I. Введение

APT-атаки, распространяющиеся по Азиатско-тихоокеанскому региону (APAC), 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 APAC, 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 APT 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 APT 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 APT Group

- **Середина 2021 года**: впервые замечена деятельность Dark Pink APT 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

II. Основные задачи Dark Pink APT Группы

Основные цели Dark Pink APT 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

III. Инструменты Dark Pink APT Group

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

A. 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 письмас 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.

B. 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.

C. 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.

IV. 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 инструментарий на базе .NET, известный как Cucky. 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%\backuplog, без передачи по сети

V. ОБЪЕКТЫ И СУБЪЕКТЫ АТАК

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

A. 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.

B. 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)

VI. 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 сохранять 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).

A. 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.

B. 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 вредосного 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

VII. 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
- 098f6bcd4621d373cade4e832627b4f6