Кібератака групи UAC-0056 на державні органи України з використанням шкідливих програм GraphSteel та GrimPlant (CERT-UA#4293)

Загальна інформація

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA отримано інформацію щодо розповсюдження електронних листів з темою "Заборгованість по зарплаті" серед державних органів України. У додатку до листа знаходиться документ "Заборгованість по зарплаті.xls", який містить легітимні статистичні дані та макрос. Разом з тим, до згаданого документу у вигляді вкладення додано hex-кодовані дані. Макрос, після активації, здійснить декодування даних, створення EXE-файлу "Base-Update.exe" на комп'ютері та його виконання.

Згаданий файл є програмою-завантажувачем, розробленою з використанням мови програмування GoLang. Програма здійснить завантаження і запуск іншого завантажувача, який, у свою чергу, забезпечить завантаження і запуск на комп'ютері шкідливих програм GraphSteel та GrimPlant.

Виявлену активність асоційовано з дільністю групи UAC-0056.

Індикатори компрометації

Файли:

```
da305627acf63792acb02afaf83d94d1
c1afb561cd5363ac5826ce7a72f0055b400b86bd7524da43474c94bc480d7eff
Заборгованість по зарплаті.xls
06124da5b4d6ef31dbfd7a6094fc52a6
9e9fa8b3b0a59762b429853a36674608df1fa7d7f7140c8fccd7c1946070995a    Base-
Update.exe (GoDownloader)
36ff9ec87c458d6d76b2afbd5120dfae
8ffe7f2eeb0cbfbe158b77bbff3e0055d2ef7138f481b4fac8ade6bfb9b2b0a1    java-
sdk.exe (GoDownloader)
4a5de4784a6005aa8a19fb0889f1947a
99a2b79a4231806d4979aa017ff7e8b804d32bfe9dcc0958d403dfe06bdd0532    oracle-
java.exe (GrimPlant)
6b413beb61e46241481f556bb5cdb69c
c83d8b36402639ea3f1ad5d48edc1a22005923aee1c1826afabe27cb3989baa3
microsoft-cortana.exe (GraphSteel) (2022-03-20)
```

Мережеві:

```
hxxp://194[.]31.98.124:443/i
hxxp://194[.]31.98.124:443/p
hxxp://194[.]31.98.124:443/m
ws://194[.]31.98.124:443/c
194[.]31.98.124
```

Хостові:

```
%TMP%\Base-Update.exe
%USERPROFILE%\.java-sdk\java-sdk.exe
%USERPROFILE%\.java-sdk\oracle-java.exe
%USERPROFILE%\.java-sdk\microsoft-cortana.exe
```

Графічні зображення