Кібератака на державні органи України з використанням шкідливої програми Cobalt Strike Beacon (CERT-UA#4145)

Загальна інформація

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA від суб'єктів координації отримано повідомлення про 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. Виконуваний файл "dropper.exe" здійснить завантаження base64-кодованих даних, та їхнє декодування в EXE-файл, розроблений з використанням мови програмування Go. Аналіз файлів продовжується. Зауважимо, що EXE-файли 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
aa5e8268e741346c76ebfd1f27941a14    one.exe (містить Cobalt Strike Beacon)
15c525b74b7251cfa1f7c471975f3f95    dropper.exe
c8bf23864162121290151757 0e96fae7   i.exe
```

Мережеві:

```
hxxps://forkscenter[.]fr/BitdefenderWindowsUpdatePackage.exe
hxxps://cdn.discordapp[.]com/attachments/947916997713358890/949948174636830761/one.exe
hxxps://cdn.discordapp[.]com/attachments/947916997713358890/949948174838165524/dropper.ex

hxxps://nirsoft[.]me/s/2MYmbwpSJLZRAtXRgNTAUjJSH6SSoicLPIrQl/field-keywords/
hxxp://45[.]84.0.116:443/i
forkscenter[.]fr (2022-01-29)
nirsoft[.]me    (2022-02-17)
45[.]84.0.116
```

Хостові:

```
%TMP%\alt.exe
%PROGRAMDATA%\one.exe
%PROGRAMDATA%\dropper.exe
```

Графічні зображення