Ukraine's DELTA military system users targeted by info-stealing malware

bleepingcomputer.com/news/security/ukraines-delta-military-system-users-targeted-by-info-stealing-malware/

Bill Toulas

By
Bill Toulas

- December 19, 2022
- 12:39 PM
- 1

A compromised Ukrainian Ministry of Defense email account was found sending phishing emails and instant messages to users of the 'DELTA' situational awareness program to infect systems with information-stealing malware.

The campaign was highlighted in a report today by CERT-UA (Computer Emergency Response Team of Ukraine), which warned Ukrainian military personnel of the malware attack.

DELTA is an intelligence collection and management system created by Ukraine with the help of its allies to help the military track the movements of enemy forces.

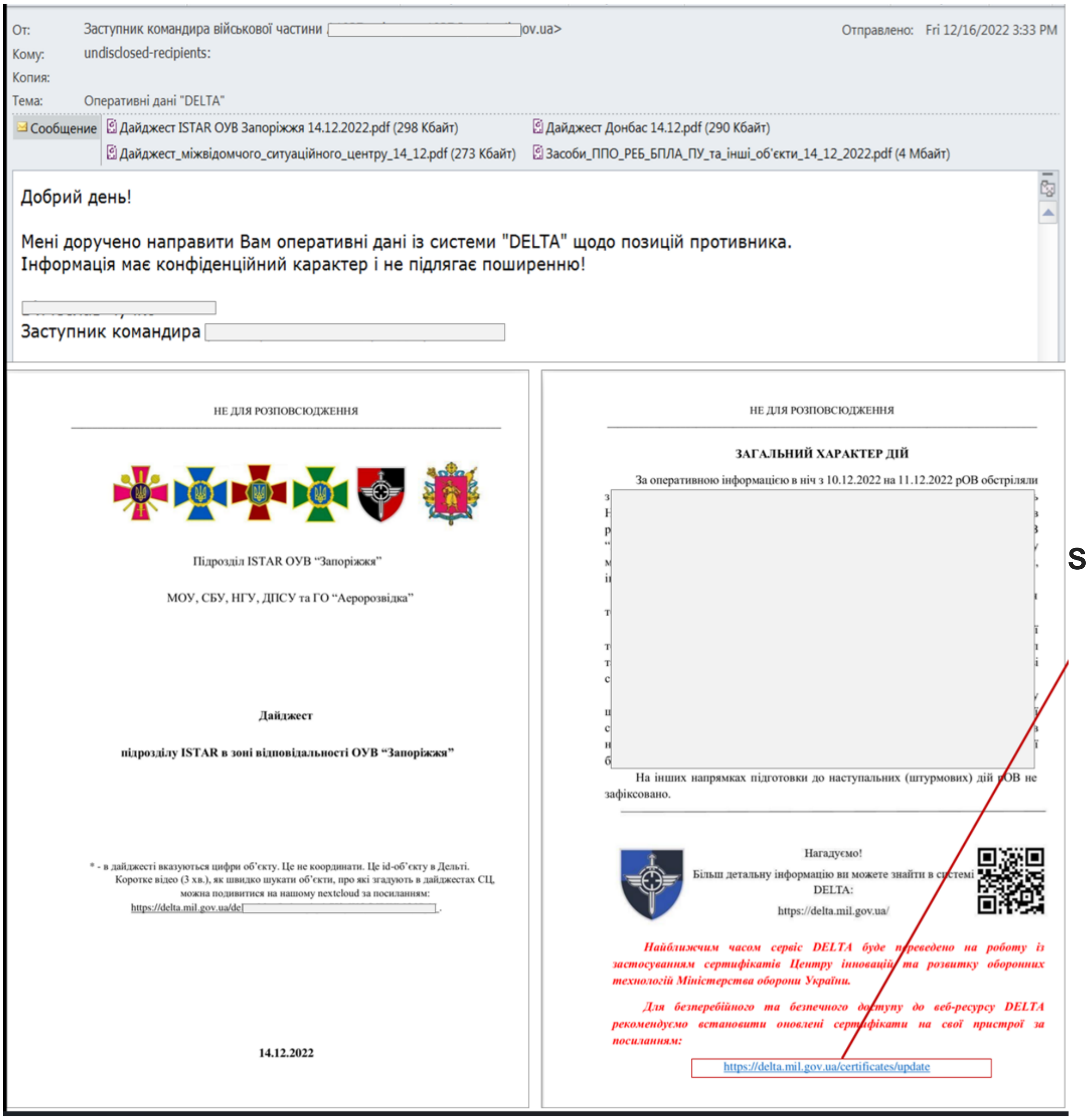
The system provides comprehensive real-time information with high-level integration from multiple sources on a digital map that can run on any electronic device, from a laptop to a smartphone.

Digital certificates are used for signing software code and authenticating servers, telling security products running on the OS that the application has not been tampered with and that the server operator is who they claim to be.

Infection process

As part of this campaign, threat actors used email or instant messages with fake warnings that users need to update the 'Delta' certificates to continue using the system securely.

The malicious email contains a PDF document purportedly with certificate installation instructions, which includes links to download a ZIP archive named "certificates_rootCA.zip."



От: Заступник командира військової частини [redacted]ov.ua>

Отправлено: Fri 12/16/2022 3:33 PM

Кому: undisclosed-recipients:

Копия:

Тема: Оперативні дані "DELTA"

Дайджест ISTAR ОУВ Запоріжжя 14.12.2022.pdf (298 Кбайт)

Дайджест Донбас 14.12.pdf (290 Кбайт)

Дайджест_міжвідомчого_ситуаційного_центру_14_12.pdf (273 Кбайт)

Засоби_ППО_РЕБ_БПЛА_ПУ_та_інші_об'єкти_14_12_2022.pdf (4 Мбайт)

Добрий день!

Мені доручено направити Вам оперативні дані із системи "DELTA" щодо позицій противника.
Інформація має конфіденційний характер і не підлягає поширенню!

[redacted]

Заступник командира [redacted]

НЕ ДЛЯ РОЗПОВСЮДЖЕННЯ

Підрозділ ISTAR ОУВ "Запоріжжя"

МОУ, СБУ, НГУ, ДПСУ та ГО "Аеророзвідка"

Дайджест

підрозділу ISTAR в зоні відповідальності ОУВ "Запоріжжя"

* - в дайджесті вказуються цифри об'єкту. Це не координати. Це id-об'єкту в Дельті.
Коротке відео (3 хв.), як швидко шукати об'єкти, про які згадують в дайджестах СЦ,
можна подивитися на нашому nextcloud за посиланням:
https://delta.mil.gov.ua/de[redacted].

14.12.2022

НЕ ДЛЯ РОЗПОВСЮДЖЕННЯ

ЗАГАЛЬНИЙ ХАРАКТЕР ДІЙ

За оперативною інформацією в ніч з 10.12.2022 на 11.12.2022 рОВ обстріляли [redacted]

На інших напрямках підготовки до наступальних (штурмових) дій рОВ не зафіксовано.

Нагадуємо!

Більш детальну інформацію ви можете знайти в системі DELTA:

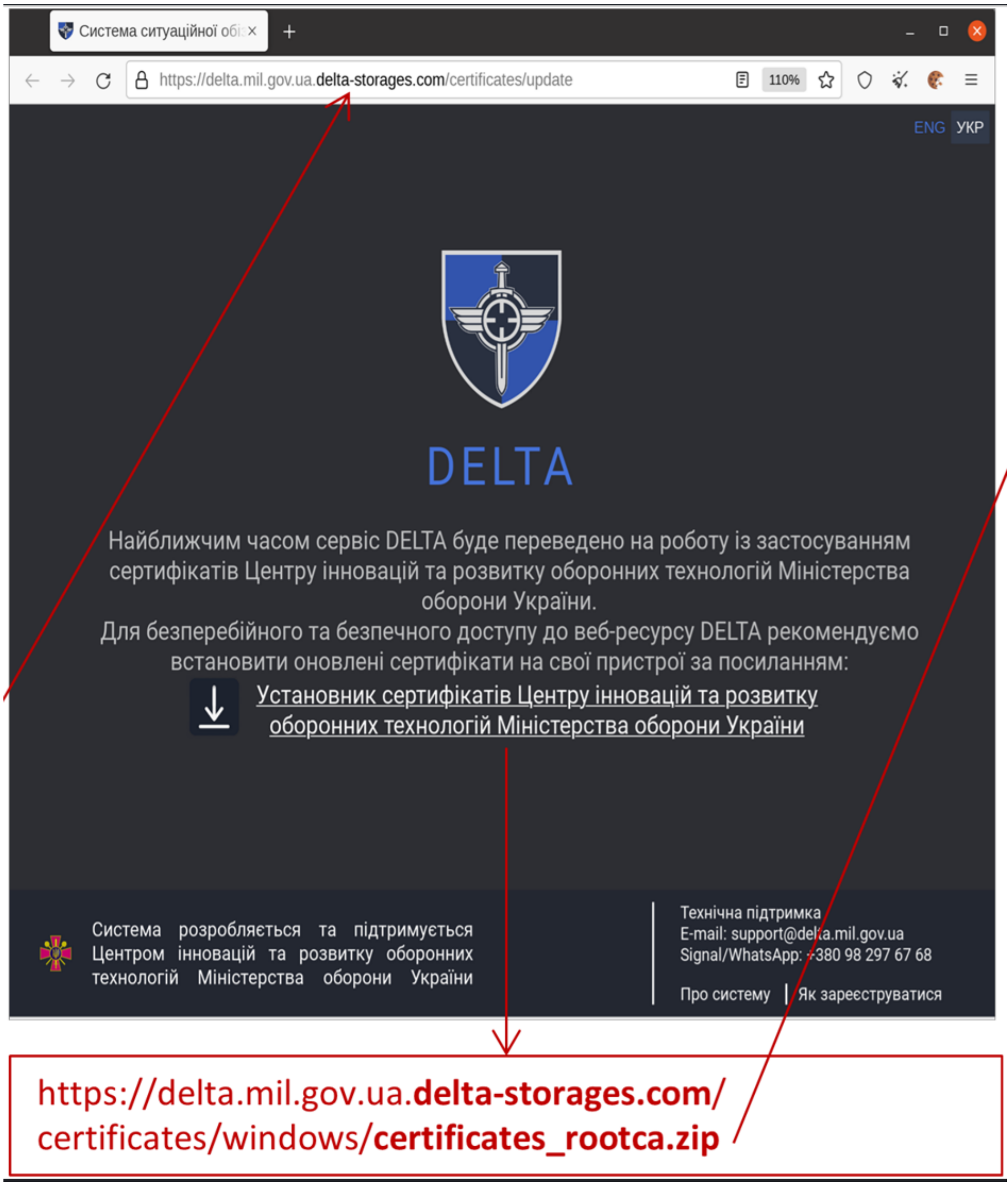
https://delta.mil.gov.ua/

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

Sample of email used in the campaign *(CERT-UA)*


Система ситуаційної обі
https://delta.mil.gov.ua.delta-storages.com/certificates/update
110%
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

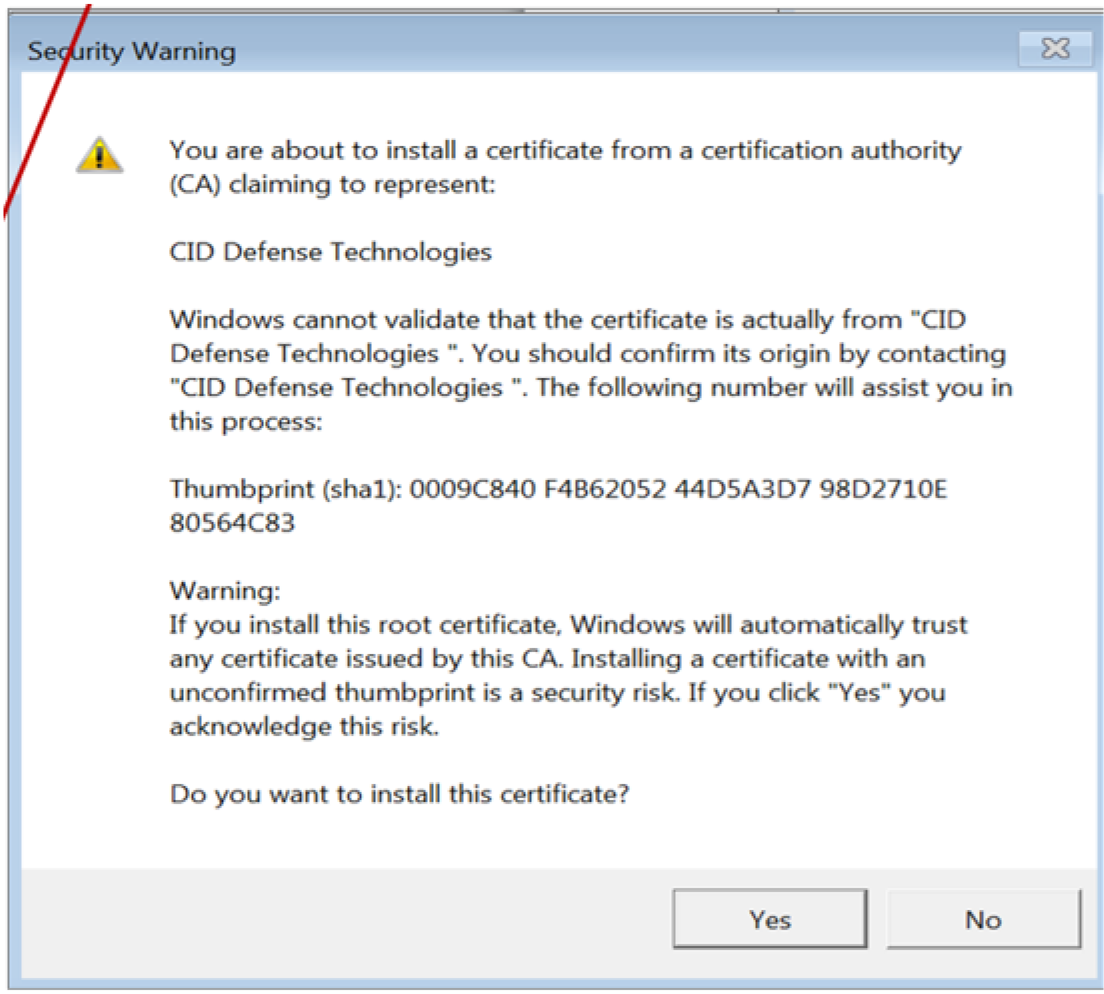
Про систему | Як зареєструватися

https://delta.mil.gov.ua.**delta-storages.com**/
certificates/windows/**certificates_rootca.zip**

Landing page from where victims download the ZIP file *(CERT-UA)*

The archive contains a digitally signed executable named "certificates_rootCA.exe," which, upon launch, creates several DLL files on the victim's system and launches "ais.exe," which simulates the certificate installation process.

This step convinces the victim that the process was legitimate and reduces the chances of them realizing they have been breached.



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?

Certificate installation dialog *(CERT-UA)*

Both the EXE files and the DLLs are protected by VMProtect, a legitimate software that is used for wrapping files in standalone virtualized machines, encrypting their content, and making AV analysis or detection impossible.

The dropped DLLs, "FileInfo.dll" and "procsys.dll," are malware, identified by CERT-UA as 'FateGrab' and 'StealDeal.'

FateGrab is an FTP file stealer targeting documents and emails of the following file formats: '.txt', '.rtf', '.xls', '.xlsx', '.ods', '.cmd', '.pdf', '.vbs', '.ps1', '.one', '.kdb', '.kdbx', '.doc', '.docx', '.odt', '.eml', '.msg', '.email.'

StealDeal is an information stealer malware that can, among other things, steal internet browsing data and passwords stored on the web browser.

CERT-UA was unable to link the above operation to any known threat actors.

Related Articles:

Malicious ‘Lolip0p’ PyPi packages install info-stealing malware

Over 1,300 fake AnyDesk sites push Vidar info-stealing malware

New Dark Pink APT group targets govt and military with custom malware

Malicious PyPi packages create CloudFlare Tunnels to bypass firewalls

New info-stealer malware infects software pirates via fake cracks sites

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.