

CERT-UA

Archived: 2026-04-05 18:45:00 UTC

Оновлено 22.12.2022

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA 17.12.2022 від Центру інновацій та розвитку оборонних технологій Міністерства оборони України отримано інформацію щодо розповсюдження засобами електронної пошти (з використанням скомпрометованої електронної адреси одного зі співробітників оборонного відомства), а також, месенджерів, повідомлення щодо необхідності оновлення сертифікатів в системі "DELTA". При цьому, вкладення у вигляді PDF-документів імітують легітимні дайджести підрозділу ISTAR ОУВ "Запоріжжя", але містять посилання на шкідливий ZIP-архів.

У разі переходу за посиланням на комп'ютер буде завантажено архів "certificates_rootca.zip", що містить виконуваний файл "certificates_rootCA.exe", захищений за допомогою VMProtect (файл скомпільовано та підписано цифровим підписом 15.12.2022).

Після запуску EXE-файлу на ЕОМ буде створено декілька DLL-файлів, також захищених VMProtect, і файл "ais.exe", що імітує процес встановлення сертифікату. В подальшому, на комп'ютері жертви буде здійснено запуск шкідливої програми RomCom (реєструється як COM-сервер замість oleaut32.dll), яка, у свою чергу, забезпечить виконання двох шкідливих програм: FateGrab ("FileInfo.dll"; "ftp_file_graber.dll"), функціонал якого передбачає викрадення файлів з розширеннями: '.txt', '.rtf', '.xls', '.xlsx', '.ods', '.cmd', '.pdf', '.vbs', '.ps1', '.one', '.kdb', '.kdbx', '.doc', '.docx', '.odt', '.eml', '.msg', '.email' з їх подальшою ексфільтрацією за допомогою FTP, та StealDeal ("procsys.dll"; "StealDll.dll"), призначений, серед іншого, для отримання та збереження даних Інтернет-браузерів у відповідні файли, що потім будуть ексфільтровані за допомогою RomCom з використанням протоколу HTTPS.

Активність відстежується за ідентифікатором UAC-0142, проте має схожості з кластером загроз UAC-0132 (CERT-UA#5509).

Індикатори компрометації

Файли:

d42e12a973be47c6ddd0b4a7c3a36536
4ca23d887f85206d926c1caab0b7ddb3
4e43623f2e9a31e39b62bc002b2223e9
3ddcd818f1e39467214c5b7153e2a3a0
8a54222486372f92323b9e4279e9e9c2
46cf25a8f1c22910cbc74a4b808fb926
ef802adb77dd0d0b8277994e720db2ca

60a7f038cad5086b85f0be169f478a6b06f59785c2138fc64c8fdce88f049968
f671f9c7b8d6b2553db8c563d269aa52d573857f34d58b7a9539e9d8aea9f3d5
a1a8e73ff09d5b55a6156e68c56b5cbf80cc4b9957f02e6c52136654956e334d
5d3cf96ee5e42e8f3d6548dd4fcf804ef5d5844220157ae9242cadf60a3afb3c
1c722ba09cdfb91fa6420b09f47aa15aaf7346d30f3974940d3bc73cdc84783f
6330248e2933a7ebdc873d05d7775f039a55b794eebda78ca0902b110a54c31
eadb75944134da5434174981bf295eed40d9b2404df8e6dbf12962b2e5075fa3

```
13942c7497a15176b39cac1ac7aa79df 03645ad472c8cce66b6089fb8f98bcd9027ca8ab2e01d404af09276efb84703f
e82f2226b6432fa41e15208c6f53e4ac 4122f8a6e211a8f1064ef793022ce94f64542b9eb643927a4a7beae643eee06b
bf39ee86518f69a54f004fe734e22e3c 71dae65285224050c609c8c498160df604c6a00afa34dded6aea99ed843a21c3
900d06af063b2cda241d04da62fa1662 6850e8c4d3d774dfac1c5e09df3a9acc6d97b7afb66c8417ad80b5632f9e936d
6f3ca264e301ea5b68a61ffe2051e946 14765706b2de10b6f9a90268c7690222d2ea5155c9fa24317b86e6c0231d913e
```

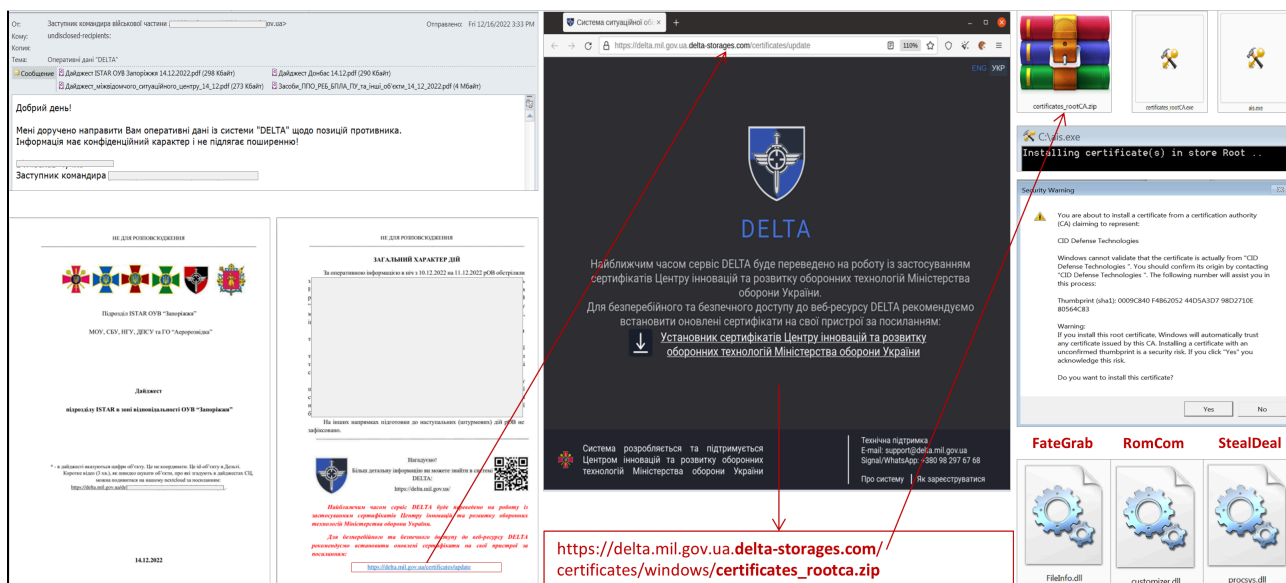
Хостові:

```
Great C Technologies Inc
0B 59 BB 29 99 06 6C A6 B0 A2 81 C1 B3 55 B9 9A
C:\Users\Public\Libraries\FileInfo.dll
C:\Users\Public\Libraries\BrowserData\procsys.dll
C:\Users\Public\Libraries\BrowserData\Result\
C:\Users\Public\Libraries\BrowserData\Result\LoginData.csv
C:\Users\Public\Libraries\BrowserData\Result\Mozilla Firefox@%USERNAME%Cookies.csv
C:\Users\Public\Libraries\BrowserData\Result\%USERNAME%Credits.csv
C:\Users\Public\Libraries\BrowserData\Result\%USERNAME%History.csv
%TMP%\ais.exe
%TMP%\temp.cmd
%TMP%\19207187.dll (ім'я файлу динамічне)
%TMP%\[0-9]+.dll
C:\Users\Public\Libraries19208093.dll (ім'я файлу динамічне)
C:\Users\Public\Libraries[0-9]+.dll
C:\Users\Public\Libraries\rtmpak1981674535.dll0 (ім'я файлу динамічне)
C:\Users\Public\Libraries\rtmpak[0-9]+.dll0
rundll32.exe %TMP%\19207187.dll,MimeSource
rundll32.exe C:\Users\Public\Libraries\rtmpak2235685807.dll0,fIt
rundll32.exe C:\Users\Public\Libraries\BrowserData\procsys.dll,stub
rundll32.exe C:\Users\Public\Libraries\FileInfo.dll,fSt %FTP_LOGIN%:%FTP_PASSWORD%:%CAMPAIGN_ID%
cmd.exe /c C:\Users\Public\Libraries\temp.cmd C:\Users\Public\Libraries\FileInfo.dll
cmd.exe /c %TMP%\temp.cmd %TMP%\ais.exe C:\Users\%USERNAME%\Desktop\certificates_rootCA.exe
nltest /domain_trusts
```

Мережеві:

```
hxxps://delta.mil.gov.ua.delta-storages[.]com/certificates/update
hxxps://delta.mil.gov.ua.delta-storages[.]com/certificates/windows/certificates_rootca.zip
hxxps://46.249.49[.]109:4444
hxxps://hexactor[.]com:4444
ftp://46.249.49[.]109
delta.mil.gov.ua.delta-storages[.]com
delta-storages[.]com (2022-12-15; @webnic[.]cc)
hexactor[.]com (2022-11-12; @namesilo[.]com; gor4j3d@proton[.]me)
46.249.49[.]109 (@serverius[.]net)
```

Графічні зображення



Source: <https://cert.gov.ua/article/3349703>