cert-gov-ua.translate.goog /article/38371

Cyberattack on state bodies of Ukraine using PseudoSteel malware (CERT-UA # 4299)

General Information

The Governmental Computer Emergency Response Team of Ukraine CERT-UA has discovered the SFX-archive "Information_about_Loss_of_Servicemen_of_Ukraine.docx.exe", which contains the lure file "Loss-1001.docx", as well as the UPX-compressed file "goo". compilation date: March 26, 2022.

As a result of the analysis, the mentioned EXE-file is classified as a malicious program PseudoSteel, developed using the C ++ programming language (compiler: Mingw-w64) and functionally provides search on the computer files by extension (* .txt, * .doc, * .docx, * .pdf, * .xls, * .xlsx, * .ppt, * .pptx, * .odt, * .rtf, * .zip, * .rar, * .7z), as well as their upload to FTP -server. A possible list of file search locations is defined in the configuration (% SYSTEMDRIVE%,% USERPROFILE% \ Documents,% USERPROFILE% \ Desktop,% TMP%, USB devices; it is also possible to specify any path).

With a low level of confidence, the activity is associated with the activities of the group UAC-0010 (Armageddon).

Indicators of compromise

Files:

```
eda76ae28628c64d9e12a86adef6dc69
13eaa638d071e7dc124cf982b8777c6ef50a3d9dc8c57d22d23abe1bae5560f5
878c30bdefb1b76ea10823a6d5a32f89
bab351b5f19ecaa24eaa438dd93decd5587e0b441fc43b78893ca2e207b2cb2f
googleupdate.exe (26.03.2022)
55cafceba527c3e68852b1af071929c0
78b492e211e91b1ef9a4bcd5ba80c9572545d5f3f63d3071e3253dcec3a5d97c
googleupdate.deupx.exe
5d29da2285390164a0a7d80e6ed23da7
c50972c11ffd1da9e0ed670b99296f75ec52933699790285d050c0654c21fda3 Loss-
1001.docx (bait document)
```

Network:

```
ftp [:] // webdavml07.bplaced [.] no: 21
webdavml07.bplaced [.] no
```

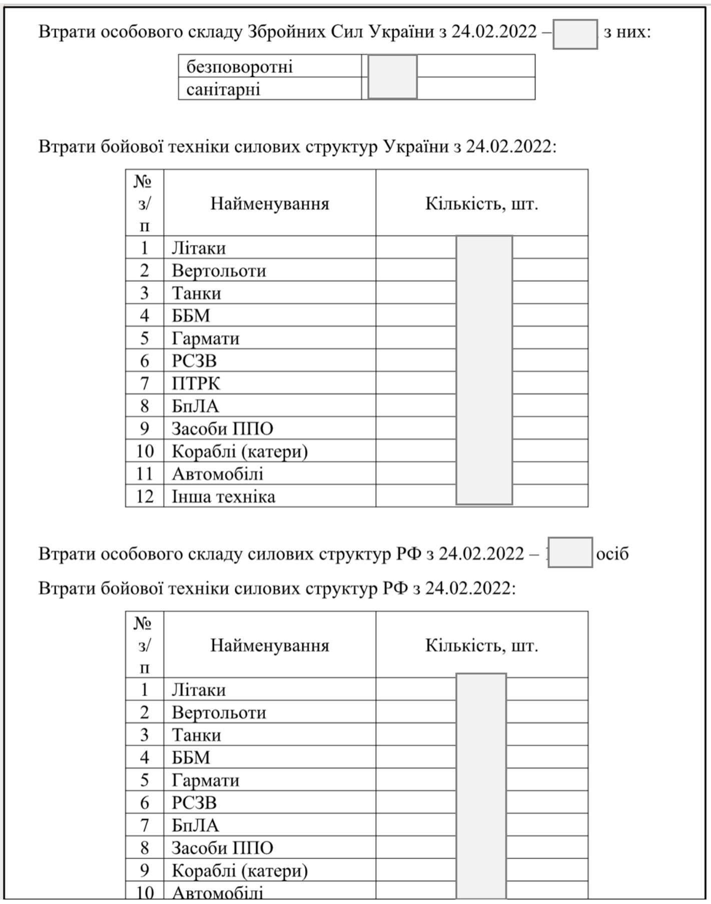
Processes:

```
ping -n 8 127.0.0.1
```

Recommendations

We emphasize the need to reduce the attack surface by filtering the output information flows.

Graphic images



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

безповоротні		
санітарні		

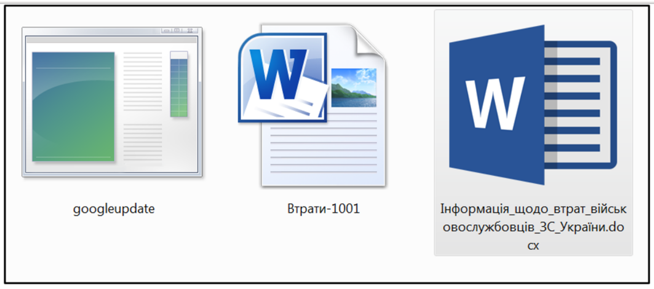
Втрати бойової техніки силових структур України з 24.02.2022:

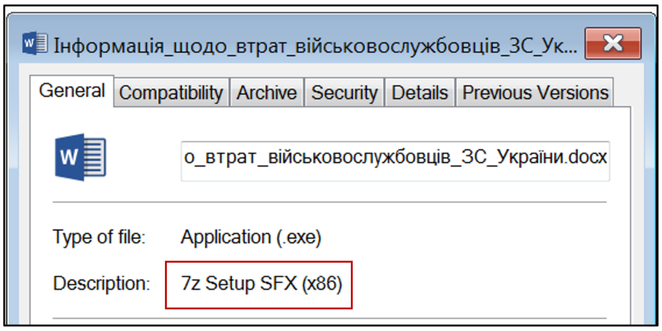
№ з/п	Найменування	Кількість, шт.
1	Літаки	
2	Вертольоти	
3	Танки	
4	ББМ	
5	Гармати	
6	РСЗВ	
7	ПТРК	
8	БпЛА	
9	Засоби ППО	
10	Кораблі (катери)	
11	Автомобілі	
12	Інша техніка	

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	

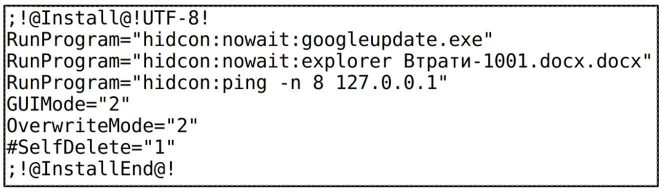




о_втрат_військовослужбовців_ЗС_України.docx

Type of file: Application (.exe)

Description: 7z Setup SFX (x86)



```
;!@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@!
```