Ukraine warns of InvisiMole attacks tied to state-sponsored Russian hackers

By Written by

Archived: 2026-04-05 17:58:31 UTC

Ukrainian security officials have warned of ongoing attacks by InvisiMole, a hacking group with ties to the Russian advanced persistent threat (APT) group Gamaredon.

Ukraine Crisis

-
-
-
-

Last week, the Computer Emergency Response Team for Ukraine (CERT-UA) said that the department has been advised of new phishing campaigns taking place against Ukrainian organizations that spread the LoadEdge backdoor.

According to CERT-UA, phishing emails are being sent that have an attached archive, 501_25_103.zip, together with a shortcut (LNK) file. If opened, an HTML Application file (HTA) downloads and executes VBScript designed to deploy LoadEdge.

Once the backdoor has formed a link to an InvisiMole command-and-control (C2) server, other malware payloads are deployed and executed including TunnelMole, malware that abuses the DNS protocol to form a tunnel for malicious software distribution, and both RC2FM and RC2CL, which are data collection and surveillance backdoor modules. Persistence is maintained through the Windows registry.

InvisiMole was first discovered by ESET researchers in 2018. The threat actors have been active since at least 2013 and have been connected to attacks against "high-profile" organizations in Eastern Europe that are involved in military activities and diplomatic missions.

In 2020, the cybersecurity researchers forged a collaborative link between InvisiMole and Gamaredon/Primitive Bear, the latter of which appears to be involved in initially infiltrating networks before InvisiMole begins its own operation.

"We discovered InvisiMole's arsenal is only unleashed after another threat group, Gamaredon, has already infiltrated the network of interest, and possibly gained administrative privileges," ESET said at the time. "This allows the InvisiMole group to devise creative ways to operate under the radar."

Palo Alto Networks has also been tracking Gamaredon, and in February, said the APT had attempted to compromise an unnamed "Western government entity" in Ukraine through fake job listings.

CERT-UA has also begun tracking the activities of Vermin/UAC-0020, a group that has been attempting to break into the systems of Ukrainian state authorities. Vermin has been using the topic of supplies in spear phishing emails as a lure, and if opened by a victim, these emails contain a letter and password-protected archive containing the Spectr malware.

In 2018, ESET and Palo Alto Networks published research on Vermin, a group that has been active for at least the past four years, although may date back as far as 2015.

Vermin was targeting Ukrainian government institutions from the outset, with remote access Trojans (RATs) Quasar, Sobaken, and Vermin being the malicious tools of choice.

While the variants of Quasar and Sobaken were compiled using freely-available open source code, Vermin is called a "custom-made" RAT able to perform activities including data exfiltration, keylogging, audio recording, and credential theft.

In related news this month, Aqua Security's Team Nautilus said that public cloud repositories are being used to host resources on both sides of the war, with Ukraine's call for an "IT Army" of volunteers becoming a catalyst for public tools to launch denial-of-service (DoS) attacks against online Russian services.

It is not just RATs and surveillance-based malware that Ukrainian organizations are having to contend with. ESET has detected three forms of wiper malware – designed to destroy computer files and resources, rather than to steal information or spy on victims – in as many weeks.

The latest wiper, dubbed CaddyWiper, has been found "on a few dozen systems in a limited number of organizations," according to ESET.

Previous and related coverage

- Security researchers warn of phishing attempts against officials helping refugees
- Ukraine security agencies warn of Ghostwriter threat activity, phishing campaigns
- CaddyWiper: More destructive wiper malware strikes Ukraine

Have a tip? Get in touch securely via WhatsApp | Signal at +447713 025 499, or over at Keybase: charlie0
