Meta: Ukrainian officials, military targeted by Ghostwriter hackers

bleepingcomputer.com/news/security/meta-ukrainian-officials-military-targeted-by-ghostwriter-hackers

Sergiu Gatlan

By
Sergiu Gatlan

- February 28, 2022
- 08:34 AM
- 0

Facebook (now known as Meta) says it took down accounts used by a Belarusian-linked hacking group (UNC1151 or Ghostwriter) to target Ukrainian officials and military personnel on its platform.

In November 2021, Mandiant security researchers linked the UNC1151 threat group with high confidence to the Belarusian government, as well as a hacking operation the company tracks as Ghostwriter.

Facebook also blocked multiple phishing domains used by the threat actors to try and compromise the accounts of Ukrainian users.

"We detected attempts to target people on Facebook to post YouTube videos portraying Ukrainian troops as weak and surrendering to Russia, including one video claiming to show Ukrainian soldiers coming out of a forest while flying a white flag of surrender," Meta's Head of Security Policy Nathaniel Gleicher and Threat Disruption Director David Agranovich said.

"We also blocked phishing domains these hackers used to try to trick people in Ukraine into compromising their online accounts."

Accounts believed to be targeted in this campaign have been secured by Facebook's security team, and the users have been alerted of the hacking attempts.

Facebook also took down a small network of a few dozen Facebook and Instagram Pages and Groups operating from Russia and Ukraine and targeting Ukrainians via fake accounts across multiple social media platforms, including Facebook, Instagram, Twitter, YouTube, Telegram, Odnoklassniki, and VK.

This operation was also behind a small number of sites that were masquerading as independent news portals and publishing claims about Ukraine being betrayed by the West and "being a failed state."

Hybrid warfare

Meta's report confirms a warning issued by the Computer Emergency Response Team of Ukraine (CERT-UA) on Friday regarding spear-phishing attacks targeting the private email accounts of the Ukrainian military.

Email accounts compromised in these attacks were then used to target the victims' contacts with similar phishing messages threatening to permanently disable their accounts unless they verified their contact information.

The Ukrainian State Service of Special Communications and Information Protection (SSSCIP) also warned of a separate and ongoing series of phishing attacks targeting Ukrainians with malicious documents.

Slovak internet security firm ESET issued its own alert the same day regarding cybercriminals impersonating humanitarian organizations to scam donors of organizations focused on helping Ukraine during the war started Thursday by Russia's invasion.

These attacks follow data-wiping attacks against Ukrainian networks with HermeticWiper malware and ransomware decoys aiming to destroy data and render devices unbootable. In January, Ukraine was also hit by data wipers when the WhisperGate wiper was deployed in attacks disguised as ransomware.

Before Russia's invasion, the Ukrainian Security Service (SSU) said the country is being targeted by a "massive wave of hybrid warfare."

Over the weekend, Ukraine's Vice Prime Minister Mykhailo Fedorov announced the creation of an "IT army" to help Ukraine "fight on the cyber front."

Related Articles:

Meta, US hospitals sued for using healthcare data to target ads

Google: Russia, China, Belarus state hackers target Ukraine, Europe

Google: Russian phishing attacks target NATO, European military

Malicious Messenger chatbots used to steal Facebook accounts

Malicious browser extensions targeted almost 7 million people