APT28 hackers use Signal chats to launch new malware attacks on Ukraine

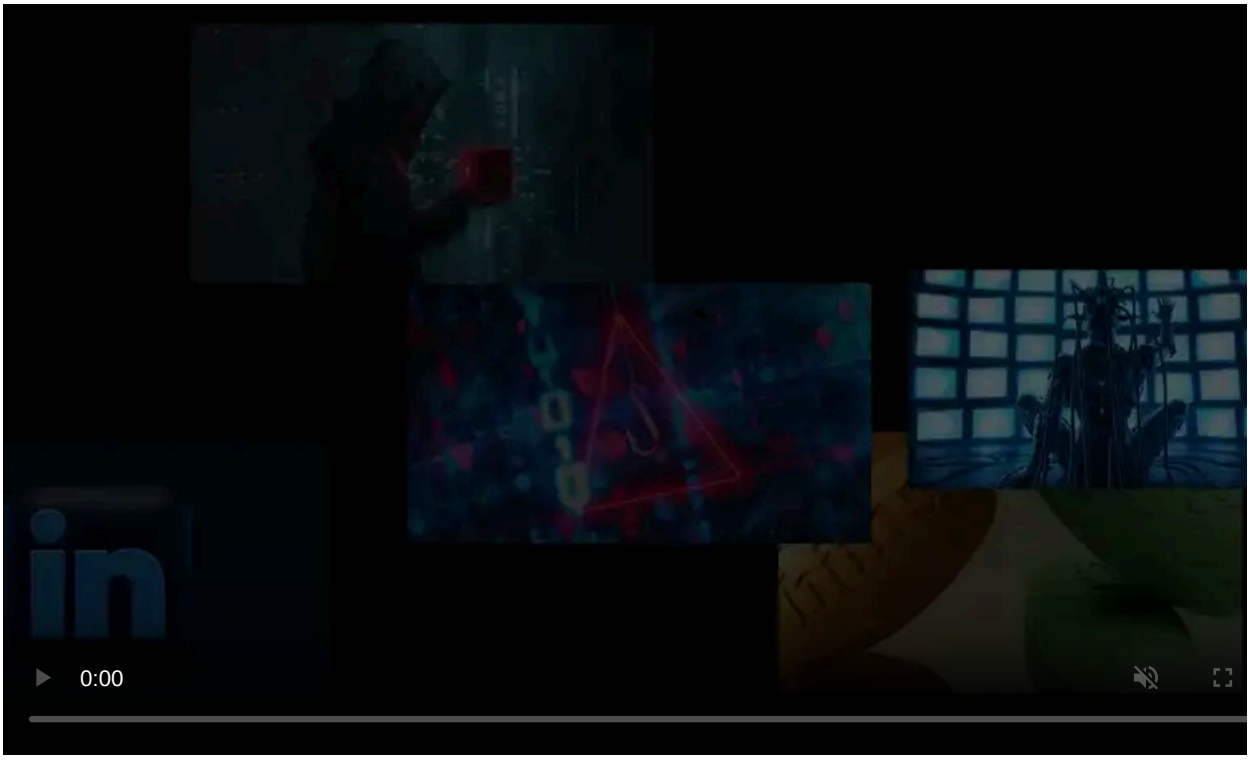
By Bill Toulas

Published: 2025-06-23 · Archived: 2026-04-05 18:09:20 UTC

The Russian state-sponsored threat group APT28 is using Signal chats to target government targets in Ukraine with two previously undocumented malware families named BeardShell and SlimAgent.

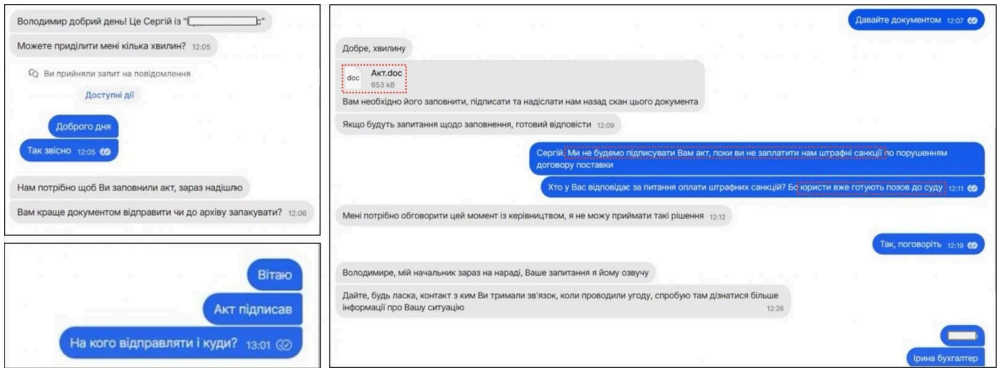
To be clear, this is not a security issue in Signal. Instead, threat actors are more commonly utilizing the messaging platform as part of their phishing attacks due to its increased usage by governments worldwide.

The attacks were first discovered by Ukraine's Computer and Emergency Response (CERT-UA) in March 2024, though limited details about the infection vector were uncovered at the time.


0:00

Over a year later, in May 2025, ESET notified CERT-UA of unauthorized access to a gov.ua email account, prompting a new incident response.

During this new investigation, CERT-UA discovered that messages sent via the encrypted messenger app Signal were used to deliver a malicious document to targets (Акт.doc), which uses macros to load a memory-resident backdoor called Covenant.

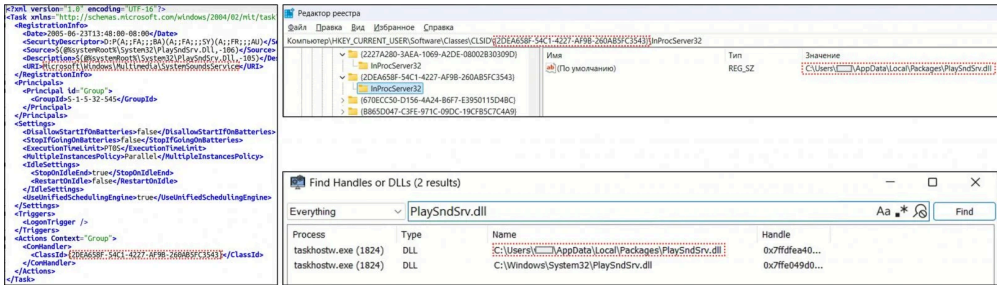


APT28 attack via Signal

Source: CERT-UA

Covenant acts as a malware loader, downloading a DLL (PlaySndSrv.dll) and a shellcode-ridden WAV file (sample-03.wav) that loads BeardShell, a previously undocumented C++ malware.

For both the loader and the primary malware payload, persistence is secured via COM-hijacking in the Windows registry.



Establishing persistence for BeardShell

Source: CERT-UA

BeardShell's main functionality is to download PowerShell scripts, decrypt them using 'chacha20-poly1305', and execute them. The execution results are exfiltrated to the command-and-control (C2) server, the communication with which is facilitated by Icedrive API.

In the 2024 attacks, CERT-UA also spotted a screenshot grabber named SlimAgent, which captures screenshots using an array of Windows API functions (EnumDisplayMonitors, CreateCompatibleDC, CreateCompatibleBitmap, BitBlt, GdipSaveImageToStream).

Those images are encrypted using AES and RSA, and stored locally, presumably to be exfiltrated by a separate payload/tool to APT28's C2 server.

CERT-UA attributes this activity to APT28, which they track as UAC-0001, and recommends that potential targets monitor network interactions with app.koofr.net and api.icedrive.net.

APT28 has a long history of targeting Ukraine as well as other key organizations in the U.S. and Europe, primarily for cyberespionage.

They are one of Russia's most advanced threat groups, exposed by Volexity in November 2024 for using a novel "nearest neighbor" technique, which remotely breached targets by exploiting nearby Wi-Fi networks.

In 2025, Signal unexpectedly became central to cyberattacks linked to Russia and Ukraine.

The popular communications platform has been abused in spear-phishing attacks that abused the platform's device-linking feature to hijack accounts and in Dark Crystal RAT distribution against key targets in Ukraine.

At some point, representatives of Ukraine's government expressed disappointment that Signal allegedly stopped collaborating with them in their effort to block Russian attacks. Ukrainian officials later voiced frustration over Signal's lack of cooperation in blocking Russian operations.

However, Signal president Meredith Whittaker met that claim with surprise, saying the platform has never shared communication data with Ukraine or any other government.

Source: https://www.bleepingcomputer.com/news/security/apt28-hackers-use-signal-chats-to-launch-new-malware-attacks-on-ukraine/