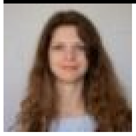
UAC-0226 Attack Detection: New Cyber-Espionage Campaign Targeting Ukrainian Innovation Hubs and Government Entities with GIFTEDCROOK Stealer

socprime.com/blog/detect-uac-0226-attacks-against-ukraine/

SOC PRIME
UAC-0226
CERT-UA Warns of Espionage Attacks Against Ukraine Using the GIFTEDCROOK Stealer



WRITTEN BY

Veronika Telychko

Technical Writer

[post-views]

April 07, 2025 · 3 min read

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.

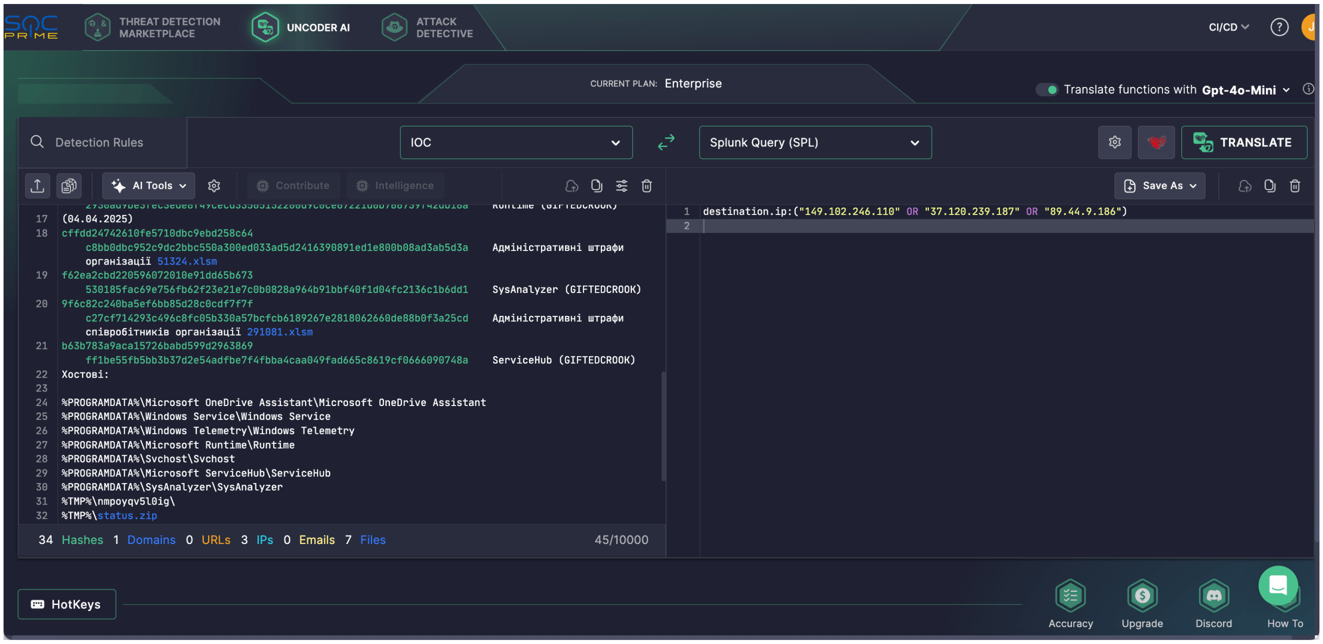
Detect UAC-0226 Attacks Covered in the CERT-UA#14303 Alert

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.



```
(04.04.2025)
cffdd24742610fe5710dbc9ebd258c64
    c8bb0dbc952c9dc2bbc550a300ed033ad5d2416390891ed1e800b08ad3ab5d3a    Адміністративні штрафи
    організації 51324.xlsm
f62ea2cbd220596072010e91dd65b673
    530185fac69e756fb62f23e21e7c0b0828a964b91bbf40f1d04fc2136c1b6dd1    SysAnalyzer (GIFTEDCROOK)
9f6c82c240ba5ef6bb85d28c0cdf7f7f
    c27cf714293c496c8fc05b330a57bcfcb6189267e2818062660de88b0f3a25cd    Адміністративні штрафи
    співробітників організації 291081.xlsm
b63b783a9aca15726babd599d2963869
    ff1be55fb5bb3b37d2e54adfbe7f4fbba4caa049fad665c8619cf0666090748a    ServiceHub (GIFTEDCROOK)
Хостові:

%PROGRAMDATA%\Microsoft OneDrive Assistant\Microsoft OneDrive Assistant
%PROGRAMDATA%\Windows Service\Windows Service
%PROGRAMDATA%\Windows Telemetry\Windows Telemetry
%PROGRAMDATA%\Microsoft Runtime\Runtime
%PROGRAMDATA%\Svchost\Svchost
%PROGRAMDATA%\Microsoft ServiceHub\ServiceHub
%PROGRAMDATA%\SysAnalyzer\SysAnalyzer
%TMP%\nmpoyqv5l0ig\
%TMP%\status.zip
```

34 Hashes 1 Domains 0 URLs 3 IPs 0 Emails 7 Files 45/10000

```
destination.ip:("149.102.246.110" OR "37.120.239.187" OR "89.44.9.186")
```

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.

Tactics	Techniques	Sigma Rule
Initial Access	Spearphishing Attachment (T1566.001)	Windows Mail Client Creating Files With Executable Extension (via file_event)
		Visual Basic Library Loading in Office Process (via image_load)
Execution	Command and Scripting Interpreter: PowerShell (T1059.001)	Call Suspicious .NET Methods from Powershell (via powershell)
	Command and Scripting Interpreter: Visual Basic (T1059.005)	Visual Basic Library Loading in Office Process (via image_load)
Collection	Archive Collected Data (T1560)	Powershell Compressing Files To An Archive In Suspicious Directory (via cmdline)
Exfiltration	Exfiltration Over Web Services (T1567)	Suspicious Process DNS Query Known Abuse Web Services (via network_connection)
		Possible Telegram Abuse As Command And Control Channel (via dns_query)