
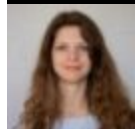


# UAC-0149 Attack Detection: Hackers Launch a Targeted Attack Against the Armed Forces of Ukraine, as CERT-UA Reports

 [socprime.com/blog/uac-0149-attack-detection-hackers-launch-a-targeted-attack-against-the-armed-forces-of-ukraine-as-cert-ua-reports/](https://socprime.com/blog/uac-0149-attack-detection-hackers-launch-a-targeted-attack-against-the-armed-forces-of-ukraine-as-cert-ua-reports/)



WRITTEN BY

Veronika Telychko

Technical Writer

[post-views]

February 26, 2024 · 4 min read

Two days before the 2nd anniversary of [russia's full-scale invasion](#), CERT-UA researchers uncovered an ongoing phishing attack against the Armed Forces of Ukraine. The adversary campaign linked to the UAC-0149 group has leveraged COOKBOX malware to infect targeted systems.

## UAC-0149 Attack Analysis Using COOKBOX Malware

---

CERT-UA in coordination with the Cybersecurity Center of the Information and Telecommunication Systems of the Military Unit A0334 unveiled a targeted attack against the Armed Forces of Ukraine covered in the corresponding [CERT-UA#9204 alert](#). The UAC-0149 group has been performing the malicious operation since at least fall 2023.

On February 22, 2024, several military employees received a lure XLS file titled “1\_ф\_5.39-2024.xlsm” related to the report challenges via the Signal messenger. In addition to a legitimate macro, the file contained VBA code designed to execute a PowerShell command responsible for downloading, decoding, and executing the PowerShell script “mob2002.data.”

The PowerShell script downloaded from GitHub performs registry modification on the operating system (OS), including writing the primary payload in the base64-encoded format, writing the decoder-launcher in the base64-encoded format to the “HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\XboxCache” branch, and creating a registry key “xbox” in the “Run” autostart branch, which is intended to execute the decoder, facilitating the execution of the main payload. The latter upon decoding contains another PowerShell script that performs GZIP decompression and executes the malicious COOKBOX program.

COOKBOX malware is a PowerShell script for loading and running PowerShell commands. For each infected device a unique identifier is computed using cryptographic transformations (SHA256/MD5 hash functions) based on a combination of the computer name and disk serial number. This identifier is transmitted in the “X-Cookie” header of HTTP requests during interactions with the C2 server.

COOKBOX malware persistence is achieved via a corresponding registry key in the “Run” branch of the OS registry. This key is created during the initial infection stage by a third-party PowerShell script, including the COOKBOX deployer. Commonly, the code leverages obfuscation like character encoding, character substitution (replace()), base64 encoding, and GZIP compression. UAC-0149 hackers apply dynamic DNS services and Cloudflare Workers for the C2 infrastructure management.

Defenders observed that adversaries managed to infect the targeted systems using COOKBOX malware in cases when the infrastructure was not properly protected. The devices without blocking the attempts of running cmd.exe, powershell.exe, mshta.exe, w(c)script.exe, hh.exe, and other executive utilities were mostly vulnerable to attacks. If the utilities were launched from within a process parented by one of the Microsoft Office programs (e.g., EXCEL.EXE), the chances of attacks increased. Notably, in one case, adversary attempts failed due to properly set EDR protection, which fuels the need for following best cybersecurity practices and strengthening cyber defense to effectively withstand such attacks.

With the exponential rise in cyber attacks targeting Ukraine and its allies mainly in the public sector, forward-looking organizations are striving to elevate cyber vigilance backed by a proactive cyber defense strategy and innovation capabilities. Leveraging [Attack Detective](#), organizations can seamlessly identify blind spots in detection coverage, gain from automated threat hunting capabilities, and minimize the risks of organization-specific threats to reinforce their cybersecurity posture.

## Detect the UAC-0149 Attack Covered in the CERT-UA#9204 Alert

Security experts estimate that around 40 Russia-backed APT groups attacked Ukraine in H1 2023, with intrusions constantly growing in number and sophistication. This time, the Armed Forces of Ukraine became a target of another malicious campaign by UAC-0149, relying on COOKBOX malware.

To help security professionals spot suspicious activity linked to UAC-0149 and COOKBOX, SOC Prime Platform for collective cyber defense aggregates a set of behavior-based detection algorithms accompanied by detailed metadata. All the rules are mapped to [MITRE ATT&CK®](#) v14.1 and compatible with 28 SIEM, EDR, XDR and Data Lake solutions. Just hit the **Explore Detections** button below and drill down to the curated rule set.

### [Explore Detections](#)

Alternatively, cyber defenders can search for related detections using “UAC-0149” and “CERT-UA#9204” tags based on the group identifier and CERT-UA alert.

Security engineers might also streamline the IOC packaging using the [Uncoder AI](#) tool. Just paste the [IOCs provided by CERT-UA](#) and automatically convert them into performance-optimized queries ready to run in the chosen environment for smooth threat investigation.

The screenshot displays the SOC Prime Platform interface. At the top, it shows 'CURRENT PLAN: Enterprise' and 'REVERSE TRANSLATIONS: 272'. Below this, there's a search bar with 'IOC' selected. The main area is divided into two panels. The left panel, titled 'Detection Rules', lists various rules with their IDs and names, such as 'COOKBOX', 'COOKBOX\_deployer', and 'COOKBOX\_deployer'. The right panel, titled 'Splunk Query (SPL)', shows a complex query for detecting malicious activity, including file paths like 'v8.dec.ps1', 'xps2.ps1', and 'xps3.ps1', and network-related terms like 'https://shorturl.at/avwpy' and 'https://github.com/kekeleashes/testdatasearch/main/mob2002.data'. The bottom of the interface shows a summary of the results: '26 Hashes', '6 Domains', '6 URLs', '1 IPs', '0 Emails', and '11 Files'.

## MITRE ATT&CK Context

Security engineers can also check out the details of the UAC-0149 attack using COOKBOX malware provided in the most recent CERT-UA alert. Explore the table below to access a comprehensive list of adversary TTPs linked to the relevant Sigma rules, facilitating a thorough analysis:

Tactics	Techniques	Sigma Rule
Initial Access	Phishing: Spearphishing Attachment ( <a href="#">T1566.001</a> )	<a href="#">Suspicious MSOffice Child Process (via cmdline)</a>
		<a href="#">Signal Messenger Drops Suspicious Files (via file_event)</a>
Execution	User Execution: Malicious File ( <a href="#">T1204.002</a> )	<a href="#">Suspicious MSOffice Child Process (via cmdline)</a>
	Command and Scripting Interpreter: PowerShell ( <a href="#">T1059.001</a> )	<a href="#">Suspicious Powershell Strings (via powershell)</a>
		<a href="#">The Possibility of Execution Through Hidden PowerShell Command Lines (via cmdline)</a>
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder ( <a href="#">T1547.001</a> )	<a href="#">Possible Persistence Points [ASEPs - Software/NTUSER Hive] (via registry_event)</a>
		<a href="#">Suspicious File Extension Added to Run Keys [ASEPs] (via registry_event)</a>
Defense Evasion	Hide Artifacts: Hidden Window ( <a href="#">T1564.003</a> )	<a href="#">The Possibility of Execution Through Hidden PowerShell Command Lines (via cmdline)</a>
	Obfuscated Files or Information ( <a href="#">T1027</a> )	<a href="#">Possible Powershell Obfuscation Indicators (via powershell)</a>

Discovery	System Information Discovery ( <a href="#">T1082</a> )	<a href="#">Possible System Enumeration (via cmdline)</a>
		<a href="#">Possible SystemRestore Disabling Activity (via cmdline)</a>
Command and Control	Proxy: Domain Fronting ( <a href="#">T1090.004</a> )	<a href="#">Possible Cloudflare Development Domain Abuse (via dns)</a>
	Ingress Tool Transfer ( <a href="#">T1105</a> )	<a href="#">Possible Github File Downloading Initiated By Unusual Process (via network_connection)</a>