# Кібератака на державні органи України з використанням шкідливої програми PseudoSteel (CERT-UA#4299)

Кібератака на державні органи України з використанням шкідливої програми PseudoSteel (CERT-UA#4299)

**Загальна інформація**

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA виявлено SFX-архів "Інформація_щодо_втрат_військовослужбовців_ЗС_України.docx.exe", який містить файл-приманку "Втрати-1001.docx", а також UPX-стиснутий файл "googleupdate.exe", дата компіляції: 26.03.2022.

В результаті проведеного аналізу згаданий EXE-файл класифіковано як шкідливу програму PseudoSteel, що розроблена з використанням мови програмування C++ (компілятор: Mingw-w64) та функціонально забезпечує пошук на комп'ютері файлів за переліком розширень (*.txt, *.doc, *.docx, *.pdf, *.xls, *.xlsx, *.ppt, *.pptx, *.odt, *.rtf, *.zip, *.rar, *.7z), а також їхнє вивантаження на FTP-сервер. Можливий перелік місць пошуку файлів визначається в конфігурації (%SYSTEMDRIVE%, %USERPROFILE%\Documents, %USERPROFILE%\Desktop, %TMP%, USB-пристрої; також можливо зазначити довільний шлях).

З низьким рівнем впевненості активність асоційовано з діяльністю групи UAC-0010 (Armageddon).

**Індикатори компрометації**

*Файли:*

```
eda76ae28628c64d9e12a86adef6dc69
13eaa638d071e7dc124cf982b8777c6ef50a3d9dc8c57d22d23abe1bae5560f5
Інформація_щодо_втрат_військовослужбовців_ЗС_України.docx.exe
878c30bdefb1b76ea10823a6d5a32f89
bab351b5f19ecaa24eaa438dd93decd5587e0b441fc43b78893ca2e207b2cb2f
googleupdate.exe (26.03.2022)
55cafceba527c3e68852b1af071929c0
78b492e211e91b1ef9a4bcd5ba80c9572545d5f3f63d3071e3253dcec3a5d97c
googleupdate.deupx.exe
5d29da2285390164a0a7d80e6ed23da7
c50972c11ffd1da9e0ed670b99296f75ec52933699790285d050c0654c21fda3
Втрати-1001.docx (документ-приманка)
```

*Мережеві:*

```
ftp[:]//webdavml07.bplaced[.]net:21
webdavml07.bplaced[.]net
```

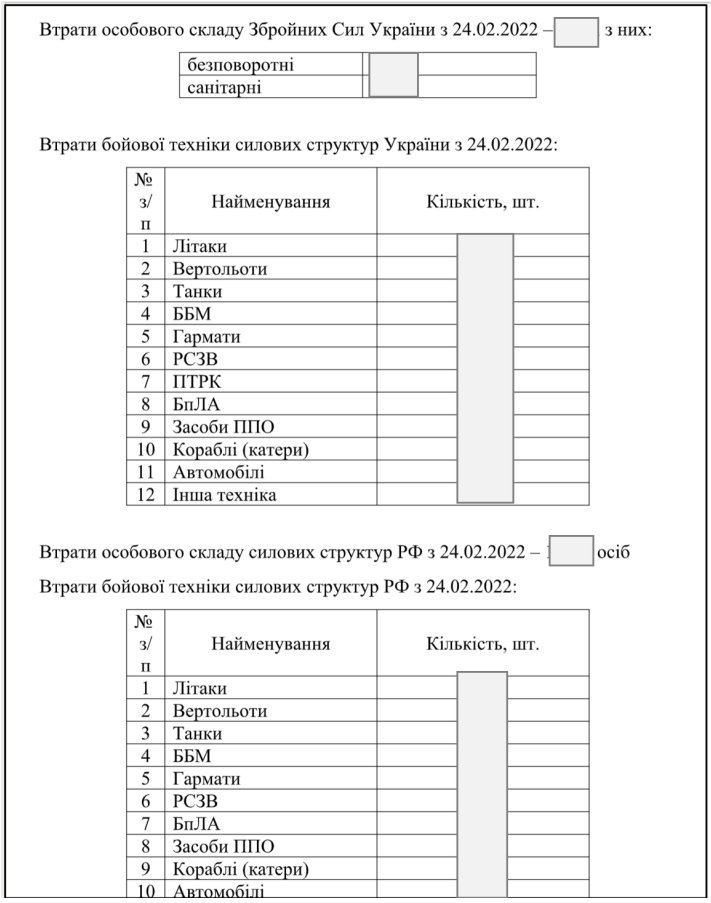
*Процеси:*

```
ping -n 8 127.0.0.1
```

### Рекомендації

Наголошуємо на необхідності зменшення поверхні атаки шляхом фільтрації вихідних інформаційних потоків.

### Графічні зображення



Втрати особового складу Збройних Сил України з 24.02.2022 – з них:

| | |
|---|---|
| безповоротні | |
| санітарні | |

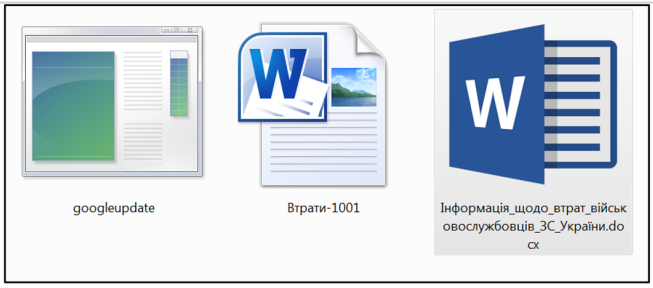
Втрати бойової техніки силових структур України з 24.02.2022:

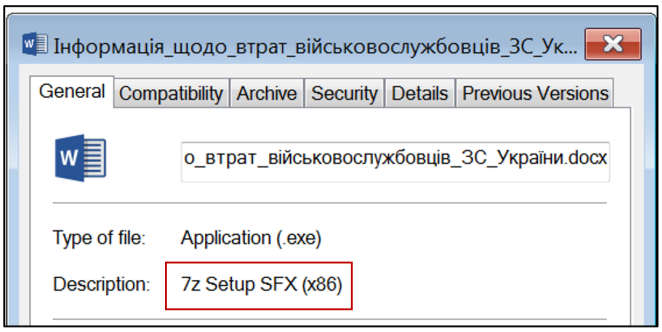
| № з/п | Найменування | Кількість, шт. |
|---|---|---|
| 1 | Літаки | |
| 2 | Вертольоти | |
| 3 | Танки | |
| 4 | ББМ | |
| 5 | Гармати | |
| 6 | РСЗВ | |
| 7 | ПТРК | |
| 8 | БпЛА | |
| 9 | Засоби ППО | |
| 10 | Кораблі (катери) | |
| 11 | Автомобілі | |
| 12 | Інша техніка | |

Втрати особового складу силових структур РФ з 24.02.2022 – осіб

Втрати бойової техніки силових структур РФ з 24.02.2022:

| № з/п | Найменування | Кількість, шт. |
|---|---|---|
| 1 | Літаки | |
| 2 | Вертольоти | |
| 3 | Танки | |
| 4 | ББМ | |
| 5 | Гармати | |
| 6 | РСЗВ | |
| 7 | БпЛА | |
| 8 | Засоби ППО | |
| 9 | Кораблі (катери) | |
| 10 | Автомобілі | |




```
;!@Install@!UTF-8!
RunProgram="hidcon:nowait:googleupdate.exe"
RunProgram="hidcon:nowait:explorer Втрати-1001.docx.docx"
RunProgram="hidcon:ping -n 8 127.0.0.1"
GUIMode="2"
OverwriteMode="2"
#SelfDelete="1"
;!@InstallEnd@!
```