cert.gov.ua /article/18273

CERT-UA

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA отримано інформацію щодо розповсюдження, начебто, від імені Національної служби здоров'я України, електронних поштових повідомлень, що містили посилання на ZIP-архів, розміщений на публічному сервісі Discord.

Згаданий ZIP-архів містить документ-приманку та два ідентичні файли-ярлики, у випадку відкриття яких на комп'ютері жертви буде виконано powershell-команду, що, в свою чергу, призведе до завантаження і запуску шкідливої програми OutSteel (дата компіляції: 28.01.2022). Остання забезпечить пошук та викрадення документів на комп'ютері жертви, а також завантажить і виконає шкідливу програму SaintBot (дата компіляції: 30.04.2021).

Згадана активність спрямована на державні організації України. Відслідковується CERT-UA не пізніше ніж з квітня 2021 року за ідентифікатором UAC-0056.

Індикатори компрометації

Файли:

```
0e16df6845cde1260087902f25842f79        d5aadb4ace8ffccb.zip
fa23f43fa759f0f38cde2b703d98ba05        Додаток_2.docx
7de66b5c7d3ddae321fa6cfeeaa94819        Додаток_1.docx.lnk
78e941e780adc1a159fdc7090194c96d        up74987340.exe
ede3bf69a09cec27ded2d20c95ca78e3        up74987340.dec.exe (OutSteel)
363e2b62f93c58c177e58dbe0a247fa0        load74h74830.exe
ab2a92e0fc5a6f63336e442f34089f16        1406.exe (SaintBot)
```

Мережеві:

```
hxxps://cdn.discordapp[.]com/attachments/908281957039869965/937420906286952568/d5aadb4ace8ffcc

hxxp://eumr[.]site/up74987340.exe
hxxp://eumr[.]site/load74h74830.exe
hxxp://185.244.41[.]109:8080/upld/
hxxp://8003659902[.]space/wp-adm/gate.php
hxxp://smm2021[.]net/wp-adm/gate.php
hxxp://8003659902[.]site/wp-adm/gate.php
eumr[.]site
8003659902[.]space
smm2021[.]net
8003659902[.]site
1000020[.]xyz
185.244.41[.]109
testsid@lthhc-zm[.]com
```

Хостові:

```
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\<назва_файлу>.exe
%TEMP%\rmm.bat
%TEMP%\svjhost.exe
%LOCALAPPDATA%\zz%USER%\
```

Додаткова інформація

OutSteel – шкідлива програма, розроблена з використанням мови програмування AutoIt; основний функціонал – викрадення файлів за визначеним переліком розширень файлів (передавання файлів на сервер управління здійснюється за допомогою HTTP POST-запитів).

Наголошуємо на необхідності додаткового моніторингу з'єднань з публічним сервісом Discord.

Графічні зображення

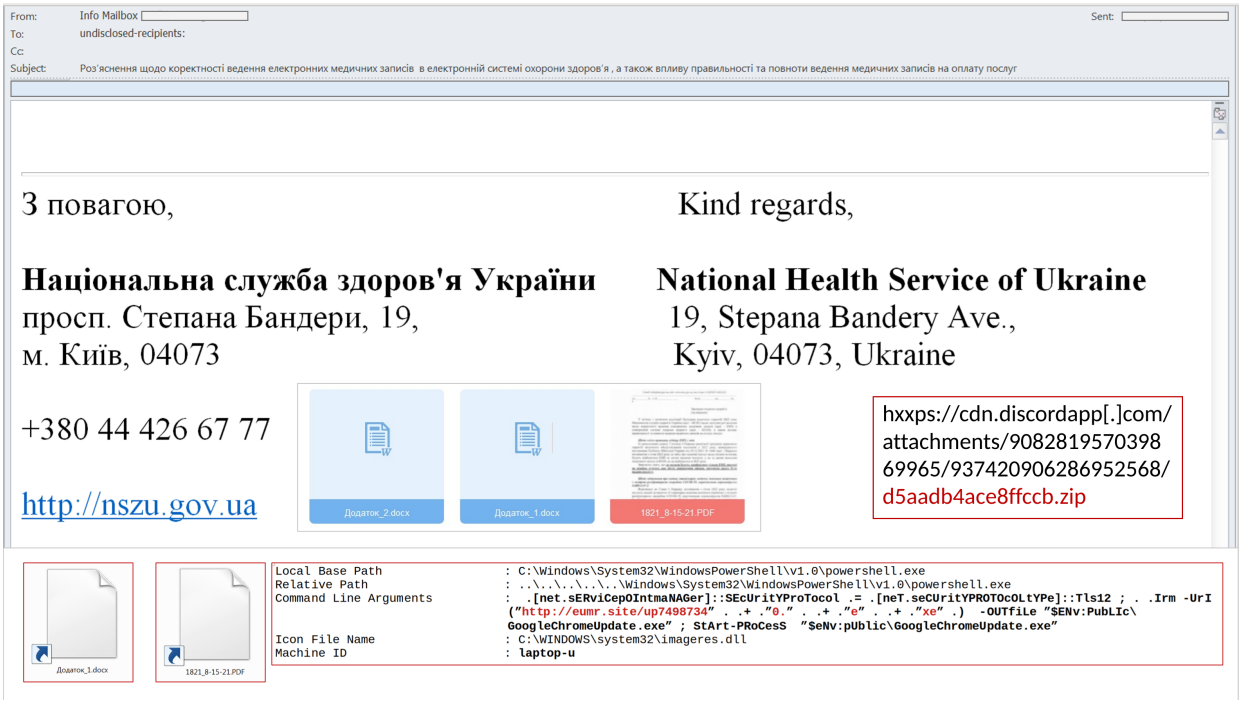

Рис. 1 Приклад шкідливого електронного листа

Рис. 2 Приклад програмного коду шкідливої програми OutSteel