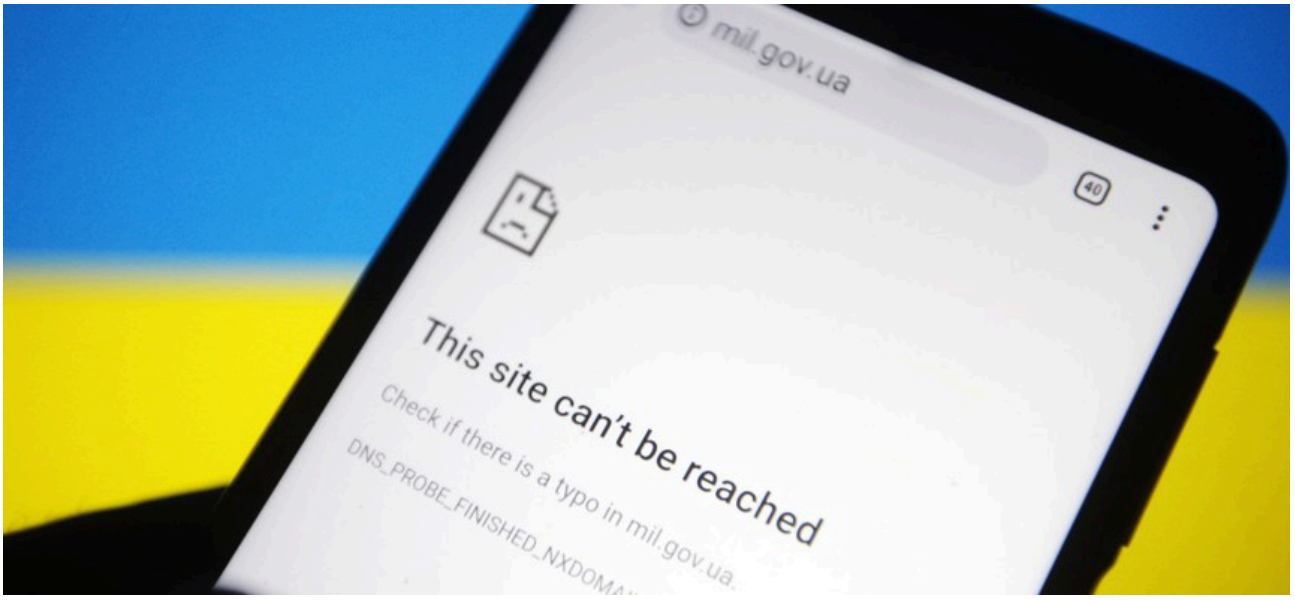
Ukrainian Cyber Lead Says ‘At Least 4 Types of Malware’ in Use to Target Critical Infrastructure and Humanitarian Aid

By Brandi Vincent

Published: 2022-03-24 · Archived: 2026-04-06 00:55:28 UTC



Pavlo Gonchar/SOPA Images/LightRocket via Getty Images

By Brandi Vincent,
Defense Technology Correspondent

By Brandi Vincent

| March 24, 2022

An hour-long press briefing shed new light on the cybersecurity implications of this evolving conflict.

- International
- Cyber Threats
- Defense

Hackers allegedly affiliated with Russia are persistently targeting Ukraine's government, energy and communications systems, and humanitarian efforts amid the ongoing invasion, a senior Ukrainian cybersecurity official told reporters on Wednesday.

"The attackers focus on critical infrastructure, both state-owned and private, and mainly with a connection to land-to-air invasion. Especially weighing are attacks on the logistic circuits and supply of the food and humanitarian support for the cities, where civilians are shelled and bombed," Victor Zhora, deputy chief of Ukraine's information protection service, explained. "So, this all is crucial for the prevention of humanitarian catastrophes and we see these logistic circuits are being attacked with the cyberattackers—hackers—financed and basically owned by the government of the Russian Federation."

Zhora provided this information during an hour-long press briefing hosted by the State Service of Special Communication and Information Protection of Ukraine, regarding cyberattacks the country faced between March 15 and March 22.

Observed attackers are also targeting organizations that publish information about war crimes online and at least four types of malware have been deployed. According to the official, they're called HermeticWiper, IsaacWiper, CaddyWiper and Double Zero.

"The attackers used phishing campaigns to deliver [certain wiper] malware and tried to bring some disruption to Ukrainian IT systems," Zhora said.

His statements come one day after President Joe Biden's administration reiterated warnings that the Russian government "is exploring options for potential cyberattacks" against America based on evolving intelligence.

Moscow has largely rejected allegations that it is conducting malicious cyber pursuits amid this conflict, and the Kremlin dismissed those White House claims.

Still, Zhora noted that the Ukrainian government is supporting companies that might be affected, in response to what the country views as Russia-affiliated cyber incidents.

"As far as we understand, the same approach—warning of businesses of this threat to come—is being taken by the United States, and to be prepared for the upcoming attacks from Russia is our recommendation as well—especially given the fact that some of the attacking groups that we identified are behind the attacks on the European charity organizations working with Ukrainian refugees," he said. "Basically, we suppose that this is another proof of the spread of cyberwar to NATO countries, since these charity organizations are European organizations which aim to help Ukrainian civilians to overcome this terrible situation."

Much of Ukraine's telecommunications infrastructure is privately owned, according to Zhora. In his view, telecom professionals who continue operating "under these highly risky conditions" and restoring connections when they are broken mark "one of factors that probably can explain the success of Ukrainian resistance."

But the Ukrainian government is not organizing offensive cyber operations with others against Russia, he said.

“So I cannot say that we are hacking back,” Zhora noted. “But, obviously, this is done by volunteers and by citizens who have appropriate skills to do this.”

Source: https://www.nextgov.com/cybersecurity/2022/03/ukrainian-cyber-lead-least-4-types-malware-are-targeting-ukrainian-institutions/363558/