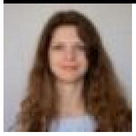
UAC-0219 Attack Detection: A New Cyber-Espionage Campaign Using a PowerShell Stealer WRECKSTEEL

SOC PRIME
UAC-0219
CERT-UA Warns Defenders of Cyber-Espionage Using WRECKSTEEL Stealer



WRITTEN BY

Veronika Telychko

Technical Writer

[post-views]

April 03, 2025 · 3 min read

In late March 2025, CERT-UA observed a surge in cyber-espionage operations targeting Ukraine, orchestrated by the UAC-0200 hacking group using DarkCrystal RAT. Researchers have recently uncovered at least three other cyber-espionage attacks throughout March against state bodies and critical infrastructure organizations in Ukraine, aiming to steal sensitive information from compromised systems using specialized malware. These attacks are attributed to the UAC-0219 hacking collective and rely on WRECKSTEEL malware, which has been observed in both VBScript and PowerShell variants.

Detect UAC-0219 Attacks Using WRECKSTEEL Covered in CERT-UA#14283 Alert

According to Cyble's research, phishing remained the dominant attack vector in Ukraine's cyber threat landscape in 2024, with attackers using spear-phishing emails containing malicious links or attachments to exploit human error as an entry point.

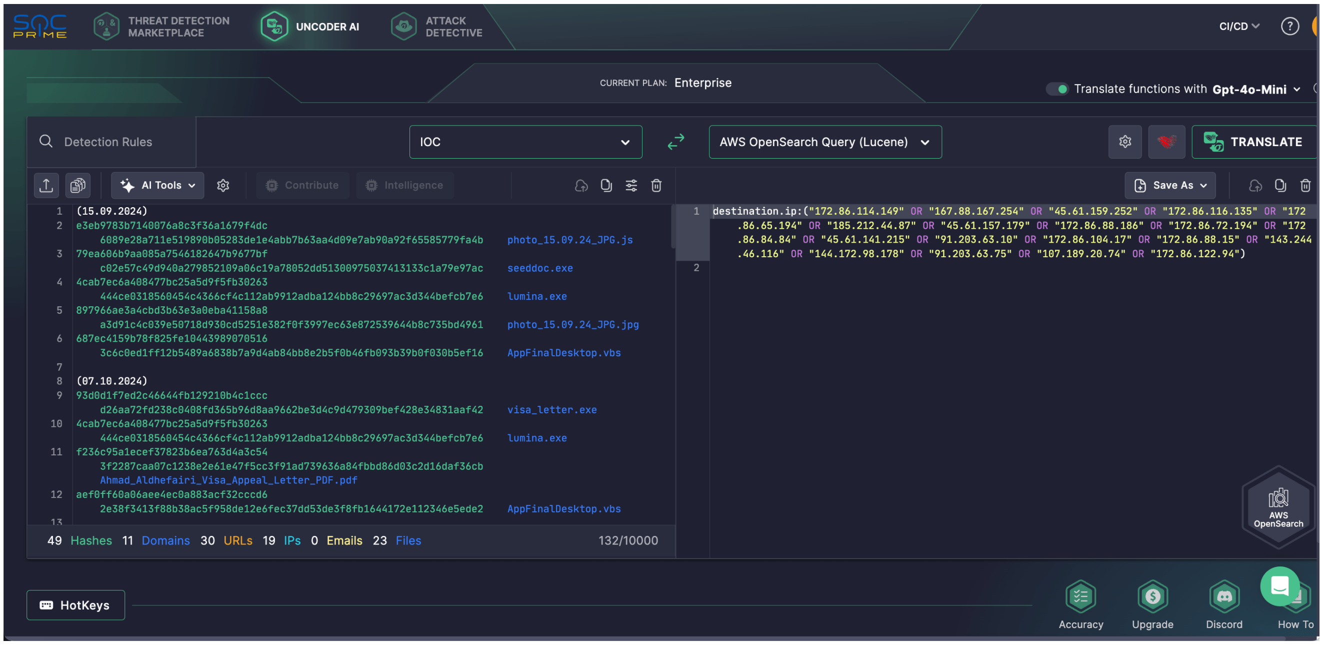
At the turn of April 2025, CERT-UA issued an alert CERT-UA#14283 warning the global cyber defender community of at least three cyber-espionage incidents focused on data theft using the specialized PowerShell-based stealer dubbed WRECKSTEEL.

SOC Prime Platform for collective cyber defense curates a dedicated collection of Sigma rules to help enterprises, including government agencies and critical infrastructure organizations, proactively defend against UAC-0219 attacks covered in the CERT-UA#14283 alert. Click the **Explore Detections** button to instantly access a relevant set of detection algorithms compatible with multiple cloud-native and on-prem SIEM, EDR, and Data Lake solutions, aligned with MITRE ATT&CK®, and enhanced with comprehensive threat intel.

Explore Detections

Alternatively, security teams can directly apply the corresponding "UAC-0219" or "WRECKSTEEL" tags to refine their content search within the Detection-as-Code library on SOC Prime Platform.

Security engineers can also rely on Uncoder AI to simplify IOC matching and enhance retrospective threat hunting. This private IDE and AI-powered co-pilot for threat-informed detection engineering seamlessly converts IOCs from the relevant CERT-UA research into custom hunting queries, ready for use in SIEM or EDR environments to identify potential UAC-0219 threats.



CURRENT PLAN: Enterprise

Translate functions with Gpt-4o-Mini

IOC

AWS OpenSearch Query (Lucene)

```
(15.09.2024)
e3eb9783b7140076a8c3f36a1679f4dc
    6089e28a711e519890b05283de1e4abb7b63aa4d09e7ab90a92f65585779fa4b    photo_15.09.24_JPG.js
79ea606b9aa085a7546182647b9677bf
    c02e57c49d940a279852109a06c19a78052dd51300975037413133c1a79e97ac    seeddoc.exe
4cab7ec6a408477bc25a5d9f5fb30263
    444ce0318560454c4366cf4c112ab9912adba124bb8c29697ac3d344befcb7e6    lumina.exe
897966ae3a4cbd3b63e3a0eba41158a8
    a3d91c4c039e50718d930cd5251e382f0f3997ec63e872539644b8c735bd4961    photo_15.09.24_JPG.jpg
687ec4159b78f825fe10443989070516
    3c6c0ed1ff12b5489a6838b7a9d4ab84bb8e2b5f0b46fb093b39b0f030b5ef16    AppFinalDesktop.vbs

(07.10.2024)
93d0d1f7ed2c46644fb129210b4c1ccc
    d26aa72fd238c0408fd365b96d8aa9662be3d4c9d479309bef428e34831aaf42    visa_letter.exe
4cab7ec6a408477bc25a5d9f5fb30263
    444ce0318560454c4366cf4c112ab9912adba124bb8c29697ac3d344befcb7e6    lumina.exe
f236c95a1ecef37823b6ea763d4a3c54
    3f2287caa07c1238e2e61e47f5cc3f91ad739636a84fbbd86d03c2d16daf36cb
    Ahmad_Aldhefairi_Visa_Appeal_Letter_PDF.pdf
aef0ff60a06aee4ec0a883acf32cccd6
    2e38f3413f88b38ac5f958de12e6fec37dd53de3f8fb1644172e112346e5ede2    AppFinalDesktop.vbs
```

```
49 Hashes  11 Domains  30 URLs  19 IPs  0 Emails  23 Files                132/10000
```

```
destination.ip:("172.86.114.149" OR "167.88.167.254" OR "45.61.159.252" OR "172.86.116.135" OR "172
    .86.65.194" OR "185.212.44.87" OR "45.61.157.179" OR "172.86.88.186" OR "172.86.72.194" OR "172
    .86.84.84" OR "45.61.141.215" OR "91.203.63.10" OR "172.86.104.17" OR "172.86.88.15" OR "143.244
    .46.116" OR "144.172.98.178" OR "91.203.63.75" OR "107.189.20.74" OR "172.86.122.94")
```

UAC-0219 Attack Analysis

CERT-UA continues to systematically collect and analyze cyber incident data to provide up-to-date threat intelligence. In March 2025, at least three cyber-attacks against government agencies and the critical infrastructure sector in Ukraine were observed in the cyber threat landscape linked to the UAC-0219 hacking group. Adversaries primarily relied on WRECKSTEEL malware designed for file exfiltration, available in both its VBScript and PowerShell iterations.

In this latest campaign addressed in the corresponding CERT-UA#14283 heads-up, the group leveraged compromised accounts to distribute phishing emails containing links to public file-sharing services such as DropMeFiles and Google Drive. In some cases, these links were embedded within PDF attachments. Clicking these links triggered the download and execution of a VBScript loader (typically with a .js extension), which then executed a PowerShell script. This script was designed to search for and exfiltrate files of specific extensions (.doc, .txt, .xls, .pdf, etc.) and capture screenshots using cURL.

Analysis indicates that this malicious activity has been ongoing since at least fall 2024. Previously, threat actors deployed EXE files created with the NSIS installer, which contained decoy documents (PDF, JPG), a VBScript-based stealer, and the image viewer “IrfanView” for taking screenshots. However, since 2025, the screenshot-capturing functionality has been integrated into PowerShell.

MITRE ATT&CK® Context

Leveraging MITRE ATT&CK provides in-depth visibility into the context of the latest UAC-0219 cyber-espionage operation targeting state bodies and critical infrastructure organizations in Ukraine. 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
Execution	Command and Scripting Interpreter: PowerShell (T1059.001)	Download or Upload via Powershell (via cmdline)
		Call Suspicious .NET Methods from Powershell (via powershell)
		The Possibility of Execution Through Hidden PowerShell Command Lines (via cmdline)
	Command and Scripting Interpreter: Visual Basic (T1059.005)	LOLBAS WScript / CScript (via process_creation)
	Command and Scripting Interpreter: JavaScript (T1059.007)	LOLBAS WScript / CScript (via process_creation)
Defense Evasion	Masquerading: Double File Extension (T1036.007)	Possible Malicious JS File with Double Extension (via cmdline)
	Hide Artifacts: Hidden Window (T1564.003)	The Possibility of Execution Through Hidden PowerShell Command Lines (via cmdline)
Discovery	System Network Configuration Discovery (T1016)	Possible IP Lookup Domain Communications Attempted (via dns)
	System Information Discovery (T1082)	Possible System Information Discovery Using Wmi Powershell Module (via powershell)
Collection	Screen Capture (T1113)	Possible Screen Capture (via powershell)

Command and Control	Application Layer Protocol: Web Protocols (T1071.001)	Suspicious File Download Direct IP (via proxy)
		Suspicious File Download Direct IP (via proxy)
	Ingress Tool Transfer (T1105)	Download or Upload via Powershell (via cmdline)
		Possible Data Infiltration / Exfiltration via Third Party Services/Tools (via proxy)
		Suspicious File Download Direct IP (via proxy)
		Suspicious CURL Usage (via cmdline)
Exfiltration	Exfiltration Over Web Services (T1567)	Suspicious CURL Usage (via cmdline)