

# UAC-0226 Attack Detection: New Cyber-Espionage Campaign Targeting Ukrainian Innovation Hubs and Government Entities with GIFTEDCROOK Stealer

By Veronika Zahorulko

Published: 2025-04-07 · Archived: 2026-04-05 14:24:36 UTC

Throughout March 2025, defenders observed increasing cyber-espionage activity by the [UAC-0219](#) hacking group targeting Ukrainian critical sectors WRECKSTEEL malware. In April, CERT-UA issued a novel alert notifying the global cyber defender community of a new surge of espionage operations orchestrated by another hacking collective tracked as UAC-0226. Since February 2025, researchers have been closely monitoring the group's targeted intelligence-gathering activities against Ukraine using another stealer known as GIFTEDCROOK, with a primary focus on military innovation hubs, the armed forces, law enforcement entities, and regional government institutions.

## Detect UAC-0226 Attacks Covered in the CERT-UA#14303 Alert


According to CERT-EU's annual Threat Landscape Report, in 2024, a significant 44% of reported incidents were linked to cyber espionage or prepositioning tactics usually attributed to state-sponsored actors with a primary focus on data exfiltration and establishing persistent, stealthy access. In the spring of 2025, CERT-UA already observed an increase in cyber-espionage activity against Ukraine attributed to [UAC-0200](#), [UAC-0219](#), and UAC-0226. The latest [CERT-UA#14303](#) alert highlights the ongoing cyber-espionage campaign by UAC-0226 leveraging the GIFTEDCROOK stealer.

[SOC Prime Platform](#) for collective cyber defense curates a dedicated collection of detection algorithms to help Ukrainian and allied organizations proactively thwart cyber-espionage attacks by UAC-0226 covered in the corresponding CERT-UA heads-up. Click **Explore Detections** to access relevant Sigma rules enriched with actionable intelligence, aligned with MITRE ATT&CK®, and compatible with multiple SIEM, EDR, and Data Lake solutions.

### [Explore Detections](#)

Security teams can also search SOC Prime's Detection-as-Code library for relevant content by using the corresponding tags "[CERT-UA#14303](#)" and "[UAC-0226](#)" to timely spot adversary activity.

In addition, security engineers can rely on [Uncoder AI](#), a private non-agentic AI for threat-informed detection engineering, to automatically convert IOCs from the CERT-UA research into actionable hunting queries and seamlessly search for UAC-0226 attacks in the SIEM or EDR instance in use.

 Use Uncoder AI to convert IOCs from the CERT-UA#14303 alert into custom queries ready to hunt in your SIEM or EDR.

## UAC-0226 Attack Analysis

On April 6, 2025, CERT-UA released a new security heads-up, [CERT-UA#14303](#), focused on cyber-espionage operations against Ukraine leveraging the C/C++-based stealer GIFTEDCROOK. Researchers have been observing the ongoing cyber-espionage campaign linked to the UAC-0226 group since February 2025, with military innovation hubs, armed forces units, law enforcement agencies, and local state bodies, particularly those located near the country's eastern border, being its primary targets.

The infection flaw starts via the [phishing](#) attack vector containing macro-enabled Excel files (.xlsm), commonly using lure topics like landmine clearance, administrative fines, drone production, or compensation for damaged property. These documents hide base64-encoded payloads within Excel cells. The embedded macros decode the content into executable files, save them without file extensions, and execute them on the victim's machine.

As of April 2025, two malware variants tied to this activity have been identified. The first is a .NET-based tool embedding a PowerShell reverse shell script sourced from the public GitHub repository PSSW100AVB. The second, dubbed GIFTEDCROOK, is a C/C++ stealer designed to extract Chrome, Edge, and Firefox browser data (cookies, history, saved credentials), archive it using PowerShell's Compress-Archive cmdlet, and exfiltrate it via Telegram. Since phishing emails are being sent from compromised accounts, including via webmail, defenders recommend system administrators review the completeness and depth of email and web server logs.

## MITRE ATT&CK Context

Leveraging MITRE ATT&CK provides in-depth visibility into the context of the latest UAC-0226 cyber-espionage operation targeting Ukrainian innovation hubs and government entities with GIFTEDCROOK stealer. Explore the table below to see the full list of dedicated Sigma rules addressing the corresponding ATT&CK tactics, techniques, and sub-techniques.

---

Source: <https://socprime.com/blog/detect-uac-0226-attacks-against-ukraine/>