

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

By Veronika Zahorulko

Published: 2025-04-03 · Archived: 2026-04-05 19:23:22 UTC

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.

 Rely on Uncoder AI to hunt for IOCs from the CERT-UA#14283 alert and timely spot intrusions by UAC-0219 actors.

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.

Source: <https://socprime.com/blog/detect-uac-0219-attacks-against-ukrainian-state-bodies/>