Sandworm-linked hackers target users of Ukraine's military app in new spying campaign

By Daryna Antoniuk

Published: 2024-12-19 · Archived: 2026-04-05 17:18:57 UTC

Ukrainian soldiers have become the target of a new espionage campaign linked to the notorious Russian state-sponsored threat actor Sandworm, according to a recent report.

As part of the operation, the hackers create fraudulent websites that mimic the official page of a Ukrainian military app, Army+, tricking users into downloading an executable file disguised as an app installation package.

Army+ has received significant attention from Ukraine's government recently. The app, introduced earlier this year, aims to digitize bureaucratic tasks for soldiers, such as submitting reports to commanders.

According to a report from Ukraine's military computer emergency response team (MIL.CERT-UA), the fake Army+ websites are hosted on a "serverless" platform, Cloudflare Workers, that deploys applications. Hackers often exploit legitimate services to obscure their operations and make fraudulent websites appear more convincing to potential victims.

The executable file delivered through the malicious Army+ app is an installer crafted with NSIS (Nullsoft Scriptable Install System), a tool frequently used by developers to create software installation packages.

When executed, the file activates a malicious program that grants hackers hidden access to the computer, sends confidential data through the anonymized Tor network, and allows the hackers to further compromise the targeted systems.

The hacker group behind this recent campaign is tracked by CERT-UA as UAC-0125 and is "highly likely" to be linked to the notorious Russian threat actor APT44, also known as Sandworm, MIL.CERT-UA said.

Sandworm is responsible for major cyberattacks targeting Ukraine, including the 2015 disruption of the country's power grid using BlackEnergy malware, the 2017 destructive attack against Ukrainian government agencies, energy companies, and critical infrastructure with NotPetya malware, and the 2023 hack of Ukraine's largest telecom operator, Kyivstar. Sandworm hackers are believed to be associated with Russia's military intelligence service (GRU).

Ukrainian researchers have not provided many details about the Army+ hack, likely due to the sensitivity of the topic. It remains unclear how the malicious websites were distributed, how successful the attack was, how many users were affected, and what the ultimate goal of the operation is.

Ukrainian soldiers and the services they use have become a popular target for hackers associated with Russia, including Sandworm.

Google-owned Mandiant discovered earlier this year that Sandworm hackers established an infrastructure allowing Russian military forces to exfiltrate encrypted Telegram and Signal communications from mobile devices captured on the battlefield.

In October, Ukrainian researchers described a new Russia-linked cyber campaign targeting Ukrainian draft-age men with information-stealing malware. As part of this campaign, the hackers promoted “free software programs” purportedly designed to help potential Ukrainian conscripts view and share crowdsourced locations of military recruiters. Once installed, these programs delivered malware alongside a decoy app, tracked as Sunspinner.

Earlier in April, CERT-UA reported that hackers had increasingly attempted to plant data-stealing malware on messaging apps used by the Ukrainian armed forces. To trick victims into opening malicious files, hackers disguised them as fake court documents, videos from the frontlines, or archives.

No previous article

No new articles

Daryna Antoniuk

is a reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.
