Microsoft: Hackers turn Exchange servers into malware control centers

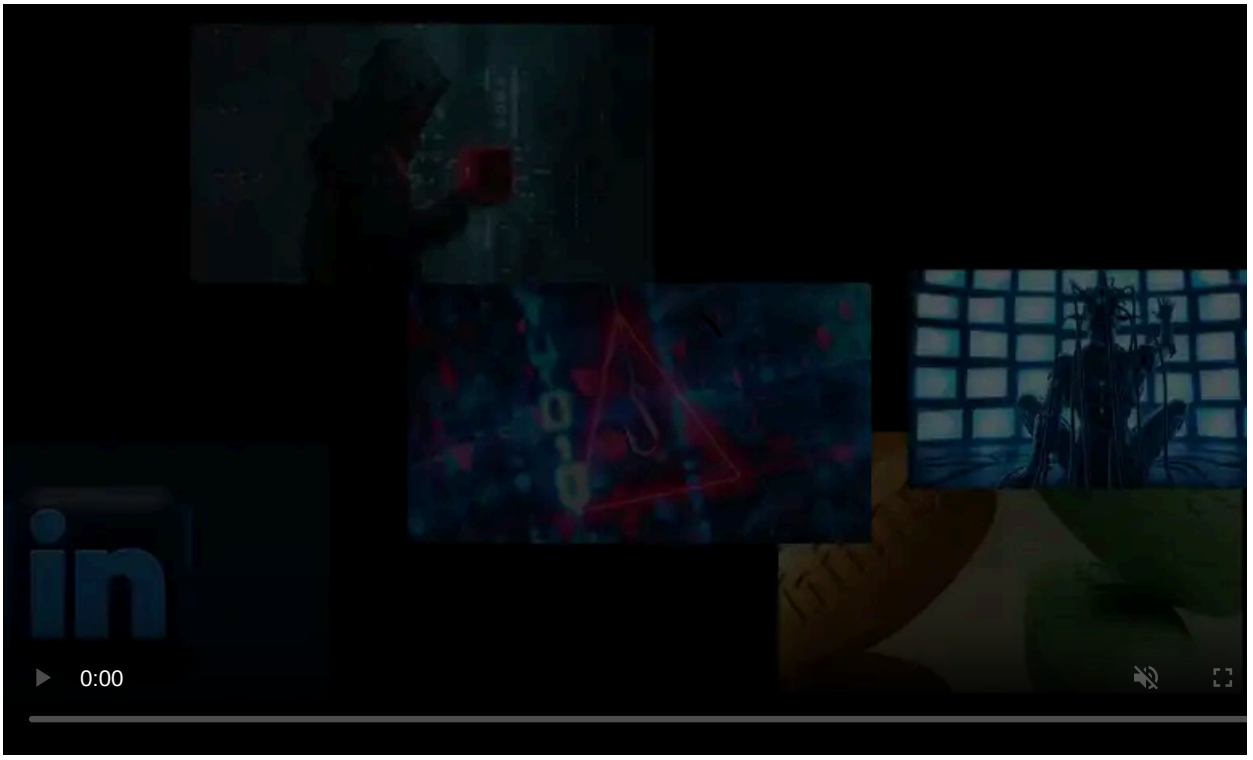
By Lawrence Abrams

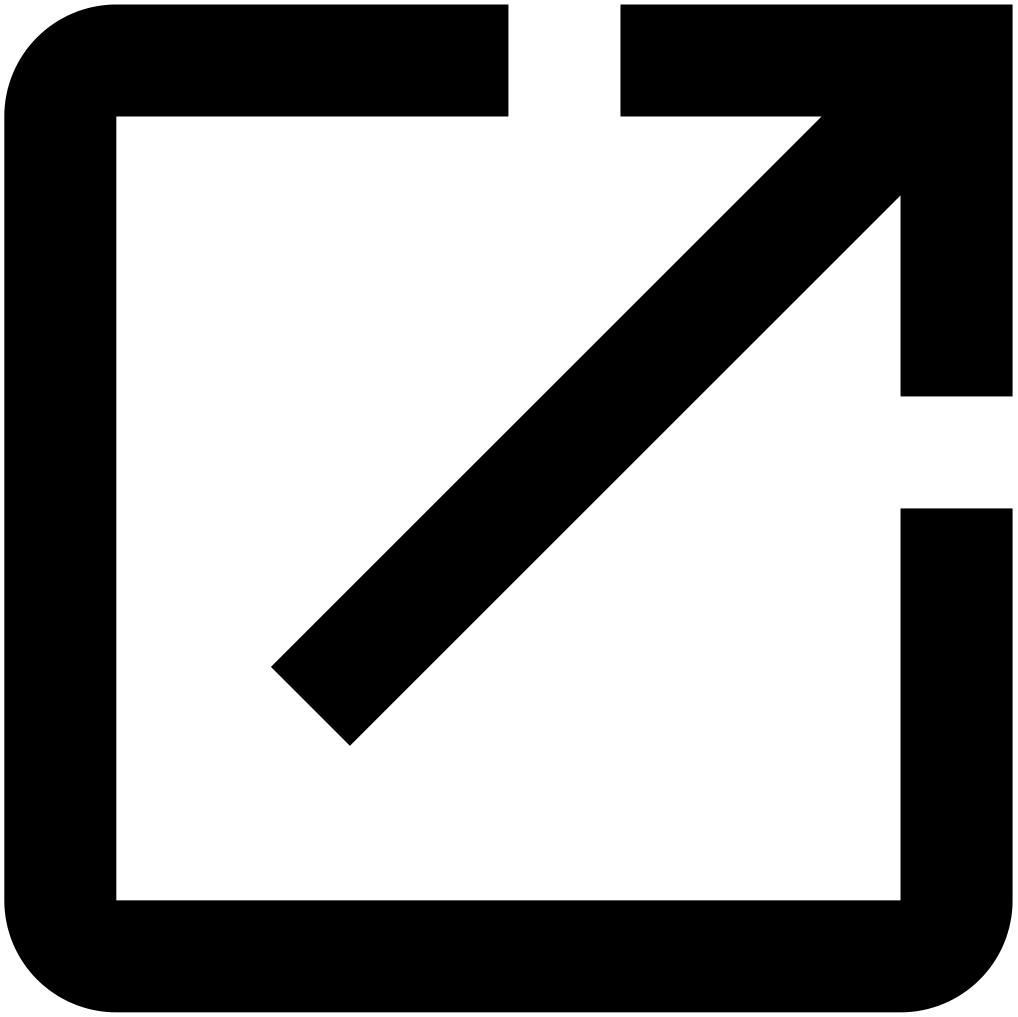
Published: 2023-07-19 · Archived: 2026-04-05 18:53:26 UTC

Microsoft and the Ukraine CERT warn of new attacks by the Russian state-sponsored Turla hacking group, targeting the defense industry and Microsoft Exchange servers with a new 'DeliveryCheck' malware backdoor.

Turla, aka Secret Blizzard, KRYPTON, and UAC-0003, is believed to be an advanced persistent threat actor (APT) linked to Russia's Federal Security Service (FSB).

The cyberspies have been associated with a wide array of attacks against Western interests over the years, including the Snake cyber-espionage malware botnet that was recently disrupted in an international law enforcement operation titled Operation MEDUSA.


0:00



Visit Advertiser websiteGO TO PAGE

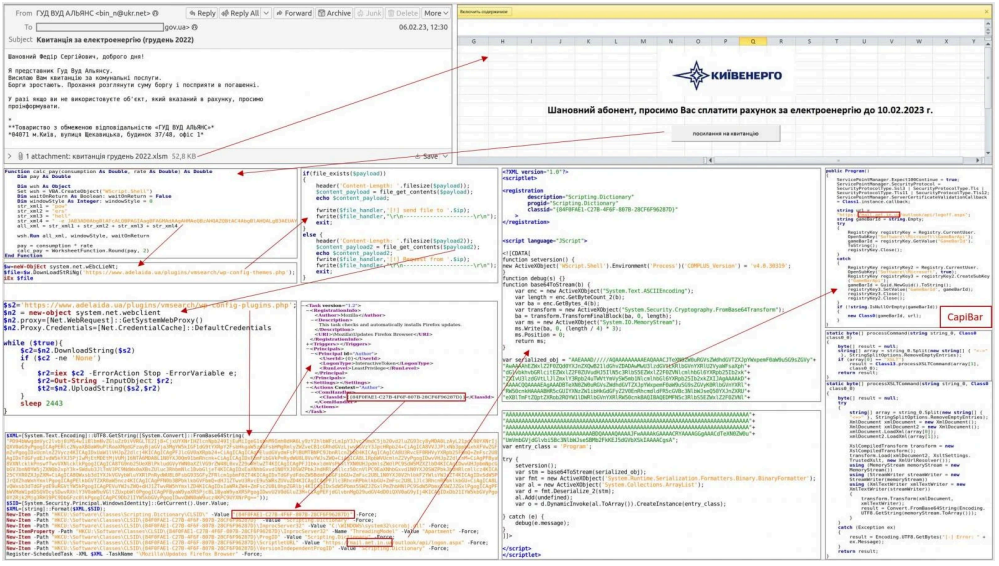
Targeting Microsoft Exchange

In a coordinated report and Twitter thread published today by CERT-UA and Microsoft, researchers outline a new attack where the Turla threat actors target the defense sector in Ukraine and Eastern Europe.

The attacks start with phishing emails containing Excel XLSM attachments that contain malicious macros. When activated, these macros execute a PowerShell command, creating a scheduled task impersonating a Firefox browser updater.

However, this task downloads the DeliveryCheck backdoor (also known as CapiBar and GAMEDAY) and launches it in memory, where it connects to the threat actor's command and control server to receive commands to execute or deploy further malware payloads.

Microsoft says that these malware payloads are embedded and launched from XSLT stylesheets.



Attack flow that delivers the DeliveryCheck malware
Source: CERT-UA

After infecting devices, the threat actors utilize the backdoor to exfiltrate data from the compromised devices using the Rclone tool.

What makes DeliveryCheck stand out is a Microsoft Exchange server-side component that turns the server into a command and control server for the threat actors.

Microsoft says this component is installed using Desired State Configuration, a PowerShell module that allows admins to create a standardized server configuration and apply it to devices.

This feature is usually used to create a default configuration template that can then be used to configure multiple devices with the same settings automatically.

The threat actors use DSC to automatically load a base64-encoded Windows executable which converts the legitimate Exchange server into a malware-distribution server.

Microsoft Exchange server-side componet of DeliveryCheck

Source: UA-CERT

During the attack, Microsoft and CERT-UA also saw Turla drop the KAZUAR information-stealing backdoor, a "fully-featured Secret Blizzard implant".

This malware is a cyberespionage tool that allows the threat actors to launch javascript on the device, steal data from event logs, steal information about systems files, and steal authentication tokens, cookies, and credentials from a wide variety of programs, including browsers, FTP clients, VPN software, KeePass, Azure, AWS, and Outlook.

"The threat actor specifically aims to exfiltrate files containing messages from the popular Signal Desktop messaging application, which would allow the actor to read private Signal conversations, as well as documents, images, and archive files on targeted systems," the Microsoft Threat Intelligence team tweeted.

CERT-UA says they have shared samples of the new malware with cybersecurity companies to aid detection.

However, at this time, only 14/70 vendors on VirusTotal detected a submitted DeliveryCheck sample as malware, which will likely increase as the day progresses.

Source: https://www.bleepingcomputer.com/news/security/microsoft-hackers-turn-exchange-servers-into-malware-control-centers/