Ukraine cyber officials warn of a ‘surge’ in Smokeloader attacks on financial, government entities

By Daryna Antoniuk

Published: 2023-10-24 · Archived: 2026-04-05 20:04:38 UTC

Suspected Russian cybercriminals have increased their attacks against Ukrainian financial and government organizations using Smokeloader malware, according to Ukrainian cybersecurity officials.

Since May of this year, the malware operators have targeted Ukrainian organizations with intense phishing attacks, primarily attempting to infiltrate their systems and steal sensitive information, according to research published Tuesday by Ukraine's National Cyber Security Coordination Center (NCSCC).

Smokeloader is a highly complex malware primarily functioning as a loader, which downloads stealthier or more effective malicious software into the system. However, because of its modular design, Smokeloader can perform a wide range of functions, including stealing credentials, executing distributed denial-of-service (DDoS) attacks, and intercepting keystrokes.

The price for this malicious toolkit varies, with options ranging from $400 for the basic bot to $1,650 for the complete package, featuring all available plugins and functions.

The researchers did not attribute this campaign to a specific hacker group, but they noted that the prevalence of Russian domain registrars suggests potential connections to Russian cybercriminal operations.

Back in May, Ukraine's Computer Emergency Response Team (CERT-UA) linked the Smokeloader activity to a threat actor they identified as UAC-0006. CERT-UA described it as a financially motivated operation aiming to steal credentials and execute unauthorized fund transfers.

The researchers from the NCSCC said that the attacks on Ukrainian organizations by both financially motivated cybercriminals and state-sponsored hackers indicate that the threat landscape in Ukraine 'has evolved into a multifaceted arena.”

Smokeloader attacks on Ukraine

In their recent campaign, the hackers used Smokeloader to attack state, private, and financial institutions, with a particular focus on accounting departments, the NCSCC told Recorded Future News.

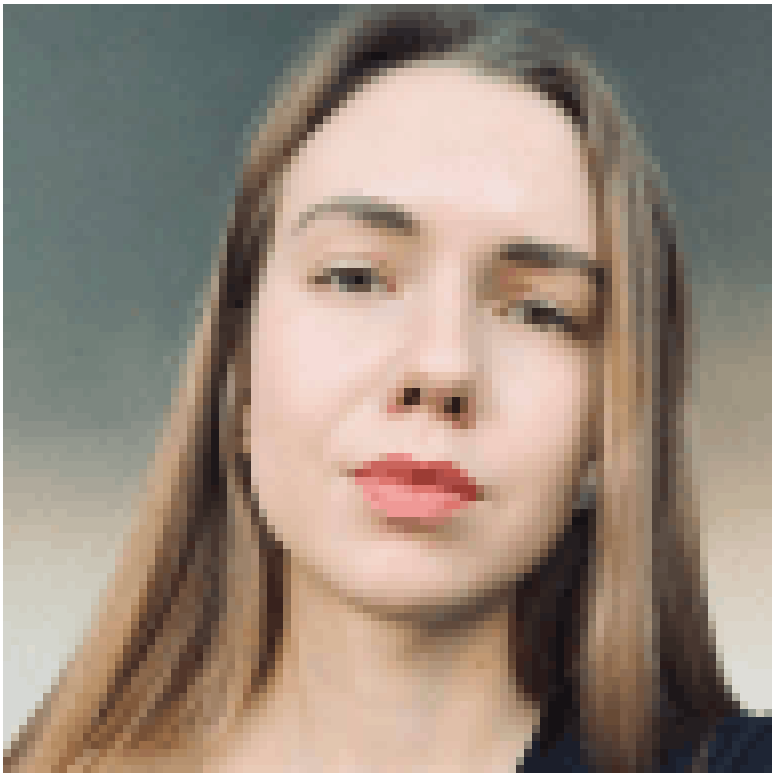
The hackers used “meticulously crafted” financially-themed emails to trick victims into downloading malicious attachments. Financial themes created a sense of urgency and relevance for recipients, researchers said.

The hackers concealed Smokeloader under layers of seemingly harmless financial documents. Most of these files were legitimate and were stolen from organizations that had been previously compromised.

Smokeloader uses various evasion strategies to slip through security measures undetected. After finally gaining access to the system, it can extract crucial device information, including operating system details and location data.

In recent attacks, attackers also compromised money transfer processes, redirecting funds to their own accounts by replacing legitimate account details.

Such cases highlight cybercriminals' evolving tactics, which now include manipulating financial processes to divert and steal resources, the researchers said.



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.