CERT-UA

General information

The orderly command of the response on the computer of the supremacy of Ukraine CERT-UA took away the information about the rozpovsudzhennya, nachebto, in the name of the National Health Service of Ukraine, electronic mail notifications, which were sent to the ZIP-archive

ZIP-archives guessing to avenge a decoy document and two identical shortcut files, when they appear on the victim's computer, a powershell command will be written, which, in its turn, will lead to the capture and launch of the OutSteel program (compilation date: 28.01. 2022). It remains to secure the search for stolen documents on the victim's computer, as well as to grab and download the SaintBot program (compilation date: 04/30/2021).

This activity is directed at the state organizations of Ukraine. Valid for CERT-UA no later than April 2021 under identifier UAC-0056.

Indicators of compromise

Files:

```
0e16df6845cde1260087902f25842f79 d5aadb4ace8ffccb.zip
fa23f43fa759f0f38cde2b703d98ba05 Addendum_2.docx
7de66b5c7d3ddae321fa6cfeeaa94819 Addendum_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%\
```

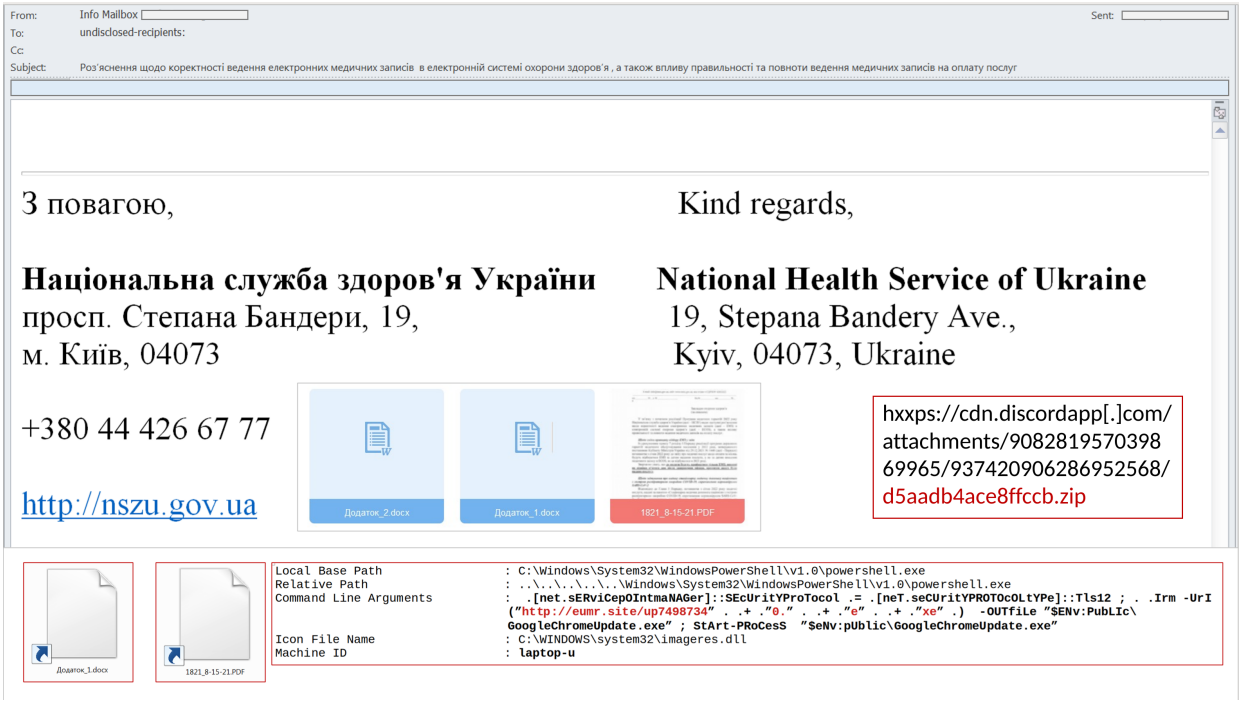
Додаткова інформація

OutSteel - a slick program, divided into different versions of AutoIt; the main functionality is the transfer of files after a specific transfer of file extensions (transferring files to the control server is required for the help of HTTP POST

requests).

We swear on the need for additional monitoring of the connection with the public Discord service.

Graphic images



Rice. 1 Butt of a swivel electronic sheet

Rice. 2 Application of the program code of the OutSteel program