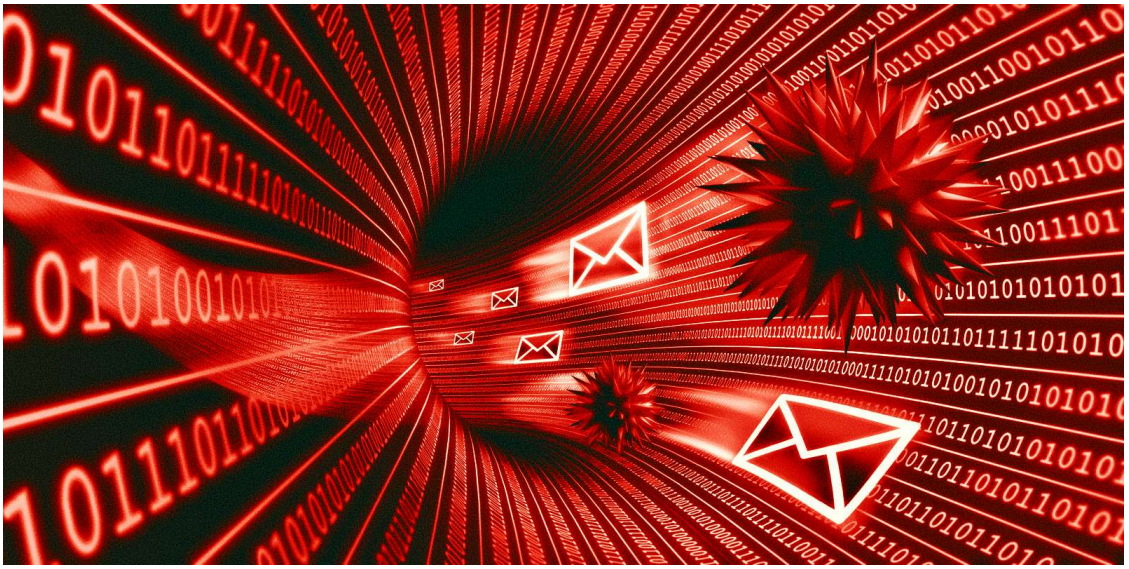
Ukraine links Belarusian hackers to phishing targeting its military

By Sergiu Gatlan

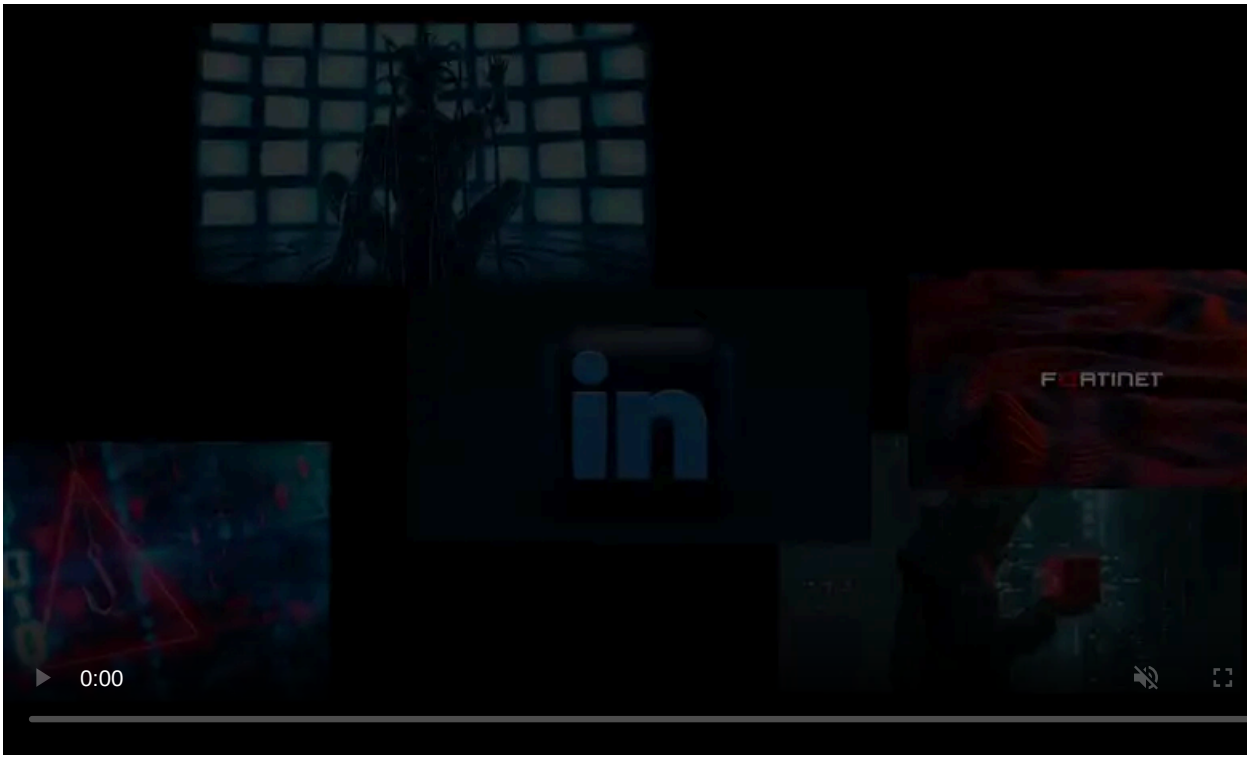
Published: 2022-02-25 · Archived: 2026-04-05 19:52:26 UTC

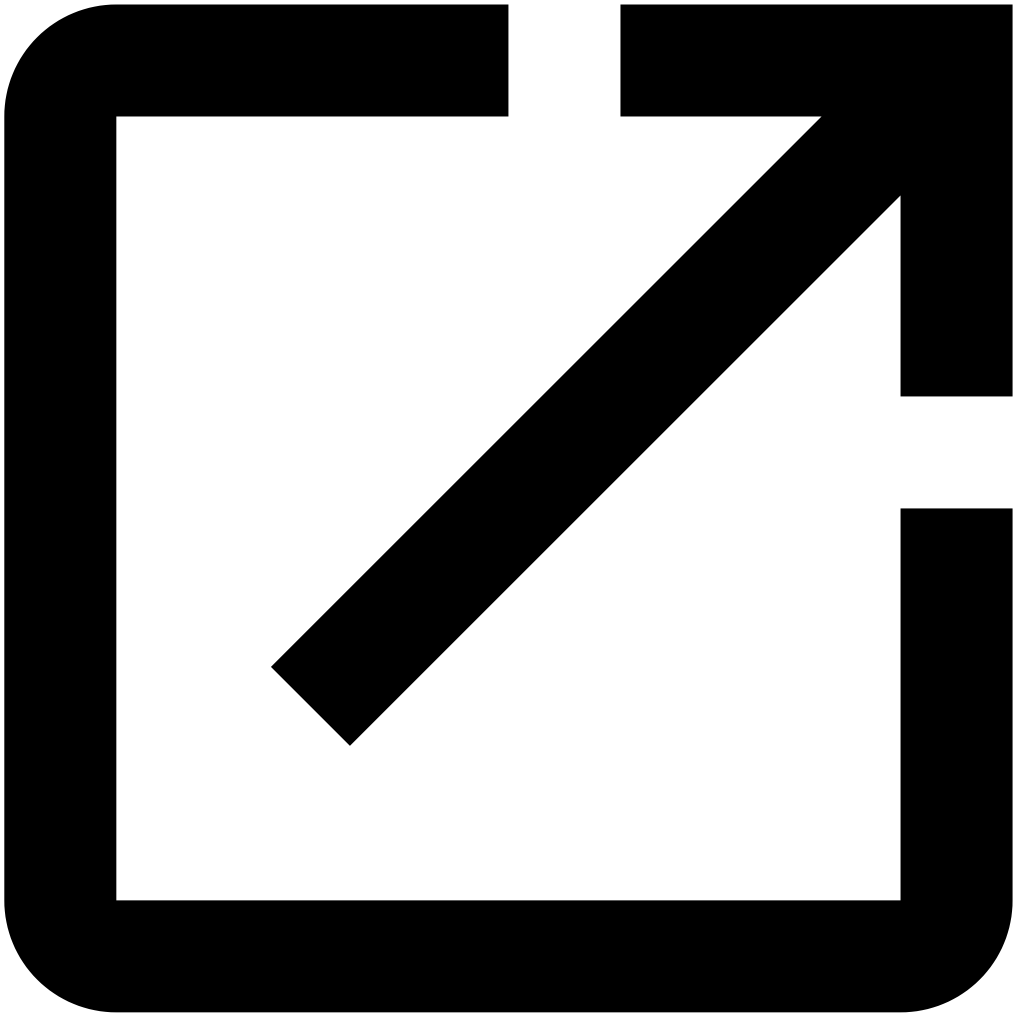


The Computer Emergency Response Team of Ukraine (CERT-UA) warned today of a spearphishing campaign targeting private email accounts belonging to Ukrainian armed forces personnel.

Accounts compromised in these attacks are then used to send additional phishing messages to contacts in the victims' address books.

The phishing emails are being sent from two domains (i[.]ua-passport[.]space and id[.]bigmir[.]space), the former trying to impersonate the i.ua free Internet portal providing email services to Ukrainians since 2008.


0:00



"Mass phishing emails have recently been observed targeting private 'i.ua' and 'meta.ua' accounts of Ukrainian military personnel and related individuals," CERT-UA said earlier today.

"After the account is compromised, the attackers, by the IMAP protocol, get access to all the messages. Later, the attackers use contact details from the victim's address book to send the phishing emails."

The emails ask the targets to click an embedded link to verify their contact information and avoid having their email accounts permanently suspended.

Attacks linked to Belarusian hacking group

CERT-UA's report attributes this ongoing phishing campaign to the UNC1151 threat group, linked by Mandiant researchers with high confidence in November 2021 to the Belarusian government and a hacking operation the company tracked as Ghostwriter.

Mandiant also found evidence supporting a link between the UNC1151 operators and the Belarusian military, confirming CERT-UA's assessment that the attackers are actually military cyberspies and officers of the Belarus Ministry of Defense.

"The Minsk-based group ‘UNC1151’ is behind these activities. Its members are officers of the Ministry of Defence of the Republic of Belarus," CERT-UA added.

Today, the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) also warned Ukrainian citizens of another active phishing campaign targeting them with malicious documents.

"The enemy forces aim to gain access to the electronic devices of Ukrainians to gather a large amount of information," SSSCIP said.

A separate alert issued by Slovak internet security firm ESET says cybercriminals are also impersonating humanitarian organizations in attempts to scam those who would want to donate to organizations focused on helping Ukraine during the ongoing war started by Russia's invasion on Thursday morning.

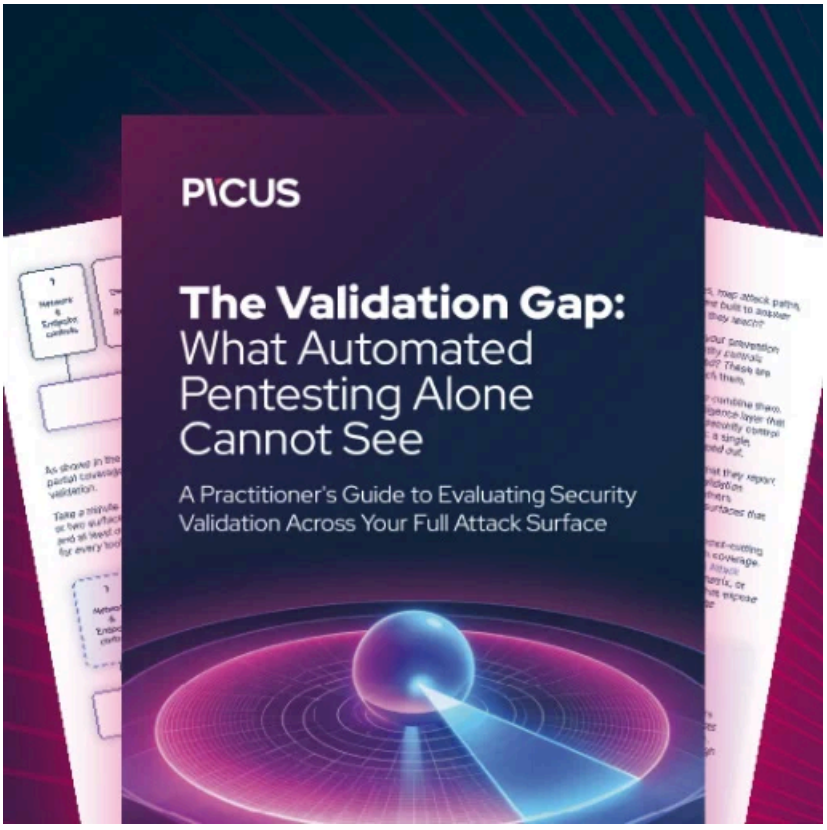
Cyberattacks part of a hybrid warfare campaign

These developments come on the heels of data-wiping attacks against Ukrainian networks, using the HermeticWiper malware and ransomware decoys to destroy data on targets' devices and render them unbootable.

As Vikram Thakur, Technical Director at Symantec Threat Intelligence, told BleepingComputer, targets that were hit in this week's wiper attacks also included finance and government contractors from Latvia and Lithuania.

This was the second time since the start of the year that Ukrainian organizations have been hit by data wipers after the destructive WhisperGate malware was deployed in attacks targeting Ukraine disguised as ransomware in January.

The February DDoS and malware attacks that hit Ukrainian networks align with the Security Service (SSU) Ukraine saying just over a week ago that the country is being targeted by a "massive wave of hybrid warfare."



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/ukraine-links-belarusian-hackers-to-phishing-targeting-its-military/