Файл лога: Logfile_3.PML

Цель: Найти вредоносный процесс, исследовать его вредоносную активность и разработать систему его обнаружения.

Инструменты: procmon

Результаты анализа

Имя вредоносного ПО: Adobe-Acrobat-2019-Eng-portable.exe

Назначение вредоносного ПО: кража пользовательских данных и данных аутентификации из браузеров.

Тип вредоносного ПО: Stealer

PID вредоносного процесса в файле лога: 3908

Механизм обеспечения поддержания заражения: социальная инженерия

Предполагаемая схема работы вредоносного ПО:

- Запуск ПО пользователем из Downloads
  - Запуск вредоносной ветви посредством запуска ПО самим собой
    - Создание C:\Users\D7c87h\AppData\Roaming\uyynmaiv.ycs куда будет производится копирование украденных данных
    - Копирование данных из папок браузеров:
      - %AppData%\Roaming\Mozilla\Firefox\profiles.ini
      - %AppData%\Roaming\Mozilla\Firefox\Profiles\85m6ciry.default\key3.db
      - %AppData%\Roaming\Mozilla\Firefox\Profiles\85m6ciry.default\logins.json
      - %AppData%\Roaming\Mozilla\Firefox\profiles.ini
      - %AppData%\Local\Google\Chrome\User Data\Default\Cookies
      - %AppData%\Roaming\Mozilla\Firefox\Profiles\85m6ciry.default\cookies.sqlite
    - Отправка украденных данных:
      - Соединение с сервером по адресу 208.91.197.13 и порту 587 таким образом происходит маскировка под почтовую службу.
    - Удаление папки, куда копировались данные с целью сокрытия следов.
- Запуск легитимной ветви (не представляет интереса)

Обоснование вредоносности: Легитимное ПО Adobe-Acrobat не будет собирать такие данные, создавать папки со случайными названиями и выстраивать в них ту же иерархию, что и в оригинальных папках. Также оно не будет запускать себя само и тем более отправлять собранные данные куда-либо.

Объяснение механизма самозащиты после перезагрузки: программа не прописывает себя в автозагрузку через реестр, не записывается в папки автозагрузки и не записывает себя в качестве сервиса. Если же посмотреть на название ПО, то становится ясно, что это портативная сборка Adobe-Acrobat (и сам Acrobat скорее всего в ней действительно есть). То есть эта программа запускается именно пользователем вручную каждый раз через файл Adobe-Acrobat-2019-Eng-portable.exe. Вредоносное ПО пользуется своим существованием внутри портативной сборки. Таким образом, каждый раз, когда пользователь запускает Adobe-Acrobat, он запускает Stealer, который отрабатывает, крадет данные и засыпает до следующего раза.

Рекорда 1:

```
Для каждого процесса проверяем:

Доступ_к_чувствительным_данным (ДКЧД) = False

Создание_подозрительных_папок (СПП) = False

Запуск_самого_себя (ЗСС) = False

Соединение_с_контрольным_сервером (ССКС) = False

Если (операция TCP TCPCopy или TCP Receive или TCP Connect и при этом хост = 208.91.197.13 на порту 587) ССКС = True

Если (операция ReadFile с путями из приложения_1) ДКЧД = True

Если (операция CreateFile с путем *.stringConcatinate(приложение 1 в итеративном порядке)) СПП = True

Если (операция Process Create с совпадением имен вызывающего и вызываемого процессов) ЗСС = True

Если (ССКС или (ЗСС и ДКЧД и СПП)) Детект()

Если (ЗСС и ДКЧД) Предупреждение и повышенный интерес()
```

Семейство вредоносного ПО: Stealer для чувствительных данных браузеров. Мы знаем только о том, что он крадет, о механизме кражи и месте, куда данные в результате попадают мы не знаем ничего.

Рекорда 2:

```
#Операция глубокой проверки

Глубокая_проверка() {

Если (цифровая подпись нелигитимна или SHA-256 хэш не разрешен или запуск из красной зоны приложение_3 или проблема с заголовком PE-файла) Детект()

Если (процесс легитимен, но запущен нетипичным родителем) Глубокая_проверка(родителя))

Добавление в список повышенного риска

Уведомление пользователя о действиях + отправка инцидента SOC-аналитику

В данный момент безопасно()

}

#Основная логика кода

Для каждого процесса проверяем:

Если (операция ReadFile к чувствительным данным из приложения_1)

Если (имя процесса не из приложения_2 + доп. списка легитимных процессов конкретной системы или из списка запрещенных процессов или MD5 хэши приложения не совпадает с эталонным или процесс из белого списка запущен нетипичным родителем) – Глубокая_проверка()
```

Примечание: К списку повышенного риска проявляется повышенное внимание и логируются все операции, также программа отправляется на проверку.

Приложение_1 (список чувствительных адресов для Stealer):

```
%AppData%\Roaming\Mozilla\Firefox\Profiles\
%AppData%\Roaming\Mozilla\Firefox\profiles.ini
%LocalAppData%\Google\Chrome\User Data\Default\
%LocalAppData%\Google\Chrome\User Data\Local State
%LocalAppData%\Microsoft\Edge\User Data\Default\
%LocalAppData%\Microsoft\Edge\User Data\Local State
%AppData%\Opera Software\Opera Stable\
%AppData%\Opera Software\Opera GX Stable\
%LocalAppData%\BraveSoftware\Brave-Browser\User Data\Default\
%LocalAppData%\Vivaldi\User Data\Default\
%LocalAppData%\Yandex\YandexBrowser\User Data\Default\
%LocalAppData%\Chromium\User Data\Default\
%AppData%\Waterfox\Profiles\
%AppData%\Pale Moon\Profiles\
%AppData%\K-Meleon\Profiles\
%AppData%\SeaMonkey\Profiles\
%AppData%\8pecxstudios\Cyberfox\Profiles\
%LocalAppData%\Comodo\Dragon\User Data\Default\
%LocalAppData%\Epic Privacy Browser\User Data\Default\
%LocalAppData%\SlimJet\User Data\Default\
%LocalAppData%\CCleaner Browser\User Data\Default\
%LocalAppData%\CocCoc\Browser\User Data\Default\
%LocalAppData%\UR Browser\User Data\Default\
%LocalAppData%\TorBrowser\Data\Browser\profile.default\
%LocalAppData%\Iridium\User Data\Default\
%AppData%\Local\Google\Chrome\User Data\Default\Cookies
```

Приложение 2 (список легитимных приложений для доступа к чувствительным папкам):

```
Браузеры:
firefox.exe, chrome.exe, msedge.exe, opera.exe, brave.exe, vivaldi.exe, browser.exe (Яндекс),
opera_browser.exe, waterfox.exe, palemoon.exe, k-meleon.exe, seamonkey.exe, cyberfox.exe,
dragon.exe, epic_browser.exe, slimjet.exe, ccleaner_browser.exe, coc_browser.exe, ur_browser.exe,
tor_browser.exe, iridium_browser.exe, chromium.exe


Системные процессы Windows:
explorer.exe, svchost.exe, taskhostw.exe, dllhost.exe, System, Registry, Memory Compression,
```

winlogon.exe, csrss.exe, services.exe, lsass.exe, smss.exe, sihost.exe, taskeng.exe, backgroundTaskHost.exe

Антивирусные программы:

MsMpEng.exe (Windows Defender), NisSrv.exe (Windows Defender), SecurityHealthService.exe,

avp.exe (Kaspersky), avpui.exe (Kaspersky), norton.exe, nortonSecurity.exe, symantec.exe,

avastui.exe, avastsvc.exe, avgui.exe, avg.exe, mbam.exe (Malwarebytes), mbamtray.exe,

bitdefender.exe, bdagent.exe, sophos.exe, trendmicro.exe, eset.exe, mcafee.exe, comodo.exe

Утилиты резервного копирования:

acronis* (Acronis True Image), todo* (EaseUS Todo Backup), backupper* (AOMEI Backupper),

sdclt.exe (Windows Backup), wbengine.exe (Windows Backup), vssvc.exe (Volume Shadow Copy),

backup.exe, restore.exe, carbonite.exe, crashplan.exe, backupandrestore.exe

Программы очистки и оптимизации:

ccleaner.exe, ccleaner64.exe, wise* (Wise Care 365), glary* (Glary Utilities), asc.exe (Advanced SystemCare),

iobit* (IObit products), unchecky.exe, revouninstaller.exe, youruninstaller.exe, cleanmgr.exe (Disk Cleanup),

dfrgui.exe (Disk Defragmenter)

Менеджеры паролей:

lastpass* (LastPass), 1password* (1Password), dashlane* (Dashlane), keepass* (KeePass),

bitwarden.exe, enpass.exe, roboform.exe, passwordagent.exe, sticky_password.exe

Утилиты синхронизации:

dropbox.exe, googledrivesync.exe, onedrive.exe, rslsync.exe (Resilio Sync), syncthing.exe,

mega.exe, boxsync.exe, sugarsync.exe, spideroak.exe, nextcloud.exe

Разработческие инструменты:

procmon.exe (Process Monitor), procexp.exe (Process Explorer), procexp64.exe, wireshark.exe,

windbg.exe, ollydbg.exe, ida.exe, visualstudio.exe, devenv.exe, code.exe (VS Code),

processhacker.exe, api-monitor.exe, fiddler.exe, charles.exe

Легитимные системные утилиты:

```
regedit.exe, cmd.exe, powershell.exe, pwsh.exe, robocopy.exe, xcopy.exe,
wmic.exe,

schtasks.exe, tasklist.exe, taskkill.exe, net.exe, sc.exe, wscript.exe,
cscript.exe,

msiexec.exe, dism.exe, sfc.exe, chkdsk.exe, diskpart.exe



Браузерные расширения и компоненты:

firefox.exe (браузерные процессы), chrome.exe (рендерер), msedge.exe
(дочерние процессы),

brave.exe (служебные процессы), opera.exe (обновления),
software_reporter_tool.exe (Chrome Cleanup),

browser_broker.exe (Edge), crashpad_handler.exe (обработчик сбоев)



Службы обновления браузеров:

googleupdate.exe, mozilla_maintenance_service.exe, edgeupdate.exe,
operabrowserautoupdate.exe,

brave_update.exe, yandex_update.exe, vivaldi_update.exe



Приложения для работы с браузерами:

browser_assistant.exe, password_importer.exe, bookmark_sync.exe,
profile_manager.exe,

browser_cleanup.exe, extension_manager.exe, theme_installer.exe
```

Приложение 3: (красная зона запуска)

```
%TEMP%

%TMP%

%USERPROFILE%\Downloads

%USERPROFILE%\Desktop

%APPDATA%

%LOCALAPPDATA%

%PUBLIC%\Downloads

C:\$Recycle.Bin

\Windows\Temp
```