1. РЕЗУЛЬТАТ

В результате анализа лог-файлов Sysmon подтверждено заражение устройства. Обнаружена цепочка активности, характерная для трояна-бэкдора DarkComet RAT, проникшего на устройство через установку пиратского программного обеспечения.

2. ХРОНОЛОГИЯ СОБЫТИЙ

| Время (приблизительно) | Событие |
| --- | --- |
| 14:30 - 14:50 | Пользователь активно скачивает пиратское ПО (офисные пакеты) через торрент-клиент TrayTorrent |
| 14:51 | Создание вредоносного процесса C:\Users\elk\Desktop\Skype.exe |
| 14:51 - 14:52 | Создание файлов в Temp: DARKCOMETRATLAUNCHER.EXE, DARKCOMET.EXE |
| 08:10:20 | Установка исходящего сетевого подключения от Skype.exe |

3. ВЕКТОР ЗАРАЖЕНИЯ

Первоисточник: Установка пиратского программного обеспечения:

Microsoft-Office-2019-Professional-Plus-2022.02-x64.zip

Office-2003-Word-Excel-Powerpoint.exe

Word\_Rus\_Soft\_instaler.exe

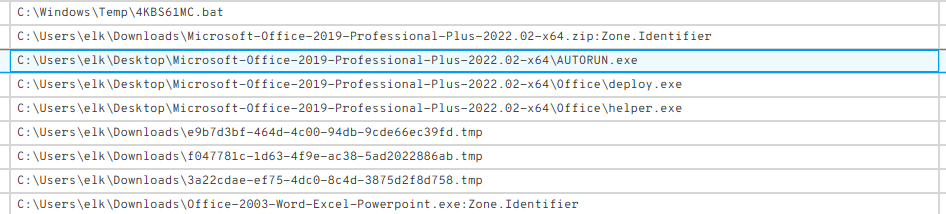
Цепочка выполнения:

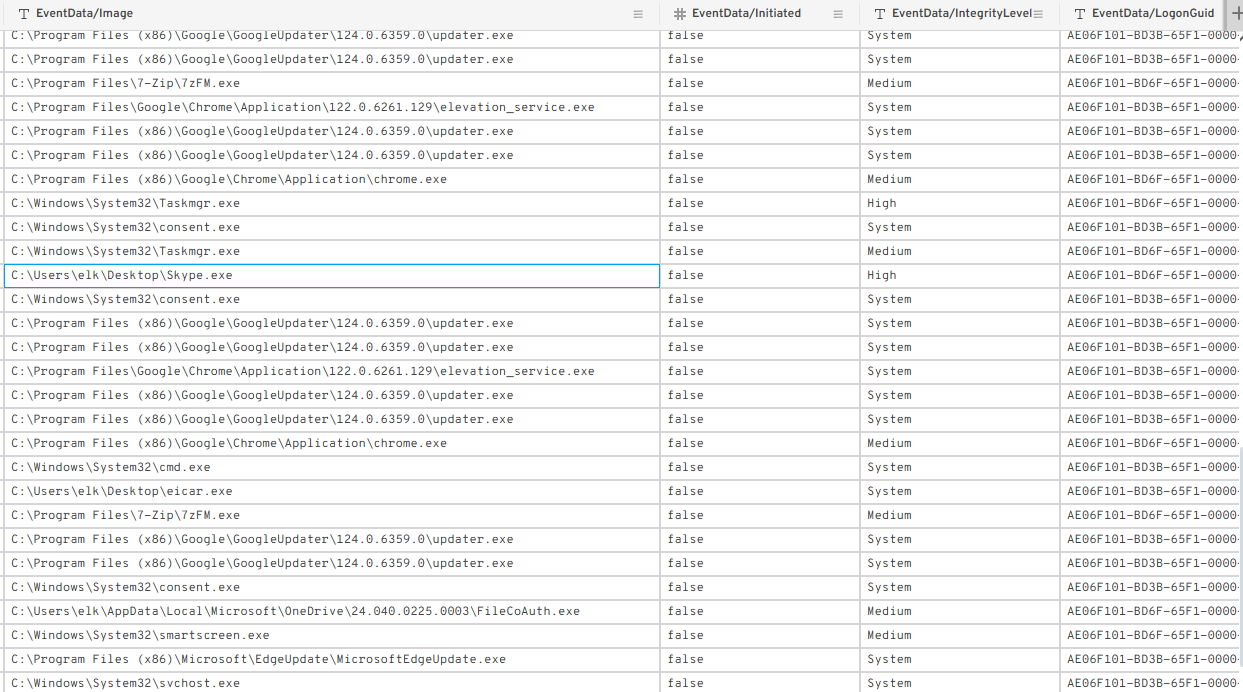
Архив с Office → AUTORUN.exe

AUTORUN.exe → start.hta (HTA-скрипт)

HTA-скрипт → BAT-файлы в C:\Windows\Temp\

BAT-скрипты → C:\Users\elk\Desktop\Skype.exe









4. ОСНОВНЫЕ ПОКАЗАТЕЛИ КОМПРОМЕТАЦИИ

Вредоносные процессы:

C:\Users\elk\Desktop\Skype.exe (основной троян)

C:\Users\elk\AppData\Local\Temp\DARKCOMET.EXE (DarkComet RAT)

C:\Users\elk\AppData\Local\Temp\DARKCOMETRATLAUNCHER.EXE (загрузчик)

Сетевые подключения:

Процесс: Skype.exe

Направление: Исходящее

Адреса: 13.107.42.12:443, 13.107.137.11:443

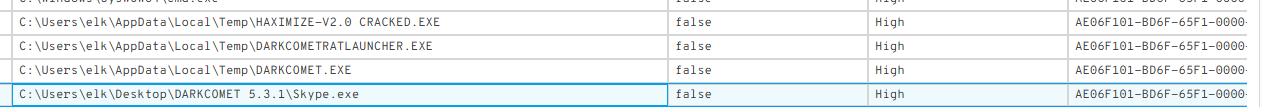
Протокол: HTTPS

Изменения в системе:

Создание BAT-файлов в C:\Windows\Temp\

Создание HTA-скрипта start.hta

Установка торрент-клиента TrayTorrent



5. КЛАССИФИКАЦИЯ ВРЕДОНОСНОГО ПО

Класс ВПО: Троян-бэкдор (DarkComet RAT)

Характерные признаки:

Маскировка под легитимное ПО (Skype)

Использование HTA-скриптов для запуска

Установка исходящих HTTPS-подключений

Наличие в временных папках

Создание дополнительных исполняемых файлов



6. РЕКОМЕНДАЦИИ

Немедленно:

Заблокировать исходящие подключения на порт 443 к указанным IP-адресам

Выполнить проверку антивирусным ПО

Удалить выявленные вредоносные файлы

Профилактика:

Ограничить установку непроверенного ПО

Обучение пользователей кибергигиене

Внедрение системы белых списков приложений