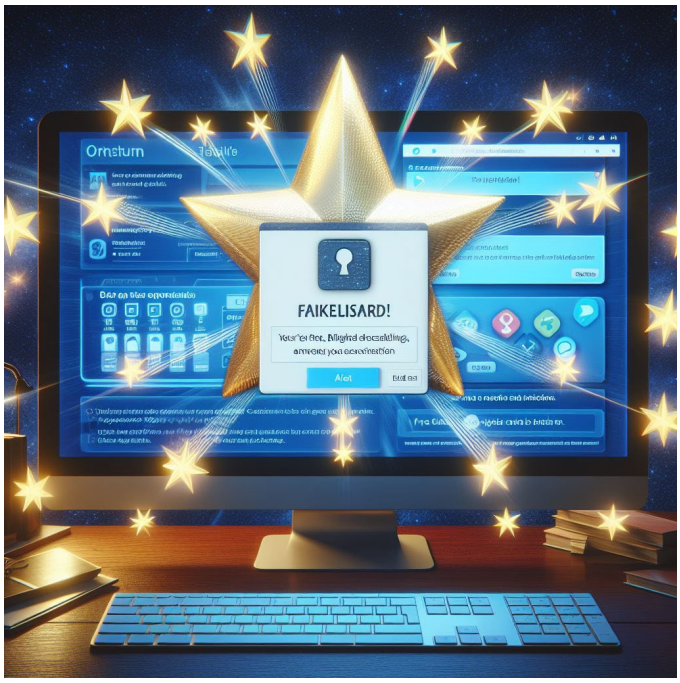

I. Введение

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 учётные данные своей учётной записи электронной почты, которые затем используются для получения несанкционированного (и постоянного) доступа к учётным 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.

II. Распространенные цели фишинговых атак

Фишинговые кампании обычно нацелены на конкретных лиц или организации с целью кражи конфиденциальной информации, такой как учётные 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 предлога для отправки электронного письма

- **Известные или авторитетные личности**: выдавать себя за кого-либо, занимающего руководящую должность, или известного контактного лица, чтобы вызвать доверие

III. 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
- **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

A. 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.

B. 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.

C. 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

D. Распространенные типы файлов, включенные в фишинговые электронные письма Star Blizzard

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

E. 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/XXXXXXXXXXXXX X/view?usp=sharing
- https://onedrive.live.com/?authkey=%XXXXXXXXX XXXXXXXXXXXXXXXXX%XXXX&cid=8XXXX XXXXX9B7
- https://www.dropbox.com/s/XXXXXXXXXXXXX/St ar_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.

IV. Применяемые методы кампаний Star Blizzard

A. 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
- **Имперсонизация**: 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

B. 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
- **Имперсонизация**: 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

V. 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

A. 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.

B. Услуги платформы для маркетинга по электроннойпочте

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.

C. 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.

D. 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.

E. 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.

VI. 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.

A. 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.

VII. Защита (Рекомендации Microsoft)

A. 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 отзывать 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 уровни 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 команду 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

B. 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.

C. 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 многочисленным 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 событиями (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-spay 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 isnotempty(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 isnotempty(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-spay 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 зафиксирует 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