах заражения, которые использует столь сложная вредоносная кампания:

- **Фишинговые атаки.** могут использоваться методы фишинга, чтобы обманом заставить пользователей установить вредоносные приложения или перейти по ссылкам, ведущим к загрузке вредоносного ПО.
- **Использование уязвимостей.** Могут использоваться известные уязвимости в операционной системе Android или установленных приложениях для получения несанкционированного доступа и установки.
- **Социальная инженерия.** социальная инженерия используется, чтобы убедить пользователей предоставить разрешения или отключить функции безопасности, которые в противном случае помешали бы выполнению или закреплению вредоносного ПО.
- **Сторонние магазины приложений:** Chisel может распространяться через сторонние магазины приложений или веб-сайты, предлагающие заражённые версии оригинальных приложений.
- **Вредоносная реклама.** Вредоносная реклама может перенаправлять пользователей на веб-сайты, которые автоматически загружают и устанавливают вредоносное ПО на их устройства.
- **Целевой фишинг.** кампании целевого фишинга могут использоваться для заражения устройств конкретных лиц или организаций вредоносным ПО.
- **Chain-атаки.** взлом цепочек поставок ПО с целью внедрения в легитимные приложения.

#### H. Проактивные и реактивные меры

Подход к защите от таких сложных кампаний вредоносного ПО обычно включает в себя сочетание превентивных и реактивных мер кибербезопасности. Кроме того, получение информации о последних киберугрозах и

сотрудничество с агентствами по кибербезопасности и отраслевыми партнёрами могут повысить способность организации защищаться от таких угроз.

Проактивные меры включают в себя:

- **Осведомлённость:** обучение сотрудников рискам вредоносного ПО и важности соблюдения передовых методов обеспечения безопасности, таких как отказ от перехода по подозрительным ссылкам или загрузки непроверенных вложений.
- **Регулярные обновления программного обеспечения:** обеспечение актуальности всего ПО, включая ОС и приложения, с использованием новейших исправлений безопасности для устранения известных уязвимостей.
- **Надёжные антивирусные и антивирусные решения:** развёртывание комплексных антивирусных и вредоносных решений, которые могут обнаруживать и предотвращать выполнение вредоносного кода на устройствах организации.
- **Сетевая безопасность:** реализация мер сетевой безопасности, таких как брандмауэры, системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS), для мониторинга и контроля входящего и исходящего сетевого трафика на основе набора правил.
- **Контроль доступа:** обеспечение строгого контроля доступа и использование принципа наименьших привилегий, чтобы гарантировать, что пользователи имеют только доступ, необходимый для выполнения их рабочих функций.
- **Реагирование на инциденты:** разработка и поддержание плана реагирования на инциденты для быстрого и эффективного реагирования на потенциальные инциденты безопасности.

Реактивные меры включают в себя:

- **Обмен информацией об угрозах:** участие в обмене информацией об угрозах с другими организациями и агентствами по кибербезопасности, чтобы быть в курсе последних угроз и стратегий их устранения.
- **Мониторинг и обнаружение:** постоянный мониторинг систем на предмет признаков компрометации и наличие механизмов обнаружения для оповещения о подозрительных действиях.
- **Forensic анализ:** проведение forensic-анализа в случае нарушения безопасности для понимания масштабов компрометации, устранения угрозы и восстановления затронутых систем.
- **Регулярные проверки безопасности:** проведение регулярных проверок безопасности и оценок уязвимостей для выявления и устранения пробелов в безопасности в инфраструктуре организации.

- **Резервное копирование и восстановление:** регулярное резервное копирование важных данных и наличие плана аварийного восстановления для восстановления операций в случае атаки вредоносного ПО.

Меры для устройств Android:

- **Регулярное обновление:** регулярное обновление ОС Android и все установленные приложения, чтобы гарантировать устранение известных уязвимостей. Вредоносное ПО часто использует недостатки безопасности в устаревшем ПО.
- **Защитное ПО.** Применение антивирусных решений для устройств Android для обнаружения и удаления вредоносного ПО.
- **Неизвестные источники:** отключение установки приложений из неизвестных источников и использование доверенных магазинов приложений (например, Google Play Store).
- **Осторожность при работе со ссылками и вложениями.** Не следует переходить по ссылкам и загружать вложения из неизвестных т.к. фишинг – один из методов доступа.
- **Применение VPN.** При подключении к общедоступным сетям Wi-Fi следует использовать VPN для шифрования интернет-соединения и защиты от перехвата сети.
- **Применение двухфакторной аутентификации (2FA).** Использование 2FA для сетевых учётных записей добавит дополнительный уровень безопасности, что усложнит злоумышленникам доступ, даже если им удастся украсть учётные данные.
- **Мониторинг сетевого трафика.** мониторинг сетевого трафика на предмет необычной активности позволяет обнаружить наличие вредоносных программ. Внедрение сегментации сети, чтобы ограничить распространение вредоносного ПО.
- **Резервное копирование важных данных:** следует регулярно выполнять резервирование важных данных, хранящихся на устройстве. В случае заражения вредоносным ПО наличие резервных копий может предотвратить потерю данных.
- **Шифрование устройства:** использование шифрования устройства для защиты данных на устройстве. Это затрудняет злоумышленникам доступ к информации, если устройство взломано.
- **Ограничение разрешений приложений:** необходимо регулярно проверять и ограничивать разрешения, предоставленные приложениям. Ограничение разрешений может уменьшить объем данных, к которым может получить доступ приложение, тем самым ограничивая то, что может быть украдено вредоносным ПО.





XIII. **CYBER TOUFAN  
AL-AQSA**



*Аннотация – В этом документе представлен анализ хакерской группы Cyber Toufan Al-Aqsa, которая быстро приобрела известность благодаря кибератакам, нацеленным в первую очередь на израильские организации.*

*В анализе рассматриваются различные аспекты деятельности группы, включая её предысторию и возникновение, методы работы, заметные атаки и нарушения, предполагаемое государственное спонсорство и последствия её деятельности для специалистов по кибербезопасности и других специалистов в различных отраслях. Он также направлен на то, чтобы подчеркнуть его значительное влияние на практику кибербезопасности и более широкий геополитический ландшафт.*

*Анализ служит ценным ресурсом для профессионалов в области кибербезопасности, ИТ-специалистов и лидеров отрасли, предлагая понимание проблем и возможностей, связанных с меняющимся ландшафтом киберугроз.*

#### *A. Введение*

Cyber Toufan Al-Aqsa – хакерская группировка, возникшая в конце 2023 года и взявшая на себя ответственность за серию кибератак против израильских компаний и организаций.

Группа участвовала в различных типах кибератак, включая порчу веб-сайтов, несанкционированный доступ к учреждениям, предприятиям и частным резиденциям, взлом камер видеонаблюдения и утечку данных. Одна из атак была направлена против Signature-IT, израильской компании, специализирующейся на размещении международных веб-сайтов для бизнеса, в ходе которой удалось украсть примерно 16 гигабайт файлов данных. Также в фокусе внимания оказались Radware, фирма по кибербезопасности, Израильское управление инноваций и

Икеа в Израиле. Деятельность группы не ограничивалась утечкой данных; они также использовали домены корпоративной электронной почты своих жертв для распространения хактивистских сообщений. Некоторые даже предполагают потенциальную связь с Ираном из-за стиля и продемонстрированных в атаках возможностей.

#### *B. Последствия атак*

Деятельность группы привела к увеличению числа кибератак в Израиле на 20%, при этом количество атак на государственный сектор увеличилось более чем на 50%.

Операция поставила под угрозу более 150 целей, разбросанных по правительству, производству, электронной коммерции, кибербезопасности и другим секторам. Группировка утверждала, что уничтожила более 1000 серверов и нанесла удары по 150 израильским целям. Атаки не нанесли ущерба израильской экономике, но они нанесли большой ущерб, и некоторые компании до сих пор расплачиваются за это.

Потенциальное воздействие кибератак осложнилось продолжающимся конфликтом между Израилем и различными организациями, включая ХАМАС и связанные с Ираном группировки, т.к. привёл к увеличению числа атак, направленных против израильской инфраструктуры, предприятий и государственных структур.

Эти атаки были нацелены на сектора, включая госсектор, электронную коммерцию, водоснабжение, энергетику, судоходство, и телекоммуникации. В атаках использовались различные методы, такие как распределённые атаки типа "Отказ в обслуживании" (DDoS), атаки с порчей данных, утечки данных и использование учётных данных по умолчанию в критически важных системах.

Однако, несмотря на рост числа кибератак, Израиль, похоже, уверен в своей способности справиться с этими угрозами, противопоставляя имеющиеся в стране надёжную инфраструктуру кибербезопасности и богатую экосистему стартапов.

#### *C. Ключевые особенности атак*

Группировка "Toufan Al-AqsaCyber" использовала различные тактики для проведения кибератак

- **Порча веб-сайтов:** изменение внешнего вида веб-сайта, часто для отображения политического сообщения или демонстрации того, что сайт был скомпрометирован
- **Несанкционированный доступ:** несанкционированный доступ к различным учреждениям, предприятиям и частным резиденциям. Это может быть связано с использованием уязвимостей в программном обеспечении, использованием фишинговых методов для кражи учётных данных для входа или других методов обхода мер безопасности
- **Компрометация камер наблюдения:** компрометация камер видеонаблюдения

потенциально позволяет отслеживать действия своих целей

- **Утечка данных:** группа умело извлекает большие объёмы данных из объектов, которые затем размещают публично. Это не только наносит ущерб целевым организациям, но и потенциально влияет на отдельных лиц, чья личная информация может быть включена во взломанные данные
- **Использование платформ социальных сетей:** группа активна на платформах социальных сетей, таких как Twitter и Telegram, где они распространяют информацию о своей деятельности и потенциально координируют атаки
- **Вредоносное ПО wiper:** Группа использовала вредоносное ПО wiper в своих атаках, которое предназначено для удаления данных или нарушения работы систем
- **Психологическая война:** группа выпустила публикации, оправдывающие их кибератаки на Израиль, ссылаясь на возмездие за те вещи, что они считают израильской жестокостью и преступлениями
- **Последующие атаки:** после первоначальных взломов группа проводит последующие атаки, потенциально используя скомпрометированные системы для дальнейшего проникновения в сеть цели или для атаки на другие связанные системы

#### D. Цели и последствия

Цели кибер-атак были весьма разнообразными:

- **Правительственные структуры:** Группа поставила под угрозу цели, разбросанные по всему израильскому правительственному сектору
- **Промышленность:** Производственные фирмы оказались в числе пострадавших секторов
- **Электронная коммерция:** под прицелом оказались платформы онлайн-торговли и предприятия, которые могут включать данные клиентов и информацию о деловых транзакциях
- **Фирмы по кибербезопасности:** группа атаковала компании по кибербезопасности, такие как Radware, что указывает на сосредоточенность на организациях, которые являются неотъемлемой частью кибер-защиты Израиля

#### 1) Государственные структуры

Последствия атак на государственные структуры:

- **Утечка данных:** Группа успешно взломала несколько государственных структур, что привело к существенной утечке данных. Это не только ставит под угрозу безопасность и конфиденциальность затронутых организаций, но и потенциально влияет на отдельных лиц, чья личная информация может быть включена во взломанные данные

- **Нарушение работы служб:** Атаки привели к нарушению работы служб, что повлияло на нормальное функционирование целевых правительственных организаций
- **Ущерб репутации:** публичный характер этих атак и последующие утечки данных могут нанести ущерб репутации целевых организаций, подорвав общественное доверие
- **Возможность последующих атак:** Первоначальные нарушения потенциально могут быть использованы для проведения последующих атак, используя скомпрометированные системы для дальнейшего проникновения в сеть цели или для атаки на другие связанные системы
- **Психологическое воздействие:** Атаки служат формой цифровой психологической войны, создавая атмосферу страха и неуверенности
- **Экономический эффект:** Атаки могут иметь экономические последствия, включая затраты, связанные с реагированием на инциденты, восстановлением системы, а также потенциальные штрафы регулирующих органов или судебные иски, связанные с утечками данных
- **Проблемы национальной безопасности:** Учитывая конфиденциальный характер государственных структур, эти атаки потенциально могут представлять угрозу национальной безопасности, в зависимости от характера взломанных данных и затронутых систем

#### 2) Производство

Последствия кибератак на производственный сектор:

- **Сбои в работе:** Кибератаки, особенно программы-вымогатели, могут привести к остановке производственных линий, что приведёт к значительным сбоям в работе. Это может вынудить производителей переводить свои физические системы в автономный режим, иногда на длительные периоды, чтобы смягчить последствия атаки и восстановить нормальную работу
- **Финансовые потери:** Финансовые последствия кибератак для производителей существенны. Сообщалось, что средняя стоимость утечки данных в производственном секторе в 2022 году составила 4,47 миллиона долларов, что больше, чем годом ранее. Эти затраты включают расследование, устранение последствий и реагирование на кибератаки, а также потенциальные убытки от остановки производства и продаж
- **Утечка данных и кража интеллектуальной собственности:** Кибератаки могут привести к краже конфиденциальных данных, включая интеллектуальную собственность, коммерческие секреты и информацию о клиентах. Это не только влечёт за собой немедленные финансовые

последствия, но и может привести к долгосрочным недостаткам в конкурентной борьбе

- **Уязвимости цепочки поставок:** взаимосвязанный характер производственной цепочки поставок означает, что атака на одного производителя может иметь волновой эффект, затрагивающий поставщиков, партнёров и заказчиков. Атаки на цепочки поставок могут поставить под угрозу целостность продуктов и услуг, что приводит к более широким проблемам безопасности
- **Ущерб репутации:** Публичное раскрытие факта атаки может подорвать доверие к производителю, повлиять на отношения с клиентами и потенциально привести к потере бизнеса. Ущерб, нанесённый репутации компании, может быть, одним из самых сложных последствий, после которого приходится восстанавливаться
- **Комплаенс и юридические риски:** Производителям могут грозить штрафы регулирующих органов и судебные иски, если кибератаки приведут к потере защищённых или конфиденциальных данных. Это особенно актуально для производителей в отраслях с высоким уровнем регулирования или для тех, кто обрабатывает личные данные
- **Физический ущерб и риски для безопасности:** В случаях, когда целью являются операционные технологические системы (ОТ), кибератаки могут привести к физическому повреждению оборудования и создать угрозу безопасности для сотрудников. Манипулирование производственными процессами может привести к выходу из строя оборудования, нанесению ущерба окружающей среде и даже поставить под угрозу жизни людей
- **Психологическая война:** помимо ощутимых последствий, кибератаки могут также служить формой психологической войны, создавая атмосферу страха и неуверенности среди сотрудников, руководства и заинтересованных сторон

### 3) *Электронная коммерция*

Последствия атак на сектор электронной коммерции:

- **Операционные сбои:** Кибератаки могут серьёзно нарушить работу предприятий электронной коммерции, повлияв на их способность обрабатывать транзакции и обслуживать клиентов. Эти сбои могут привести к простоям, что напрямую влияет на продажи и доставку
- **Финансовые потери:** Финансовые последствия кибератак на предприятия электронной коммерции могут быть существенными. Сюда входят прямые затраты, связанные с расследованием, устранением последствий и реагированием на атаки, а также косвенные затраты, такие как потеря продаж во

время простоя. Средняя стоимость утечки данных в 2022 году достигла 4,35 миллиона долларов, что подчёркивает значительную финансовую нагрузку, которую могут налагать эти инциденты

- **Утечка данных и потеря конфиденциальной информации:** Платформы электронной коммерции часто хранят большие объёмы личных и финансовых данных. Атаки могут привести к утечке данных, раскрывая конфиденциальную информацию клиентов, такую как данные кредитной карты, адреса и личную идентификационную информацию. Это не только нарушает конфиденциальность клиентов, но и подвергает бизнес санкциям регулирующих органов и судебным искам
- **Ущерб репутации и доверию клиентов:** Публичное раскрытие кибератаки может нанести значительный ущерб репутации бизнеса электронной коммерции, что приведёт к потере доверия клиентов. Восстановление такого доверия может быть долгим и сложным процессом, и некоторые предприятия, возможно, никогда полностью не восстановятся
- **Риски регулирования и соблюдения требований:** Предприятия электронной коммерции подчиняются различным нормативным актам и стандартам соответствия, связанным с защитой данных и конфиденциальностью. Кибератаки, приводящие к утечке данных, могут привести к несоблюдению требований, что влечёт за собой значительные штрафы и пени
- **Увеличение затрат на кибербезопасность:** после кибератаки предприятиям электронной коммерции часто приходится вкладывать значительные средства в улучшение своей системы кибербезопасности. Это включает в себя внедрение новых технологий, наем дополнительного персонала службы безопасности и внедрение более строгих мер безопасности. Эти возросшие издержки могут повлиять на прибыль бизнеса и могут быть переданы потребителям в виде более высоких цен
- **Уязвимости цепочки поставок:** Предприятия электронной коммерции являются частью более крупной цифровой и физической цепочки поставок. Кибератаки на одну платформу электронной коммерции могут иметь волновой эффект, затрагивающий поставщиков, партнёров и клиентов. Эта взаимосвязанность может усилить последствия атаки, затрагивая более широкую экосистему

### 4) *Фирмы по Кибербезопасности*

Последствия атак на ИБ-компании:

- **Операционные сбои:** Фирмы, занимающиеся вопросами кибербезопасности, как и любой другой бизнес, могут сталкиваться с операционными сбоями в результате кибератак. Это может повлиять

на их способность обслуживать клиентов и выполнять повседневные операции, потенциально приводя к временному сокращению услуг безопасности, которые они предоставляют

- **Финансовые потери:** Финансовые последствия для компаний, занимающихся кибербезопасностью, могут быть существенными, включая затраты на расследование, устранение последствий и реагирование на атаки. Кроме того, возможны финансовые потери из-за простоя в работе и потенциальных требований о компенсации от пострадавших клиентов
- **Утечки данных и кража интеллектуальной собственности:** Фирмы, занимающиеся вопросами кибербезопасности, часто владеют конфиденциальными данными, включая запатентованные инструменты и методы обеспечения безопасности, а также информацией о клиентах. Нарушение может привести к потере интеллектуальной собственности и конфиденциальных клиентских данных, подрывая конкурентные позиции фирмы и доверие клиентов
- **Ущерб репутации:** возможно, в большей степени, чем в других отраслях, кибератака на фирму, занимающуюся вопросами кибербезопасности, может нанести значительный ущерб её репутации. Клиенты ожидают, что эти фирмы будут наиболее безопасными, и взлом может привести к потере доверия, что затруднит удержание и привлечение клиентов
- **Регуляторные риски и риски соответствия требованиям:** Фирмы, занимающиеся кибербезопасностью, подчиняются строгим нормативным требованиям. Кибератака, приводящая к утечке данных, может привести к проблемам с соблюдением требований, штрафам и судебным действиям
- **Увеличение затрат на кибербезопасность:** после атаки фирме, занимающейся кибербезопасностью, вероятно, потребуется вложить значительные средства в укрепление своей защиты. Это может включать внедрение новых технологий, наем дополнительного персонала и внедрение более строгих мер безопасности, все из которых могут быть дорогостоящими
- **Уязвимости в цепочке поставок:** Фирмы, занимающиеся кибербезопасностью, являются частью более крупной цифровой экосистемы. Атака на одну фирму может иметь волновые эффекты, потенциально ставя под угрозу безопасность клиентов и партнеров
- **Психологическое воздействие и потеря морального духа:** Кибератаки могут создать атмосферу страха и неуверенности среди сотрудников и руководства. Для фирмы, занимающейся кибербезопасностью, стать жертвой атаки также может привести к падению морального духа, поскольку это напрямую ставит под угрозу основную миссию организации



xiv. **MALLOX**

**RANSOMWARE**



*Аннотация – В этом документе представлен анализ группы вымогателей Mallox, которая быстро развивалась с момента своего первого выявления в июне 2021 года.*

*Анализ посвящён различным аспектам деятельности группы, включая её отличительную практику добавления названий целевых организаций к зашифрованным файлам, эволюцию её алгоритмов шифрования и тактику обеспечения постоянства и обхода средств защиты.*

*Выводы, полученные в результате этого анализа, имеют решающее значение для разработки стратегий защиты и повышения готовности к таким развивающимся киберугрозам.*

#### *A. Вредоносное ПО и тактика предотвращения обнаружения*

Ransomware-группа TargetCompany, или Mallox, известна своими целенаправленными атаками программ-вымогателей, в первую очередь нацеленными на незащищенные серверы Microsoft SQL, работающие в Интернете. Программа-вымогатель шифрует данные жертв и требует выкуп, как правило, в криптовалюте, за ключ расшифровки.

Группа добавила в свой арсенал такие инструменты, как Remcos RAT, BatCloak и Metasploit, демонстрирующие передовые методы обфускации, позволяющие избежать обнаружения. Они используют полностью необнаруживаемые программы-обфускаторы (FUD) для шифрования своих программ-вымогателей, что затрудняет обнаружение и блокировку вредоносного ПО. Также – сбор конфиденциальных данных с использованием таких инструментов, как MIMIKATZ, и выполнение атак с помощью Trojan.BAT.TARGETCOMP\*. Они также используют методы предотвращения обнаружения, такие как GMER, расширенное завершение процесса и YDark

#### *B. Смягчение последствий и дешифрование*

Mallox добавляет уникальное расширение зашифрованного файла к именам файлов целевой организации. Было замечено, что для поддержания работоспособности заражённой системы следует избегать шифрования определённых папок и типов файлов. Программа-вымогатель помещает записку в каждый каталог на диске жертвы, содержащий инструкции по оплате

Компания Avast выпустила бесплатные дешифраторы для программ-вымогателей TargetCompany, которые при определённых обстоятельствах могут расшифровывать файлы. Важно отметить, что выплата выкупа не гарантирует, что злоумышленники предоставят ключ дешифрования, и это может стимулировать дальнейшую преступную деятельность

#### *C. Программа-вымогатель как услуга (RaaS)*

Mallox работает по модели RaaS, используя подпольные форумы для рекламы своих услуг. Группа поддерживает сайт на базе TOR, где публикует объявления о недавно скомпрометированных данных

##### *1) Распространение*

Mallox, распространяется различными способами. Программа-вымогатель в первую очередь нацелена на компании, а не на отдельных пользователей.

Одним из первоначальных методов доступа является фишинг, при котором для получения доступа к системе жертвы используются вредоносные файлы Microsoft OneNote. Другой метод заключается в атаках методом перебора на серверы Microsoft SQL, т.е. недостаточно защищённые серверы MS-SQL, используя атаки по словарю в качестве точки входа для проникновения в сети жертв.

Оказавшись внутри системы, программа-вымогатель использует команду PowerShell для извлечения полезной нагрузки программы-вымогателя с удалённого сервера. Полезная нагрузка пытается остановить и устранить службы, связанные с SQL, удалить теньные копии томов, очистить журналы системных событий и завершить процессы, связанные с безопасностью. После этих шагов он инициирует процесс шифрования и впоследствии оставляет записку с требованием выкупа в каждом каталоге.

Программа-вымогатель также собирает системную информацию и передаёт её на C2C-сервер. Программа-вымогатель шифрует файлы жертвы с помощью алгоритма шифрования ChaCha20 и генерирует ключ шифрования с использованием ECDH, примера криптографии с эллиптическими кривыми, и AES-128. К зашифрованным файлам добавляются расширения, которые соответствуют названию затронутой компании.

##### *2) Симптомы атаки вымогателей на целевую компанию*

Симптомы атаки могут варьироваться в зависимости от конкретного варианта программы-вымогателя и тактики, однако общие признаки включают:

- **Невозможность доступа к файлам:** наиболее заметным симптомом атаки программ-вымогателей является невозможность открыть файлы, хранящиеся на компьютере, или получить к ним доступ. Файлы зашифрованы и их расширения изменены на название затронутой компании, такое как ".artiis", ".brg", ".mallox", ".architek", ".tohnichi", ".hertco" и другие
  - **Повышенная активность процессора и диска:** Повышенная активность диска или основного процессора может указывать на то, что программа-вымогатель работает в фоновом режиме
  - **Записка с требованием выкупа:** после процесса шифрования программа-вымогатель оставляет в каждом каталоге записку с требованием выкупа, озаглавленную "How to decrypt files.txt" или "RECOVERY FILES.txt". Это примечание обычно содержит инструкции о том, как заплатить выкуп, чтобы получить ключ расшифровки
  - **Сетевые аномалии:** используется сканирование сети для сбора информации о сетевом подключении, что может привести к необычной активности в сети
  - **Завершение определённых процессов и служб:** Программа-вымогатель пытается остановить и устранить службы, связанные с SQL, удалить теньевые копии томов, очистить журналы системных событий и завершить процессы, связанные с безопасностью
- 3) *Методология*
- **Первоначальный доступ:** Группа часто получает первоначальный доступ к системам жертв с помощью фишинговых кампаний, в которых задействованы вредоносные файлы OneNote. Они также используют слабые SQL-серверы на начальном этапе развёртывания
  - **Выполнение:** Полезная нагрузка программы-вымогателя выполняется с использованием различных методов. Например, группа внедряет исполняемый файл программы-вымогателя в AppLaunch.exe. Они также используют командные строки и PowerShell для загрузки полезной нагрузки программы-вымогателя с удалённого сервера
  - **Постоянство:** Группа стремится к постоянству с помощью различных методов, включая изменение URL-адресов или путей до тех пор, пока выполнение Remcos RAT (вредоносное ПО удалённого доступа) не завершится успешно
  - **Предотвращения обнаружения:** Группа использует полностью необнаруживаемые упаковщики-обфускаторы (FUD), чтобы избежать обнаружения решениями безопасности. Они также удаляют разделы реестра и теньевые копии, чтобы повредить службам восстановления
- **Повышение привилегий:** присваивает своему процессу привилегии SeTakeOwnershipPrivilege и SeDebugPrivilege, чтобы облегчить свою собственную вредоносную работу
  - **Обнаружение:** используется сканирование сети
  - **Сбор:** Группа использует такие инструменты, как MIMIKATZ, для сбора данных
  - **Командование и контроль (C&C):** Группа устанавливает соединение с сервером C&C с помощью "ap.php" точки
  - **Шифрование:** Программа-вымогатель получает маски всех логических дисков в системе, используя GetLogicalDrives() Win32 API. Тип каждого диска проверяется с помощью GetDriveType(). Если этот диск действителен (стационарный, съёмный или сетевой), шифрование диска продолжается
  - **Воздействие:** после шифрования программа-вымогатель оставляет записку с требованием выкупа. Группа использует метод двойного вымогательства, угрожая утечкой украденных данных, если выкуп не будет выплачен
- 4) *Точки входа и Способы доставки*
- Атаки программ-вымогателей могут проникать в систему через различные точки входа:
- **Скомпрометированные учётные данные:** украденные или скомпрометированные учётные данные – это может произойти, когда сотрудники становятся жертвами фишинговых атак или когда учётные данные приобретаются в тёмной Сети
  - **Неуправляемые устройства или принесите своё собственное устройство (BYOD):** Неуправляемые устройства или персональные устройства, используемые в рабочих целях, могут стать точкой входа для программ-вымогателей, если они не защищены должным образом
  - **Приложения с уязвимостями, подключённые к Интернету:** Уязвимости в приложениях, подключённых к Интернету, могут быть использованы злоумышленниками для получения доступа к сети. Сюда входят такие приложения, как VPN SSL, серверы Microsoft Exchange и веб-интерфейсы на основе пользовательского интерфейса Telerik
  - **Фишинг:** Фишинговые атаки часто нацелены на конечных пользователей, обманом заставляя их раскрывать конфиденциальную информацию или загружать вредоносное программное обеспечение. Сотрудники играют жизненно важную роль в защите от этой угрозы, поэтому организациям крайне важно инвестировать в обучение своих сотрудников навыкам распознавания попыток фишинга и предотвращения таких попыток



- **Заражённые программные пакеты или исправления:** Скомпрометированные исправления или программные пакеты могут стать точками входа для преступников-вымогателей. Эта тактика основана на том факте, что пользователи часто быстро загружают и устанавливают обновления для обеспечения безопасности своих систем, непреднамеренно позволяя вымогателям проникать
- **Атаки методом "грубой силы" на внешние шлюзы:** Киберпреступники все чаще используют такие методы, как атаки методом "грубой силы", для получения доступа к системам. Это включает в себя систематическое перебирание всех возможных комбинаций паролей до тех пор, пока не будет найден правильный
- **Протокол удалённого рабочего стола (RDP) и злоупотребление учётными данными:** Злоумышленники часто используют уязвимости в удалённых службах, таких как RDP или VPN-серверы. Они могут прибегать к фишинговым действиям, чтобы завладеть учётными данными, или использовать дампы учётных данных, доступные на форумах dark web
- **Электронная почта:** Электронная почта является распространённой точкой входа для атак программ-вымогателей. Злоумышленники часто прикрепляют к электронным письмам вредоносные файлы. Когда ничего не подозревающие жертвы открывают эти документы, выполняются макросы, запускающие полезную нагрузку программы-вымогателя

Mallox, использует различные точки входа для проникновения в системы:

- **Бэкдор Remcos:** Группа использует бэкдор Remcos в качестве начальной точки доступа. Remcos - который позволяет злоумышленникам удалённо управлять заражённой системой
- **Незащищённые серверы Microsoft SQL:** Группа нацелена на незащищённые серверы Microsoft SQL, используя их в качестве точек входа в инфраструктуру ИКТ жертв
- **BatLoader:** Группа использует BatLoader для запуска полезных программ-вымогателей. BatLoader – это вредоносное ПО, которое загружает и устанавливает дополнительные вредоносные программы в заражённую систему
- **Сканирование сети:** Группа использует сканирование сети в качестве метода обнаружения для выявления потенциальных целей в сети
- **Trojan.BAT.TARGETCOMP:** Это вредоносная программа, используемая группой для выполнения. Он предназначен для того, чтобы поставить под угрозу безопасность заражённой системы
- **GMER:** Группа использует GMER, детектор и средство для удаления руткитов, для

предотвращения обнаружения. Это позволяет группе скрывать свои действия и закрепляться в заражённой системе

#### *a) Точки входа в отрасли*

##### **Промышленное производство:**

- **Промышленные системы управления (ICS) и устройства промышленного Интернета вещей (IIoT):** уязвимости в этих системах используются для нарушения операций на производстве
- **Атаки на цепочку поставок:** Компрометация цепочки поставок, включая сторонних поставщиков, может стать отправной точкой для программ-вымогателей

##### **Розничная торговля**

- **Системы торговых точек (POS):** Вредоносное ПО может заразить эти системы для кражи информации о кредитной / дебетовой карте
- **Серверы Microsoft SQL:** нацелены на незащищённые серверы MS-SQL, используемые в розничных операциях

##### **Телекоммуникации**

- **Уязвимости удалённого выполнения кода (RCE):** Использование уязвимостей, таких как CVE-2019-1069 и CVE-2020-0618, для выполнения произвольного кода
- **Серверы Microsoft SQL:** использование функции xp\_cmdshell в Microsoft SQL для удалённого выполнения

##### **Бизнес-услуги**

- **Устаревшие и не исправленные системы:** использование устаревших систем облегчает получение преступниками доступа
- **Функциональная зависимость от ИТ:** невозможность работать без ИТ стимулирует быстрые выплаты выкупа.

##### **Здравоохранение**

- **Фишинг и социальная инженерия:** использование ложных электронных писем для обмана медицинского персонала с целью установки программ-вымогателей
- **Скомпрометированные учётные данные:** использование украденных учётных данных для доступа к сетям здравоохранения

##### **Финансы**

- **Атаки на доступ к серверу и неправильные настройки:** использование уязвимостей сервера и ошибок конфигурации

- **Фишинг и кража учётных данных:** нацелены на ценные аккаунты, такие как аккаунты генеральных директоров и CFOs

#### Госсектор

- **Фишинг и социальная инженерия:** использование ложных электронных писем для обмана государственных служащих
- **Программа-вымогатель как услуга (RaaS):** использование моделей RaaS для нацеливания на государственные организации

#### Образование

- **Фишинг и социальная инженерия:** использование ложных электронных писем для обмана педагогического персонала и студентов
- **Скомпрометированные учётные данные:** использование украденных учётных данных для доступа к образовательным сетям

#### Информационные технологии

- **Эксплойты уязвимостей ПО:** Использование известных уязвимостей в ИТ-инфраструктуре
- **Учётные записи:** получение доступа к ИТ-системам через скомпрометированные учётные записи

#### Транспорт

- **Фишинг и социальная инженерия:** нацеливание сотрудников на фишинговые электронные письма с целью получения доступа к сети
- **Скомпрометированные учётные данные:** использование украденных учётных данных для доступа к транспортным сетям

#### D. География и отраслевые цели

В поле зрения Mallox попали компании различных размеров, в т.ч. малый и средний бизнес. В 37% компаний, пострадавших от программ-вымогателей, работало менее 100 сотрудников, а 82% атак программ-вымогателей в 2021 году были направлены против компаний с численностью менее 1000 сотрудников. В то время как доля крупных организаций была выше в первом полугодии 2022 года, доля малых и средних организаций была выше в первом полугодии 2023 года, что указывает на тенденцию к увеличению числа целевых показателей малого и среднего бизнеса. Средний размер целевой компании, подвергшейся атаке вымогателей, составил 275 сотрудников, что на 10% больше, чем в предыдущем квартале

Группа в первую очередь нацелена на предприятия в Азиатско-Тихоокеанском регионе, за которыми следуют Европа и Ближний Восток (США, Индия, Саудовская Аравия, Канада, Германия, Австралия, Бразилия, Болгария, Китай, Вьетнам) и проявила интерес к организациям, работающим в промышленных отраслях, госсекторе, отраслях образования, розничной торговли, ИТ,

здравоохранение, бизнес-услуг, телекоммуникаций, финансовой автомобильной и транспортной отрасли

#### 1) Промышленное производство

В этом секторе атаки программ-вымогателей часто используют уязвимости в промышленных системах управления (ICS) и устройствах промышленного Интернета вещей (IIoT). Эти системы являются неотъемлемой частью производственных операций, и их компрометация может привести к значительным сбоям.

Эти атаки выходят за рамки непосредственных финансовых потерь, приводя к значительным затратам на реагирование на нарушения, возможному контакту с третьими сторонами, уменьшению доли рынка и нанесению ущерба корпоративной репутации. В некоторых случаях злоумышленники могут также потребовать выкуп в обмен на разрешение компании восстановить доступ к своим компьютерным системам. Более того, атаки программ-вымогателей могут привести к потере конфиденциальной и личной информации, что может иметь долгосрочные последствия для затронутых компаний и их клиентов

#### Сбой в работе

Атаки нарушают производственные операции, часто приводя к существенным потерям в производстве и разрозненным операциям. Когда программа-вымогатель выводит из строя производство, операции могут быть приостановлены на несколько дней или недель, что приводит к финансовым потерям, остановке производственных линий, что означало невозможность выполнения заказов клиентов.

#### Финансовые последствия

Финансовые последствия атак программ-вымогателей на производственный сектор огромны. В период с 2018 по 2023 год 478 производственных компаний подверглись атаке программ-вымогателей, что привело к потере примерно 46,2 миллиарда долларов только из-за простоев. Затраты на простой значительны, поскольку это сказывается на повседневной работе, а производственные линии иногда останавливаются.

#### Репутационный ущерб

Атаки также могут нанести значительный репутационный ущерб, который может быть длительным и иногда приводить к тому, что бизнес так и не оправится от репутационных последствий.

#### Проблемы конфиденциальности

Утечка данных является распространённым следствием атак программ-вымогателей. В 32% атак злоумышленники не только шифровали данные, но и крали их. В результате этих атак было взломано более 7,5 миллионов индивидуальных записей.

#### Правовые и нормативные последствия

Атаки программ-вымогателей могут иметь правовые и нормативные последствия, особенно когда они приводят к утечке данных. Компаниям могут грозить штрафы за

неспособность должным образом защитить данные клиентов, и они также могут столкнуться с судебными исками от клиентов или деловых партнёров, пострадавших от нарушения.

### Долгосрочные эффекты

Долгосрочные последствия атак программ-вымогателей могут включать незапланированное сокращение персонала и даже полное закрытие бизнеса. В некоторых случаях атаки программ-вымогателей приводили к тому, что компании просили передать их в конкурсное управление с сокращением рабочих мест.

### Повышенная частота атак

В 2023 году производственный сектор пострадал сильнее всего, что свидетельствует о значительных уязвимостях в этом секторе. Количество атак на производственные предприятия также выросло примерно на 107% по сравнению с предыдущим годом

#### 2) Розничная торговля

В сфере розничной торговли одной из распространённых точек входа для атак программ-вымогателей являются системы торговых точек (POS). Злоумышленники часто используют вредоносное ПО для заражения этих систем и кражи информации о кредитных / дебетовых картах. Кроме того, были замечены группы программ-вымогателей, нацеленные на серверы Microsoft SQL (MS-SQL), которые часто используются в операциях розничной торговли, и атакующие их

Атаки могут нанести ущерб розничному бизнесу, что приведёт к прямым финансовым потерям, остановкам в работе, долгосрочному ущербу репутации и юридическим последствиям. Зависимость сектора розничной торговли от цифровых систем и обработки конфиденциальных данных клиентов делает его прибыльной мишенью для атак.

### Сбой в работе

- **Потеря продаж:** атака может привести к упущенным возможностям для продаж, особенно в пиковые сезоны
- **Непрерывность бизнеса:** атаки могут нарушать критически важные бизнес-операции, предотвращая или ограничивая доступ к системам продаж
- **Время простоя:** даже несколько часов простоя интернет-магазина могут иметь огромные финансовые последствия, и потерей клиентов

### Финансовые последствия

- **Потеря доходов:** Организации розничной торговли сообщают о значительной потере доходов в результате атак программ-вымогателей
- **Выплаты выкупа:** Розничные торговцы могут чувствовать себя вынужденными платить выкупы, особенно в периоды высоких продаж, и доля розничных организаций, выплачивающих более высокие выкупы, увеличилась

- **Затраты на восстановление:** у розничных продавцов-жертв, которые платят выкуп, средние затраты на восстановление в четыре раза выше, чем у тех, которые этого не делают

### Репутационный ущерб

- **Доверие клиентов:** атаки подрывают доверие клиентов, особенно в случаях, когда личная информация была скомпрометирована
- **Ущерб бренду:** Восприятие "небезопасного" бизнеса может нанести больший ущерб, чем непосредственные финансовые потери, и повлиять на репутацию розничного продавца
- **Общественное мнение:** Успешные атаки могут рассматриваться как признак слабых методов обеспечения безопасности, что вынуждает клиентов вести бизнес в другом месте

### Утечка данных

- **Конфиденциальная информация:** Розничные продавцы обрабатывают данные кредитных карт и личную информацию, которая может быть раскрыта в результате атаки программ-вымогателей
- **Утечки данных:** атаки представляют значительный риск утечки данных, что может привести к потере доверия потребителей

### Влияние на сотрудников

- **Увольнения:** половина розничных продавцов столкнулись с увольнениями сотрудников после того, как стали жертвами программ-вымогателей
- **Приостановление деятельности:** трети розничных торговцев пришлось временно приостановить или приостановить свою деятельность

### Риски, связанные с цепочкой поставок и третьими сторонами

- **Цепочки поставок:** злоумышленники могут заразить многие организации, нацеливаясь на конкретных поставщиков
- **Зависимость от сторонних производителей:** Розничные продавцы зависят от сторонних производителей, которые могут создавать ИБ-риски

### Правовые и нормативные последствия

Розничные продавцы могут столкнуться с юридическими последствиями в случае компрометации данных клиентов, включая штрафы за несоблюдение правил защиты данных.

#### 3) Телекоммуникации

В телекоммуникационной отрасли для атак используют уязвимости удалённого выполнения кода (RCE), такие как CVE-2019-1069 и CVE-2020-0618, которые позволяют злоумышленникам выполнять произвольный код.

Злоумышленники также могут использовать удалённое выполнение с помощью функции `xp_cmdshell` в MS SQL

Атаки могут нанести ущерб телекоммуникационному бизнесу, что приведёт к прямым финансовым потерям, остановкам в работе, долгосрочному репутационному ущербу и юридическим последствиям.

#### Сбой в работе

- **Прерывание обслуживания:** атаки нарушают работу телекоммуникационных служб, затрагивая индивидуальные и корпоративные коммуникации
- **Проникновение в сеть:** созависимый характер телекоммуникационных сетей увеличивает риск проникновения, потенциально обеспечивая доступ через различные подключённые системы

#### Финансовые последствия

- **Потеря доходов:** атака может серьёзно повлиять на операционную способность организации, приведя к снижению доходов или полной остановке операций на время восстановления
- **Выплаты выкупа и затраты на восстановление:** компании могут столкнуться со значительными расходами, связанными с выплатами выкупа, усилиями по восстановлению, судебными издержками и другими сопутствующими расходами

#### Репутационный ущерб

- **Доверие клиентов:** успешная атака может нанести ущерб репутации телекоммуникационной компании из-за предполагаемых слабых методов обеспечения безопасности.
- **Ущерб бренду:** восприятие "небезопасного" бизнеса может нанести больший ущерб, чем немедленные финансовые потери

#### Проблемы конфиденциальности

- **Раскрытие конфиденциальных данных:** телекоммуникационные компании хранят обширные данные о клиентах, и атаки программ-вымогателей могут привести к утечке конфиденциальных данных
- **Двойное вымогательство:** злоумышленники могут угрожать разглашением конфиденциальных данных организации, если выкуп не будет выплачен, что приводит к атакам с двойным вымогательством

#### Правовые и нормативные последствия

- **Нарушения комплаенса:** Компании могут столкнуться с юридическими последствиями в случае компрометации данных клиентов, включая штрафы и неустойки за несоблюдение правил защиты данных

**Риски, связанные с цепочкой поставок и третьими сторонами**

- **Атаки на цепочки поставок:** злоумышленники могут заразить многие организации, нацеливаясь на поставщиков
- **Зависимость от сторонних производителей:** телекоммуникационные компании полагаются на расширенные цепочки поставок и зависимости от сторонних производителей, которые могут создавать риски кибербезопасности

#### Кража интеллектуальной собственности

Ценная интеллектуальная собственность телеком компаний находится под угрозой кражи или компрометации, что потенциально наносит ущерб конкурентным преимуществам и инновационным усилиям

#### Долгосрочный шпионаж

Некоторые атаки на операторов связи проводятся высокоразвитыми группами угроз, нацеленными на долгосрочный шпионаж

#### 4) Транспорт

Атаки могут нанести ущерб транспортному сектору, что приведёт к прямым финансовым потерям, остановкам в работе, долгосрочному репутационному ущербу и юридическим последствиям.

#### Сбой в работе

- **Остановка производства:** Атаки могут привести к остановке заводов-производителей, вызывая задержки в производстве и доставке
- **Уязвимость цепочки поставок:** цепочка поставок сложна и взаимосвязана, что делает её уязвимой для атак, которые могут иметь каскадный эффект

#### Финансовые последствия

- **Выплаты выкупа:** были зафиксированы одни из самых высоких выплат за вымогательство: промышленные компании потратили в 2019 году 6,9 миллиона долларов, что составило 62% от всех выплат за вымогательство
- **Потеря доходов:** атаки могут серьёзно повлиять на операционную способность организаций, приводя к снижению доходов или полной остановке операций на время восстановления

#### Репутационный ущерб

- **Доверие клиентов:** успешные атаки могут нанести ущерб репутации автомобильных компаний, вынуждая клиентов вести бизнес в других местах из-за предполагаемых слабых методов обеспечения безопасности
- **Ущерб бренду:** восприятие "небезопасного" бизнеса может нанести больший ущерб, чем немедленные финансовые потери

#### Проблемы конфиденциальности

- **Раскрытие конфиденциальных данных:** компании хранят обширные данные о клиентах, и атаки программ-вымогателей могут привести к утечке конфиденциальных данных
- **Двойное вымогательство:** злоумышленники могут угрожать разглашением конфиденциальных данных организации, если выкуп не будет выплачен, что приводит к атакам с двойным вымогательством
- **Доверие клиентов:** атака может серьезно повредить репутации компании, в результате чего клиенты потеряют доверие и, возможно, перенесут свой бизнес в другое место
- **Ущерб бренду:** восприятие неадекватных мер безопасности может запятнать имидж бренда, влияя на долгосрочные перспективы бизнеса

#### Правовые и нормативные последствия

Компании могут столкнуться с юридическими последствиями в случае компрометации данных клиентов, включая штрафы и неустойки за несоблюдение правил защиты данных

#### Кража интеллектуальной собственности

Интеллектуальная собственность автомобильных компаний находится под угрозой кражи или компрометации, что потенциально наносит ущерб конкурентным преимуществам и инновационным усилиям

#### Долгосрочный шпионаж

Некоторые атаки на поставщиков автомобильных услуг проводятся высокоразвитыми группами угроз, нацеленными на долгосрочный шпионаж

##### 5) Бизнес-услуги

Атаки программ-вымогателей могут нанести ущерб бизнесу в сфере услуг, что приведёт к прямым финансовым потерям, остановкам в работе, долгосрочному ущербу репутации и юридическим последствиям.

#### Сбой в работе

- **Время простоя:** атаки могут привести к остановке операций, что приведёт к значительному простоем и нарушению деловой активности
- **Потеря бизнеса:** если важные файлы зашифрованы, предприятия могут оказаться неспособными работать, что приведёт к потере доходов

#### Финансовые последствия

- **Выплаты выкупа:** Предприятия могут почувствовать необходимость заплатить выкуп, чтобы быстро восстановить доступ к своим данным, особенно если резервные копии недоступны или также скомпрометированы
- **Затраты на восстановление:** помимо выплаты выкупа, предприятия сталкиваются со затратами на усилия по исправлению, включая ИТ-услуги, судебные издержки и потенциальные штрафы регулирующих органов
- **Потеря доходов:** невозможность работать во время и после атаки может привести к значительному снижению доходов

#### Репутационный ущерб

#### Проблемы конфиденциальности

- **Раскрытие конфиденциальных данных:** Фирмы, предоставляющие бизнес-услуги, часто обрабатывают конфиденциальные данные клиентов. Атака может привести к утечке данных, раскрыв конфиденциальную информацию
- **Двойное вымогательство:** злоумышленники могут не только шифровать данные, но и угрожать их обнародованием, если выкуп не будет выплачен, что усугубляет последствия

#### Правовые и нормативные последствия

При компрометации клиентских данных предприятия могут столкнуться с юридическими последствиями и штрафами за несоблюдение правил защиты данных

#### Риски, связанные с цепочкой поставок и третьими сторонами

Атаки могут выходить за рамки затронутого бизнеса, затрагивая клиентов, партнёров и поставщиков

#### Кража интеллектуальной собственности

Для фирм, которые полагаются на запатентованные методы или данные, атаки программ-вымогателей представляют риск кражи интеллектуальной собственности

#### Долгосрочный шпионаж

Некоторые атаки могут быть частью долгосрочных шпионских усилий, направленных на сбор стратегической информации с течением времени

##### 6) Здравоохранение

Атаки программ-вымогателей могут нанести ущерб организациям здравоохранения, что приведёт к прямым финансовым потерям, остановкам в работе, долгосрочному ущербу репутации и юридическим последствиям.

#### Сбой в работе

- **Прерывание обслуживания:** Атаки могут нарушать работу здравоохранения путём шифрования или недоступности медицинских записей и систем, что приводит к задержкам в оказании помощи пациентам и потенциально может привести к смерти пациентов
- **Повышенная смертность пациентов:** атаки увеличивают внутрибольничную смертность пациентов, госпитализированных во время атаки, со значительным повышением риска смерти

#### Финансовые последствия

- **Потеря дохода и затраты на восстановление:** Организации здравоохранения могут столкнуться с финансовыми потерями, связанными с потерей дохода, выплатами выкупа, затратами на восстановление, а также ущербом для бренда и судебными издержками. Средняя стоимость атаки программы-вымогателя в сфере здравоохранения составила 4,82 миллиона долларов в 2021 году
- **Потери, связанные с простоями:** Атаки программ-вымогателей на здравоохранение привели к потерям, связанным с простоями, в размере более 77 миллиардов долларов для экономики США

### Репутационный ущерб

Успешные атаки могут серьёзно подорвать репутацию поставщиков медицинских услуг, что приведёт к потере доверия пациентов и потенциально вынудит пациентов обращаться за медицинской помощью в другое место

### Проблемы конфиденциальности

- **Раскрытие конфиденциальных данных:** организации здравоохранения хранят обширные данные о пациентах. Атаки программ-вымогателей могут привести к утечке конфиденциальных данных, включая личную медицинскую информацию (PHI), подвергая миллионы пациентов рискам конфиденциальности
- **Двойное вымогательство:** злоумышленники могут угрожать разглашением конфиденциальных данных, если выкуп не будет выплачен, что усугубляет последствия атаки

### Правовые и нормативные последствия

В случае компрометации данных пациентов медицинские организации могут столкнуться с юридическими последствиями и штрафами за несоблюдение правил защиты данных

### Риски, связанные с цепочкой поставок и третьими сторонами

Атаки программ-вымогателей могут выходить за рамки непосредственно затронутого поставщика медицинских услуг, затрагивая клиентов, партнёров и поставщиков

### Кража интеллектуальной собственности

Атаки программ-вымогателей создают риск кражи интеллектуальной собственности, потенциально нанося ущерб конкурентным преимуществам и инновационным усилиям

### Долгосрочный шпионаж

Некоторые атаки на медицинских работников осуществляются высокоразвитыми группами угроз, нацеленными на долгосрочный шпионаж

### 7) Финансы

Атаки программ-вымогателей могут нанести ущерб финансовым учреждениям, что приведёт к прямым

финансовым потерям, остановкам работы, долгосрочному ущербу репутации и юридическим последствиям. Зависимость финансового сектора от цифровых систем и обработки конфиденциальных данных клиентов делает его прибыльной мишенью для киберпреступников.

### Сбой в работе

- **Прерывание обслуживания:** Атаки нарушают финансовые операции, шифруя или делая недоступными финансовые записи и системы, что приводит к задержкам в финансовых транзакциях и потенциально вызывает значительные операционные сбои
- **Сетевое проникновение:** Взаимосвязанный характер финансовых сетей увеличивает риск проникновения, потенциально обеспечивая доступ к информации через различные связанные системы

### Финансовые последствия

- **Потеря дохода и затраты на восстановление:** Финансовые организации могут столкнуться с финансовыми потерями, связанными с потерей дохода, выплатами выкупа, затратами на восстановление, а также ущербом для бренда и судебными издержками. Средняя стоимость атаки финансового вымогателя составила 5,9 миллиона долларов за киберинцидент в 2023 году
- **Потери, связанные с простоями:** Атаки на финансовые сервисы привели к значительным финансовым потерям, включая затраты, связанные с серьёзностью атаки и степенью раскрытия данных

### Репутационный ущерб

- **Потеря доверия:** успешные атаки программ-вымогателей могут серьёзно повредить репутации финансовых учреждений, в результате чего клиенты теряют доверие и, возможно, переводят свой бизнес в другое место
- **Ущерб бренду:** восприятие неадекватных мер безопасности может запятнать имидж бренда, влияя на долгосрочные перспективы бизнеса

### Проблемы конфиденциальности

- **Раскрытие конфиденциальных данных:** Финансовые учреждения хранят обширные данные о клиентах. Атаки программ-вымогателей могут привести к утечке конфиденциальных данных, подвергая миллионы клиентов рискам конфиденциальности
- **Двойное вымогательство:** злоумышленники могут угрожать разглашением конфиденциальных данных, если выкуп не будет выплачен, что усугубляет последствия атаки

### Правовые и нормативные последствия

: В случае компрометации клиентских данных финансовые учреждения могут столкнуться с

юридическими последствиями и штрафами за несоблюдение правил защиты данных

### **Риски, связанные с цепочкой поставок и третьими сторонами**

Атаки могут распространяться за пределы непосредственно затронутого финансового учреждения, затрагивая клиентов, партнёров и поставщиков

#### **Кража интеллектуальной собственности**

Атаки создают риск кражи интеллектуальной собственности, потенциально нанося ущерб конкурентным преимуществам и инновационным усилиям

#### **Долгосрочный шпионаж**

Атаки на финансовые учреждения проводятся группами, нацеленными на долгосрочный шпионаж

#### **8) Госсектор**

Атаки на государственные учреждения могут нарушить жизненно важные операции, привести к значительным финансовым потерям, подорвать общественное доверие и иметь долгосрочные последствия для сообщества.

#### **Сбой в работе**

- **Прерывание обслуживания:** возможно отключение цифровые активы, такие как платёжные платформы или госпорталы, что приводит к остановке муниципальных операций
- **Службы экстренной помощи:** Атаки, приводящие к отключению систем диспетчеризации 911 или 311, могут поставить жизни людей под угрозу
- **Время простоя системы:** Госслужащие могут остаться без систем, прибегая к ручным процессам

#### **Финансовые последствия**

- **Затраты:** В период с 2018 по декабрь 2023 года атаки на правительственные организации США обошлись примерно в 860,3 миллиона долларов
- **Выплаты выкупа:** Правительства могут быть вынуждены платить выкупы или столкнуться с дорогостоящим решением о перестройке систем

#### **Репутационный ущерб**

- **Общественное доверие:** атака наносит ущерб репутации госструктур, потенциально приводя к потере доверия общественности
- **Восприятие безопасности:** атаки рассматриваются как свидетельство слабых методов обеспечения безопасности, что заставляет общественность сомневаться в способности правительства защищать конфиденциальную информацию

#### **Проблемы конфиденциальности**

- **Конфиденциальная информация:** Правительства рискуют потерять контроль над секретной и личной

информацией, такой как номера социального страхования или данные кредитной карты

- **Потеря данных:** Программа-вымогатель приводит к непригодности данных и систем, что приведёт к потенциальной потере данных, если резервные копии недоступны или скомпрометированы

#### **Правовые и нормативные последствия**

Правительства могут столкнуться с юридическими последствиями и штрафами за несоблюдение правил защиты данных, если данные граждан будут скомпрометированы

#### **Долгосрочные эффекты**

- **Обучение и денежные потери:** например, атаки программ-вымогателей на школы могут привести к потере знаний, а также к денежным потерям
- **Психосоциальное воздействие:** могут наблюдаться значительные краткосрочные и долгосрочные социальные и психологические последствия для лиц, пострадавших от нападений

#### **Повышенная частота атак**

Значительно увеличилось количество атак программ-вымогателей на правительственные организации, при этом на 313% увеличилось количество зарегистрированных инцидентов со службами безопасности

#### **9) Образование**

Атаки программ-вымогателей могут нанести ущерб учебным заведениям, что приведёт к прямым финансовым потерям, остановкам в работе, долгосрочному ущербу репутации и юридическим последствиям.

#### **Сбой в работе**

- **Прерывание обслуживания:** Программа-вымогатель может отключать платёжные платформы или госпорталы, что приводит к остановке муниципальных операций
- **Службы экстренной помощи:** Атаки, приводящие к отключению систем диспетчеризации 911 или 311, могут поставить жизни людей под угрозу
- **Время простоя системы:** Государственные служащие могут остаться без своих систем, прибегая к ручным процессам

#### **Финансовые последствия**

- **Затраты:** В период с 2018 по декабрь 2023 года атаки программ-вымогателей на правительственные организации США обошлись примерно в 860,3 миллиона долларов; Средняя стоимость образовательной атаки программ-вымогателей составила 2,73 миллиона долларов за киберинцидент в 2023 году.
- **Выплаты выкупа:** Правительства могут быть вынуждены платить выкупы или столкнуться с дорогостоящим решением о перестройке систем

## Репутационный ущерб

- **Общественное доверие:** атака программ-вымогателей может нанести ущерб репутации государственных структур, потенциально приводя к потере доверия общественности
- **Восприятие безопасности:** Успешные атаки могут рассматриваться как свидетельство слабых методов обеспечения безопасности, что заставляет общественность сомневаться в способности правительства защищать конфиденциальную информацию

## Проблемы конфиденциальности

- **Конфиденциальная информация:** Правительства рискуют потерять контроль над секретной и личной информацией, такой как номера социального страхования или данные кредитной карты
- **Потеря данных:** Программа-вымогатель приводит к непригодности данных и систем, что приведёт к потенциальной потере данных, если резервные копии недоступны или скомпрометированы

## Правовые и нормативные последствия

Правительства могут столкнуться с юридическими последствиями и штрафами за несоблюдение правил защиты данных, если данные будут скомпрометированы

## Долгосрочные эффекты

- **Обучение и денежные потери:** например, атаки программ-вымогателей на школы могут привести к потере знаний, а также к денежным потерям
- **Психосоциальное воздействие:** могут наблюдаться значительные краткосрочные и долгосрочные социальные и психологические последствия для лиц, пострадавших от нападений

## Повышенная частота атак

Значительно увеличилось количество атак программ-вымогателей на правительственные организации, при этом на 313% увеличилось количество зарегистрированных инцидентов со службами безопасности конечных точек

### 10) Информационные технологии

Атаки могут нанести ущерб ИТ-компаниям, что приведёт к прямым финансовым потерям, остановкам в работе, ущербу репутации и юридическим последствиям.

## Сбой в работе

- **Прерывание обслуживания:** Программы-вымогатели могут нарушать работу ИТ-служб, шифруя или делая системы и данные недоступными, что приводит к задержкам в обслуживании и потенциально вызывает значительные сбои в работе
- **Проникновение в сеть:** Взаимосвязанный характер ИТ-сетей увеличивает риск проникновения,

потенциально обеспечивая доступ к информации через различные подключённые системы

## Финансовые последствия

- **Потеря доходов:** Организации могут столкнуться со снижением доходов или полной остановкой операций во время восстановления после атаки программ-вымогателей, даже если у них есть функциональные резервные копии
- **Выплаты выкупа и затраты на восстановление:** Компании могут столкнуться со значительными расходами, связанными с выплатой выкупа, восстановлением системы, судебными издержками и другими сопутствующими расходами

## Репутационный ущерб

- **Доверие клиентов:** успешная атака может нанести ущерб репутации ИТ-компаний, вынудив клиентов вести бизнес в других местах из-за предполагаемых слабых методов обеспечения безопасности
- **Ущерб бренду:** Восприятие "небезопасного" бизнеса может нанести больший ущерб, чем непосредственные финансовые потери, и повлиять на репутацию компании

## Утечка данных и проблемы конфиденциальности

- **Раскрытие конфиденциальных данных:** ИТ-компания хранят обширные данные о клиентах и операционной деятельности. Атаки могут привести к утечке конфиденциальных данных, подвергая клиентов рискам для конфиденциальности
- **Двойное вымогательство:** злоумышленники могут угрожать разглашением конфиденциальных данных, если выкуп не будет выплачен, что приводит к атакам с двойным вымогательством

## Правовые и нормативные последствия

При компрометации данных клиентов ИТ-компания могут столкнуться с юридическими последствиями и штрафами за несоблюдение правил защиты данных

## Цепочка поставок и риски третьих сторон

Атаки программ-вымогателей могут распространяться за пределы непосредственно затрагиваемой ИТ-компания, затрагивая клиентов, партнёров и поставщиков

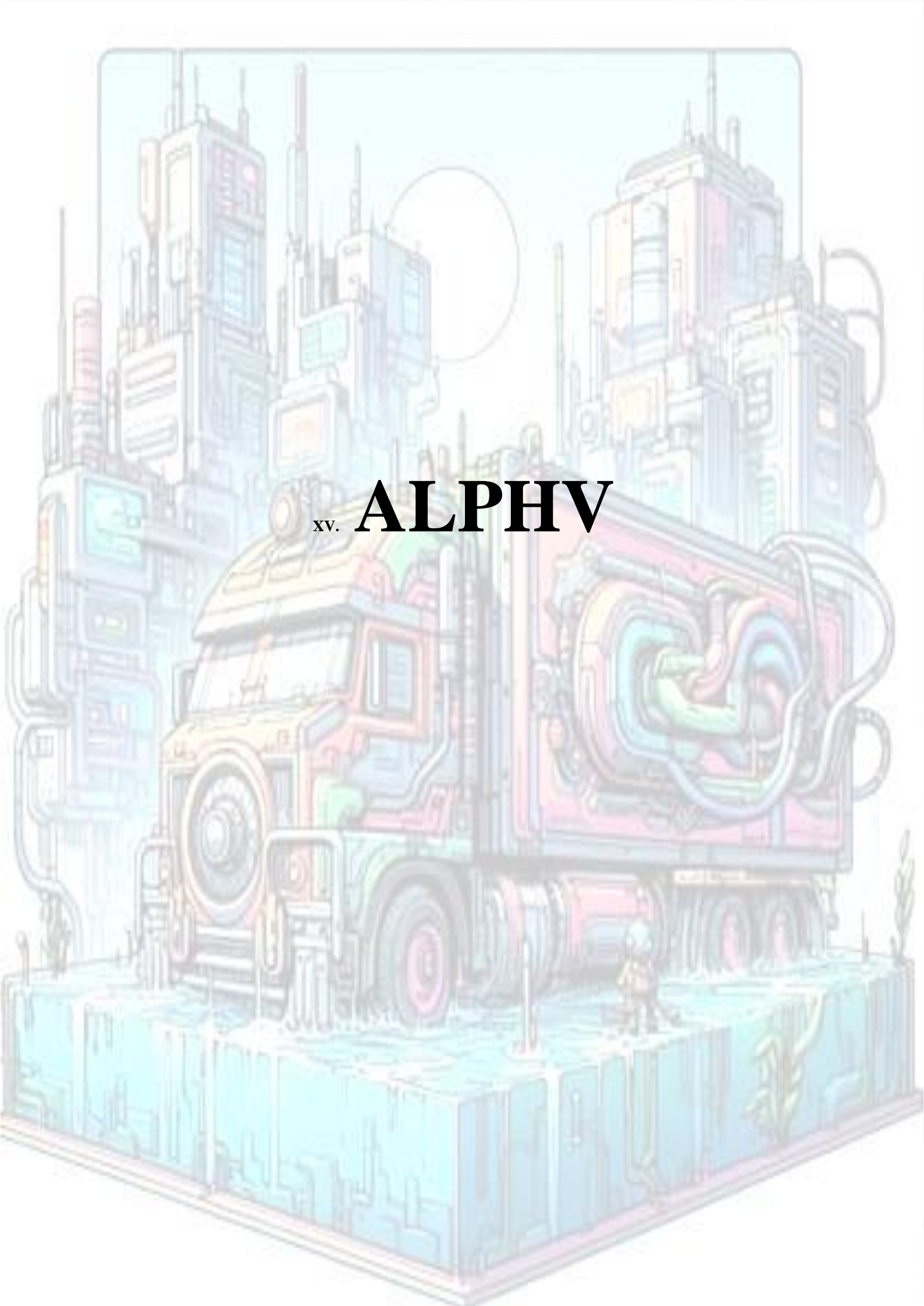
## Кража интеллектуальной собственности

Атаки создают риск кражи интеллектуальной собственности, потенциально нанося ущерб конкурентным преимуществам и инновационным усилиям

## Долгосрочный шпионаж

Некоторые атаки на ИТ-компания проводятся группами, нацеленными на долгосрочный шпионаж





xv. **ALPHV**



*Аннотация – В документе представлен анализ ситуации вокруг AlphaV (программы-вымогателя), связанного с группой BlackCat, который охватывает технические детали программы-вымогателя, включая её механизмы шифрования, векторы начального доступа, методы бокового перемещения и методы эксфильтрации данных.*

*Выводы, полученные в результате этого анализа, важны для практиков кибербезопасности, ИТ-специалистов и политиков. Понимание особенностей программ-вымогателей AlphaV/BlackCat позволяет разрабатывать более эффективные механизмы защиты, совершенствовать стратегии реагирования на инциденты.*

#### A. Введение

Сайт-вымогатель AlphaV, связанный с группой BlackCat, подвергся серии сбоев и блокировок со стороны ФБР, за которыми последовали попытки группы восстановить контроль. 19 декабря 2023 года ФБР в рамках скоординированных усилий с международными правоохранительными органами наложило арест на веб-сайт группы и опубликовало соответствующее уведомление. Это действие было частью кампании по уничтожению деятельности группы вымогателей BlackCat, которая нацелилась на компьютерные сети более 1000 жертв по всему миру, включая те, которые поддерживают критически важную инфраструктуру США.

ФБР также разработало инструмент расшифровки, который был предоставлен сотням жертв программ-вымогателей по всему миру, позволяющий предприятиям, школам, здравоохранению и экстренным службам восстанавливаться и возвращаться в Сеть. Однако официальные лица AlphaV быстро отреагировали, восстановив временный контроль над своим сайтом и разместив новое уведомление, в котором говорилось о преуменьшении значения действий ФБР и объявили, что

"VIP" филиалы получают частную поддержку в отдельных изолированных центрах обработки данных.

Несмотря на первоначальный успех ФБР, сайт AlphaV снова заработал, но без всех ссылок на жертв, ранее опубликованных в рамках их стратегии вымогательства. Группа также утверждала, что у ФБР были ключи дешифрования только для около 400 компаний, в результате чего более 3000 жертв получили зашифрованные данные. В отместку AlphaV сняла свой добровольный запрет на атаки на критически важные сектора инфраструктуры, включая здравоохранение и ядерные объекты.

«Перепалка» между ФБР и AlphaV привела к многочисленным случаям захвата веб-сайта, а затем его "отмены", демонстрируя перетягивание каната за контроль над сайтом. Несмотря на эти события, ФБР и его партнёры продолжают расследование и преследование лиц, стоящих за BlackCat, с целью привлечения их к ответственности.

#### B. AlphaV ransomware

Программа-вымогатель работает с токеном доступа, который поставляется с зашифрованной конфигурацией, которая содержит список служб / процессов, список каталогов / файлов / расширений файлов, внесённых в белый список, и список украденных учётных данных из среды жертвы. Программа-вымогатель сканирует тома на локальном компьютере, монтирует все размонтированные тома и начинает шифровать файлы. Он также удаляет все новые копии томов, затрудняя жертвам восстановление своих данных.

Программа-вымогатель эволюционировала и стала использовать более сложные конструкции, что затрудняет её обнаружение. Например, конфигурационные данные больше не имеют формат JSON; вместо этого используются бинарные структуры, и они содержат ненужный код и тысячи зашифрованных строк для затруднения статического анализа.

Было замечено, что программа-вымогатель ALPHV использует уязвимости в открытых сервисах или слабые учётные данные для первоначального доступа. Он также использует такие инструменты, как ExMatter, для кражи конфиденциальных данных перед развёртыванием программы-вымогателя.

#### C. Тактика AlphaV

ALPHV использует несколько тактик распространения для компрометации систем:

- **Фишинговые электронные письма:** вводящие в заблуждение сообщения создаются для того, чтобы заманить жертв к открытию вредоносного контента, часто замаскированного под законные сообщения
- **Вредоносная реклама:** использование вредоносной рекламы для распространения вредоносного ПО. Известно, что группа программ-вымогателей ALPHV манипулирует рекламой Google, чтобы привести ничего не подозревающих пользователей на вредоносные сайты

- **Установщики заражённого ПО:** использование заражённых установщиков для доставки программ-вымогателей. Сюда входят клонированные веб-страницы законных организаций, которые используются для распространения вредоносного кода по заражённым ссылкам или файлам
- **Использование уязвимостей ПО:** Группа использует уязвимости в операционных системах Windows, серверах Exchange и продуктах защищённого мобильного доступа для получения доступа к сетям жертв
- **Метод тройного вымогательства:** Эта возникающая угроза включает кражу данных с локальных компьютеров и облачных серверов, запуск программы-вымогателя, а затем оказание дополнительного давления на жертву посредством DDoS-атак или утечки данных

#### D. Точки входа AlphV

ALPHV была идентифицирована как один из самых распространённых вариантов программы-вымогателя "как услуга" в мире, затрагивающий различные секторы, включая производство, технологии, розничную и оптовую торговлю, финансы, здравоохранение и общественную сферу, госсектор и энергетику, и профессиональные услуги.

Первоначальными точками проникновения программы-вымогателя ALPHV в сети жертв являются, прежде всего, скомпрометированные учётные данные пользователей и использование уязвимостей программного обеспечения. Например, было замечено, что дочерние компании ALPHV нацеливались на общедоступные установки Veritas Backup Exec, которые были уязвимы для определённых CVE, для получения первоначального доступа к среде жертвы.

В секторе здравоохранения атаки программ-вымогателей часто используют множество возможных точек входа, включая фишинговые электронные письма, уязвимости программного обеспечения, атаки по протоколу удаленного рабочего стола и несанкционированные загрузки с вредоносных веб-сайтов.

В финансовом секторе атаки ALPHV подчеркнули необходимость расширения возможностей обнаружения инцидентов и надёжной своевременной отчётности перед лицом развивающихся киберугроз.

В технологическом секторе известно, что ALPHV компрометирует поставщиков технологий цифрового кредитования, что видно из атаки на MeridianLink.

В государственном секторе сбои затронули критически важную инфраструктуру США и госучреждения.

В энергетическом секторе было замечено, что программа-вымогатель нацелена на сети, поддерживающие критически важную инфраструктуру США.

В секторе профессиональных услуг ALPHV нацелена на юридические, IT-, промышленные и финансовые услуги.

В дополнение к этим методам ALPHV также использует инструменты администрирования Windows и инструменты Microsoft Sysinternals для компрометации. Также стоит

отметить, что некоторые филиалы ALPHV осуществляют фильтрацию данных и вымогательство у жертв, даже не внедряя программы-вымогатели.

#### E. Шифрование и выкупы

ALPHV использует сложные методы шифрования для блокировки данных жертв: комбинацию симметричного и асимметричного шифрования, хотя конкретные детали этих алгоритмов публично не разглашаются. Более конкретно, программа-вымогатель ALPHV использует либо AES, либо ChaCha20, в зависимости от его конфигурации. Программа-вымогатель генерирует случайный ключ для каждого файла, который затем шифруется с помощью открытого ключа RSA, хранящегося в конфигурации BlackCat. Затем файл шифруется с помощью AES.

Что касается способов оплаты, ALPHV обычно запрашивают выплаты выкупа в криптовалютах, в частности в биткоинах и Monero. Эти криптовалюты пользуются спросом из-за их децентрализованного характера и анонимности, которую они предоставляют получателям. Суммы выкупа, требуемые ALPHV, часто непомерны и варьируются от пяти до шести цифр в долларах США. Однако стоит отметить, что известно, что атакующие вели переговоры и принимали платежи ниже первоначального требования о выкупе

#### F. Цели AlphV

Было обнаружено, что ALPHV нацелена на организации различных размеров. Согласно данным с сайтов утечек с требованием выкупа, больше всего жертв приходится на компании с 51–200 сотрудниками, что составляет 20,57% от общего числа. За ними следуют компании с численностью менее 50 сотрудников, на долю которых приходится 16,91% жертв:

- Компании с численностью сотрудников 501–1000 человек: 7,12%
- Компании с численностью сотрудников от 1000 до 5000 человек: 9,92%
- Компании с численностью 5,000-10,000 сотрудников: 2,38%
- Компании с численностью сотрудников более 10 000 человек: 4,46%

Однако важно отметить, что существует категория с пометкой "неизвестно", на долю которой приходится 27,87% от общего числа, что указывает на то, что точный размер компаний некоторых жертв не известен.

В четвёртом квартале 2022 года успешные атаки BlackCat были нацелены в первую очередь на малые предприятия, составив 38,9% от общего числа, за которыми следовали компании среднего размера (28,6%).

ALPHV нацелена на широкий круг организаций в различных секторах:

- **Организации здравоохранения:** ALPHV был связан с атаками на организации здравоохранения, включая утечку конфиденциальных изображений

пациентов с раком молочной железы. Norton Healthcare также стала жертвой атаки ALPHV

- **Финансовые учреждения:** Fidelity National Financial стала мишенью ALPHV. Группа заявила о взломе систем поставщика программного обеспечения для бухгалтерского учёта Tipalti с планами вымогательства у клиентов поставщика
- **Нефтяные компании:** Две немецкие нефтяные компании стали мишенью группы BlackCat
- **Гостиничный бизнес:** Громкие атаки были связаны с ALPHV, в т.ч. MGM Resorts и Caesars Entertainment
- **Производство:** ALPHV нацелилась на производителя и поставщика складских услуг
- **Государственные учреждения и службы экстренной помощи:** Министерство юстиции США связало ALPHV с атаками на критически важную инфраструктуру США, включая госучреждения и службы экстренной помощи
- **Школы:** Школы также стали мишенью ALPHV
- **Компании оборонно-промышленной базы:** Эти компании стали мишенью ALPHV в рамках её атак на критически важную инфраструктуру США

#### 1) *Здравоохранение*

AlphV шифровал конфиденциальные данные, включая информацию о пациентах, и требовал выкуп за ключи расшифровки. Эти атаки не только привели к финансовым потерям, но и создали серьёзные риски для ухода за пациентами и их безопасности. Агрессивные действия правоохранительных органов, включая разработку инструментов дешифрования, принесли некоторую помощь жертвам.

#### **Известные атаки и воздействия**

Атака программ-вымогателей McLaren HealthCare: Крупная атака программ-вымогателей на McLaren HealthCare, крупного поставщика медицинских услуг в Мичигане, выявила уязвимость систем здравоохранения к киберугрозам.

- **Атаки на больницы и медицинские сети:** Группа атаковала больницы, раскрывая конфиденциальные данные пациентов и подвергая риску уход за пациентами и их жизни. Эти атаки были частью более широкой схемы атаки на сети критически важной инфраструктуры США
- **Влияние на уход за пациентами и безопасность данных:** Атаки на организации здравоохранения имели серьёзные последствия, включая перебои в предоставлении медицинских услуг, раскрытие конфиденциальной медицинской информации и финансовые потери.

#### **Реакция правоохранительных органов**

- **Кампания по подрыву деятельности Министерства юстиции США:** Министерство

юстиции (DOJ) в сотрудничестве с ФБР и международными партнёрами запустило кампанию против группы ALPHV/BlackCat, направленную на снижение угрозы для критически важной инфраструктуры, включая сектор здравоохранения

- **Инструмент дешифрования ФБР:** в рамках усилий по предотвращению сбоев ФБР разработало инструмент дешифрования для жертв ALPHV, включая организации здравоохранения. Этот инструмент помог спасти жертв от требований выкупа на общую сумму около 68 миллионов долларов, позволив пострадавшим предприятиям и медицинским учреждениям восстановиться и возобновить деятельность

#### 2) *Индустрия финансовых институтов*

ALPHV представляет серьёзную угрозу для индустрии финансовых учреждений, применяя эффективную тактику нападения на банки, страховые компании и других поставщиков финансовых услуг, включая шифрование файлов, кражу конфиденциальных данных и требование выкупа, часто с использованием двойного вымогательства (шифрование и угроза разглашения данных).

#### **Известные атаки и воздействия**

- **Атака на Fidelity National:** Один из самых громких инцидентов был связан с компанией Fidelity National Financial, поставщиком титульного страхования, входящей в список Fortune 500. Группа ALPHV / Black Cat взяла на себя ответственность за эту кибератаку, которая привела к сбоям в страховании титула, условном депонировании и других сопутствующих услугах.
- **Рост угроз программ-вымогателей:** В финансовой отрасли наблюдается всплеск атак программ-вымогателей, при этом заметно возросла как частота, так и эффективность этих инцидентов. Финорганизации являются привлекательной мишенью из-за огромного количества хранящихся у них конфиденциальных данных о клиентах и партнёрах, что делает их идеальными для атак с двойным вымогательством.
- **Влияние на финансовые операции:** Атаки на финучреждения имеют серьёзные последствия, включая нарушение работы важнейших финансовых услуг и торговой деятельности. Например, атака на американское торговое подразделение Промышленно-коммерческого банка Китая нарушила торги на рынке казначейских облигаций США, что подчёркивает потенциальное влияние программ-вымогателей на финансовую стабильность

#### 3) *Нефтяные компании, промышленность*

Группа работает по модели "программа-вымогатель как услуга" (RaaS) и нацелена на организации по всему миру

#### **Известные атаки и воздействия**

ALPHV раскрыла 400 ГБ данных, которые, как утверждается, были украдены у Encino Energy, основного производителя нефти в Огайо. Несмотря на это, Encino Energy сообщила, что атака не повлияла на их деятельность. В Европе ALPHV была замешана в нападении на немецкие нефтяные компании Mabanaft и Oiltanking, которое нарушило работу их систем погрузки и разгрузки и вынудило энергетического гиганта Shell перенаправить поставки. Эти атаки демонстрируют способность ALPHV нацеливаться на критически важную энергетическую инфраструктуру и разрушать её.

#### **Реакция правоохранительных органов**

Правоохранительные органы приняли меры против инфраструктуры группы ALPHV. ФБР и международные правоохранительные органы проникли в инфраструктуру группы и закрыли её, жертвами которой за 18 месяцев стали более 1000 человек. Хотя в рамках демонтажа не было объявлено ни о каких арестах, операция представляет собой значительную попытку пресечь деятельность групп программ-вымогателей, нацеленных на критически важные секторы, такие как нефтяная промышленность.

#### *4) Индустрия гостеприимства и развлечений*

AlphV совершила несколько громких атак на индустрию гостеприимства и развлечений, которые характеризуются кражей конфиденциальных данных, включая личную и финансовую информацию клиентов, за которой следуют требования выкупа. Используемая группой тактика включает социальную инженерию и недобросовестную рекламу.

#### **Известные атаки и воздействия**

- **Атака LBA Hospitality:** LBA Hospitality управляет отелями крупных сетей, таких как Marriott и Hilton. Группа утверждала, что скомпрометировала около 200 ГБ "строго конфиденциальных" внутренних данных компании, включая личные данные клиентов и сотрудников, финансовые отчёты, информацию о кредитных картах и многое другое
- **Международная атака MGM Resorts:** ALPHV была ответственна за кибератаку на MGM Resorts, вызвавшую значительные сбои в работе, вывела из строя системы онлайн-бронирования, цифровые ключи от номеров, игровые автоматы и веб-сайты. Группа использовала тактику социальной инженерии, чтобы получить доступ к системам MGM, и внедрила программу-вымогатель в более чем 100 гипервизорах ESXi в сети MGM.
- **Атака Caesars Entertainment:** Caesars Entertainment стала ещё одной жертвой ALPHV, в результате которой был нанесён ущерб по меньшей мере в 100 миллионов долларов и, как сообщается, был выплачен выкуп в размере 15 миллионов долларов
- **Westmont Hospitality Group:** Группа заявила, что взломала Westmont Hospitality Group, один из крупнейших в мире частных гостиничных бизнесов
- **Утечка данных Motel One:** Группа атаковала сеть отелей Motel One и угрожала утечкой 6 ТБ украденных данных, включая контактные данные

клиентов, внутренние документы и данные кредитной карты

#### **Технологические подходы**

Группа злоупотребляла поисковой рекламой Google для распространения программ-вымогателей, используя крупные бренды в качестве приманки, чтобы перенаправлять пользователей на вредоносные сайты. Также используются тактику социальной инженерии, такую как шпионский фишинг и звонки в службы поддержки для получения доступа к сетям.

#### *5) Производственная и складская промышленность*

AlphV связан с серией атак в различных секторах, включая производство. За последние 18 месяцев под атаку попало более 1000 жертв.

#### **Известные атаки и воздействия**

Формально сюда можно упомянутую ранее атаку на MGM Resorts International и использование Google Ads. ALPHV/BlackCat часто выдаёт себя за ИТ-специалистов компании и / или сотрудников службы поддержки и используют телефонные звонки или SMS-сообщения для получения доступа к системам.

Ещё одна атака совершена на Clarion, мирового производителя аудио- и видеооборудования для автомобилей и других транспортных средств. Группа утверждала, что произошла утечка конфиденциальных данных об их бизнесе и партнёрах, включая техническую информацию клиентов компании.

Организациям также следует знать, что группа нацелена как на устройства Windows, так и на Linux, а также на устройства хранения данных с сетевым подключением (NAS), которые часто используются для хранения резервных копий и конфиденциальных данных.

#### *6) Государственные учреждения*

AlphV оказала влияние на государственные учреждения и отрасль экстренных служб как разновидность критически важной инфраструктуры, вызывая сбои в работе и создавая угрозы национальной и общественной безопасности.

#### **Известные атаки и воздействия**

- **Нарушение работы критически важной инфраструктуры:** ALPHV была связана с атаками на критически важную инфраструктуру США, включая госучреждения и службы экстренной помощи.
- **Глобальный масштаб операций:** ALPHV/BlackCat стала вторым по распространённости вариантом программы-вымогателя "как услуга" в мире (RaaS). Её деятельность привела к значительным глобальным последствиям, в результате чего группа поставила под угрозу деятельность более 1000 юридических лиц по всему миру.
- **Финансовые последствия и выплаты выкупа:** Группа потребовала выкуп в размере более \$500M и получила выплаты в размере почти \$300M. Это финансовое воздействие подчёркивает прибыльный характер операций с программами-вымогателями, нацеленных на критически важные сектора, включая госучреждения и службы экстренной помощи

## Реакция правоохранительных органов

- **Кампания по дезорганизации Министерства юстиции:** Министерство юстиции в сотрудничестве с ФБР и международными партнёрами запустило кампанию по дезорганизации деятельности группы. Эта кампания была направлена на снижение угрозы, которую представляет программа-вымогатель для критически важной инфраструктуры, включая госучреждения и экстренные службы
- **Инструмент для расшифровки данных:** ФБР разработало инструмент для расшифровки данных, предоставляемый жертвам ALPHV, который помог сэкономить около \$68М, позволив пострадавшим организациям восстановиться и возобновить операционную деятельность

### 7) Школьная индустрия

ALPHV нацелена на сектор образования, включая школы K-12, университеты и другие учебные заведения. Эти атаки нарушили образовательные процессы и поставили под угрозу конфиденциальные данные учащихся и персонала. Восприимчивость сектора к киберугрозам из-за часто ограниченных ресурсов и большого количества потенциальных противников кибербезопасности.

#### Известные атаки и воздействия

- **Участились атаки программ-вымогателей:** резко увеличилось количество атак на школы, число таких инцидентов увеличилось на 17%. Атаки включали шифрование файлов и угрозы утечки украденных данных, если не будет выплачен выкуп
- **Пострадали крупные школьные округа:** Школьные округа, такие как государственные школы Далласа и Миннеаполиса, были в числе крупных жертв атак программ-вымогателей.
- **Глобальный охват:** Атаки на школы не ограничивались США; образовательные учреждения в Соединенном Королевстве, Австралии, Германии,

Франции и Бразилии также столкнулись с атаками программ-вымогателей

- **Влияние на образовательные операции:** Атаки на школы могут привести к значительным сбоям в работе, включая прерывание процесса подачи заявок, операций и занятий. В некоторых случаях нападения были достаточно серьёзными, чтобы привести к закрытию школ

#### Тактика и приемы

- **Двойное вымогательство:** операторы ALPHV часто используют тактику двойного вымогательства, при которой они шифруют файлы, а также угрожают утечкой украденных данных. Такой подход оказывает дополнительное давление на жертв, требуя выплатить выкуп
- **Использование уязвимостей:** Основной причиной атак в секторе образования является использование уязвимостей в устройствах, и отсутствие ресурсов для принятия надёжных мер кибербезопасности, что делает их восприимчивыми к таким атакам

### 8) Оборонно-промышленные предприятия

Особое внимание к оборонной промышленности подчёркивает стратегический подход группы к компрометации организаций, жизненно важных для национальной безопасности и экономической стабильности.

#### Известные атаки и воздействия

- **Атаки на критическую инфраструктуру:** Министерство юстиции (DOJ) определило компании оборонно-промышленной базы как один из секторов критической инфраструктуры, на которые нацелен вариант программы-вымогателя ALPHV.

**Финансовые и операционные последствия:** Глобальные потери, связанные с ALPHV, которая использует модели атак с множественным вымогательством, привели к финансовым затратам.

# ХРОНИКИ КИБЕР-БЕЗОПАСНИКА