Кібератака на користувачів системи DELTA з використанням шкідливих програм RomCom/FateGrab/StealDeal (CERT-UA#5709)

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, мессенджерів, 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
60a7f038cad5086b85f0be169f478a6b06f59785c2138fc64c8fdce88f049968
certificates_rootca.zip
```

4ca23d887f85206d926c1caab0b7ddb3
f671f9c7b8d6b2553db8c563d269aa52d573857f34d58b7a9539e9d8aea9f3d5
certificates_rootCA.exe
4e43623f2e9a31e39b62bc002b2223e9
a1a8e73ff09d5b55a6156e68c56b5cbf80cc4b9957f02e6c52136654956e334d ais.exe
(2022-12-15 08:57:54)
3ddcd818f1e39467214c5b7153e2a3a0
5d3cf96ee5e42e8f3d6548dd4fcf804ef5d5844220157ae9242cadf60a3afbac temp.cmd
8a54222486372f92323b9e4279e9e9c2
1c722ba09cdfb91fa6420b09f47aa15aaf7346d30f3974940d3bc73cdc84783f temp.cmd
46cf25a8f1c22910cbc74a4b808fb926
6330248e2933a7ebdc873d05d7775f039a55b794eebdda78ca0902b110a54c31
procsys.dll (StealDeal) (2022-12-14 13:21:47)
ef802adb77dd0d0b8277994e720db2ca
eadb75944134da5434174981bf295eed40d9b2404df8e6dbf12962b2e5075fa3
FileInfo.dll (FateGrab) (2022-12-14 12:03:50)
13942c7497a15176b39cac1ac7aa79df
03645ad472c8cce66b6089fb8f98bcd9027ca8ab2e01d404af09276efb84703f
19207187.dll (2022-12-15 09:01:47)
e82f2226b6432fa41e15208c6f53e4ac
4122f8a6e211a8f1064ef793022ce94f64542b9eb643927a4a7beae643eee06b
regInjecttNew_pumped.dll (2022-12-15 09:02:13)
bf39ee86518f69a54f004fe734e22e3c
71dae65285224050c609c8c498160df604c6a00afa34dded6aea99ed843a21c3
customizer.dll (RomCom) (2022-12-15 08:59:32)
900d06af063b2cda241d04da62fa1662
6850e8c4d3d774dfac1c5e09df3a9acc6d97b7afb66c8417ad80b5632f9e936d
Libraries19208093.dll (550MB+)
6f3ca264e301ea5b68a61ffe2051e946
14765706b2de10b6f9a90268c7690222d2ea5155c9fa24317b86e6c0231d913e
rtmpak2235685807.dll0 (700MB+)

Хостові:

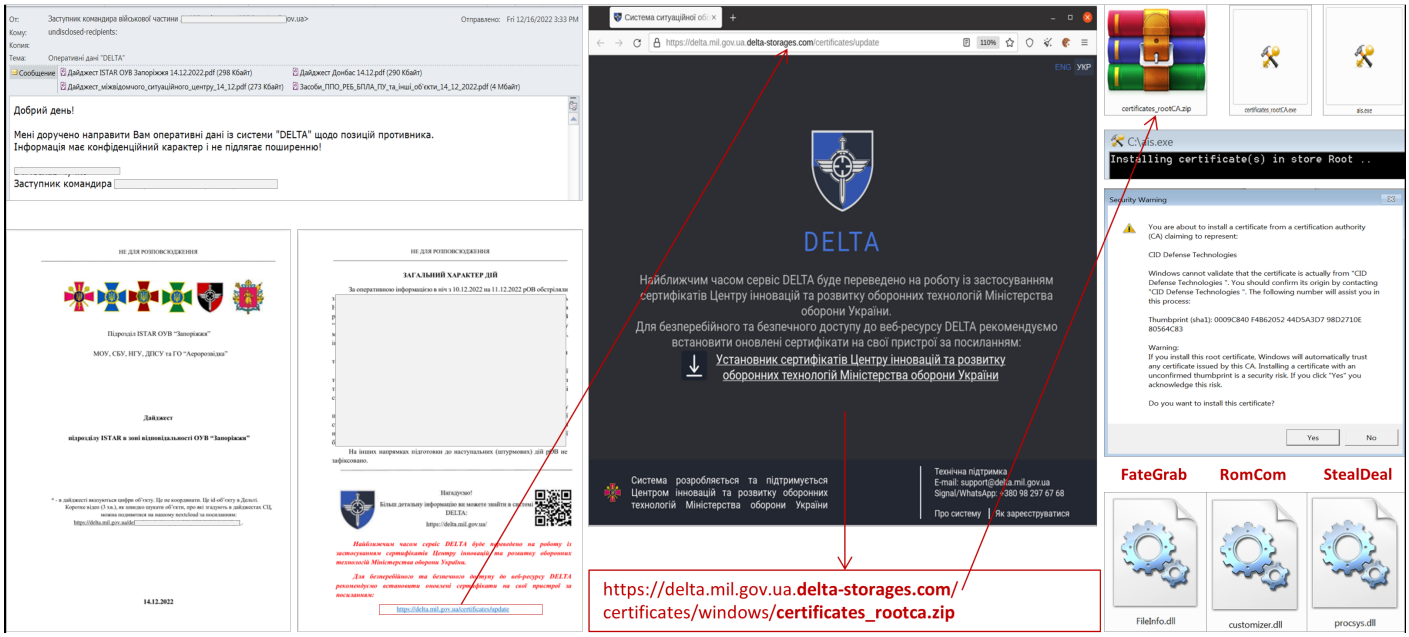
Great C Technologies Inc
0B 59 BB 29 99 06 6C A6 B0 A2 81 C1 B3 55 B9 9A
C:\Users\Public\Libraries\FileInfo.dll
C:\Users\Public\Libraries\BrowserData\procsys.dll
C:\Users\Public\Libraries\BrowserData\Result\
C:\Users\Public\Libraries\BrowserData\Result\LoginData.csv
C:\Users\Public\Libraries\BrowserData\Result\Mozilla
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


Добрий день!
Мені доручено направити Вам оперативні дані із системи "DELTA" щодо позицій противника.
Інформація має конфіденційний характер і не підлягає поширенню!
Заступник командира
НЕ ДЛЯ РОЗПОВСЮДЖЕННЯ
Підрозділ ISTAR ОУВ "Запоріжжя"
МОУ, СБУ, НГУ, ДПСУ та ГО "Аеророзвідка"
Дайджест
підрозділу ISTAR в зоні відповідальності ОУВ "Запоріжжя"
14.12.2022
НЕ ДЛЯ РОЗПОВСЮДЖЕННЯ
ЗАГАЛЬНИЙ ХАРАКТЕР ДІЙ
Нагадуємо!
Більш детальну інформацію ви можете знайти в системі DELTA:
https://delta.mil.gov.ua/
Найближчим часом сервіс DELTA буде переведено на роботу із застосуванням сертифікатів Центру інновацій та розвитку оборонних технологій Міністерства оборони України.
Для безперебійного та безпечного доступу до веб-ресурсу DELTA рекомендуємо встановити оновлені сертифікати на свої пристрої за посиланням:
https://delta.mil.gov.ua/certificates/update
Система ситуаційної
https://delta.mil.gov.ua.delta-storages.com/certificates/update
ENG УКР
DELTA
Найближчим часом сервіс DELTA буде переведено на роботу із застосуванням сертифікатів Центру інновацій та розвитку оборонних технологій Міністерства оборони України.
Для безперебійного та безпечного доступу до веб-ресурсу DELTA рекомендуємо встановити оновлені сертифікати на свої пристрої за посиланням:
Установник сертифікатів Центру інновацій та розвитку оборонних технологій Міністерства оборони України
Система розробляється та підтримується Центром інновацій та розвитку оборонних технологій Міністерства оборони України
Технічна підтримка
E-mail: support@delta.mil.gov.ua
Signal/WhatsApp: +380 98 297 67 68
Про систему
Як зареєструватися
certificates_rootCA.zip
certificates rootCA.exe
as.exe
C:\as.exe
Installing certificate(s) in store Root ..
Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
CID Defense Technologies
Windows cannot validate that the certificate is actually from "CID Defense Technologies ". You should confirm its origin by contacting "CID Defense Technologies ". The following number will assist you in this process:
Thumbprint (sha1): 0009C840 F4B62052 44D5A3D7 98D2710E 80564C83
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No
FateGrab
RomCom
StealDeal
FileInfo.dll
customizer.dll
procsys.dll
https://delta.mil.gov.ua.delta-storages.com/certificates/windows/certificates_rootca.zip