Ukraine sees surge in AI-Powered cyberattacks by Russia-linked Threat Actors

By Pierluigi Paganini

Published: 2025-10-10 · Archived: 2026-04-05 18:43:31 UTC

Russia-linked actors use AI to craft phishing and malware attacks against entities in Ukraine, says SSSCIP.

Russian hackers increasingly use AI in cyberattacks against Ukraine, the country's State Service for Special Communications and Information Protection (SSSCIP) reported. Beyond AI-generated phishing, some malware samples now show AI-generated code. In H1 2025, Ukraine recorded 3,018 cyber incidents, up from 2,575 in late 2024. Attacks on local authorities and military entities rose, while those on government and energy sectors declined.

“In the first half of 2025, specialists from the National Cyber Incident Response Team, Cyber Attacks, and Cyber Threats CERT-UA recorded a number of new activities in attacks against Ukraine.” states the report.

“As noted in the analytical report “Russian Cyber Operations” for the first half of 2025, a radical change in tactics, techniques, and procedures, the involvement of “fresh blood” in attacks, indicate a decrease in the effectiveness of already known methods due to our effective countermeasures. We will talk about several groups.”

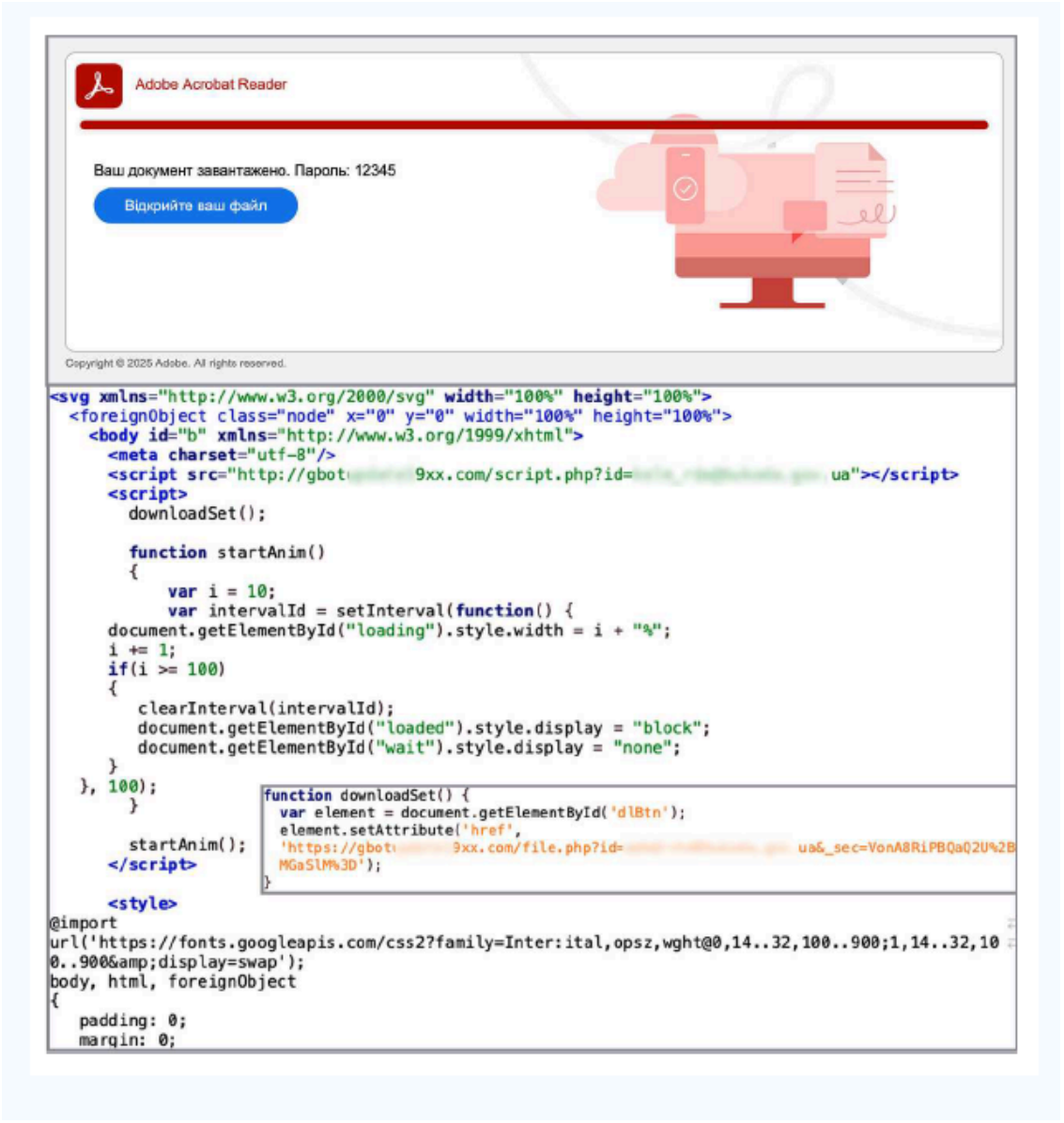
The report details several threat actors that targeted Ukraine, including UAC-0219, UAC-0218, and UAC-0226. UAC-0219 uses WRECKSTEEL to steal data and take screenshots, likely leveraging AI to generate PowerShell scripts. Active since late 2024, CERT-UA detected the APT activity in 2025.

According to the SSSCIP’s report, UAC-0218 has been active since 2024 but intensified in early 2025. Its phishing emails contain links to E-Disk archives hosted on UKR.NET, usually holding password-protected Office files and an encrypted VBE script delivering HOMESTEEL, a file-stealing malware.

UAC-0226 targets defense, government, and law enforcement sectors via malicious email attachments. It deploys Reverse-shell and GIFTEDCROOK, a stealer that extracts browser data and sends it to a hacker-controlled Telegram chat.

The government experts also warn of APT group UAC-0227, which has been active aince at least March 2025. CERT-UA has been tracking the group’s activity that is aimed at spying on local governments, critical infrastructure facilities, the Central Communications Commission and Joint Ventures, etc.

“To implement the threat, attackers send emails with various content. After trying different approaches to delivering the ransomware, the hackers settled on distributing an SVG file, which is a vector image that opens in a web browser by default.” continues the report. “Analysis of early UAC-0227 campaigns revealed files dated to late 2023 that indicate the same activity targeting European Union countries.”



SSSCIP reported that Russia-linked cyberespionage group APT28 exploited XSS flaws in Roundcube and Zimbra webmail (CVE-2023-43770, CVE-2024-37383, CVE-2025-49113, CVE-2024-27443, CVE-2025-27915) for zero-click attacks.

“The use of legitimate online resources for malicious purposes is not a new tactic,” SSSCIP concludes. “However, the number of such platforms exploited by Russian hackers has been steadily increasing in recent times.”

Follow me on Twitter: @securityaffairs and Facebook and Mastodon

Pierluigi Paganini

(SecurityAffairs – hacking, Russia)

Source: https://securityaffairs.com/183222/apt/ukraine-sees-surge-in-ai-powered-cyberattacks-by-russia-linked-threat-actors.html