UAC-0114 Group aka Winter Vivern Attack Detection: Hackers Launch Phishing Campaigns Targeting Government Entities of Ukraine and Poland

socprime.com/blog/uac-0114-group-aka-winter-vivern-attack-detection-hackers-launch-malicious-phishing-campaigns-targeting-government-entities-of-ukraine-and-poland/

Veronika Telychko

Veronika Telychko

UAC-0114 Group aka Winter Vivern Attack Detection

Since the outbreak of the global cyber war, state bodies of Ukraine and its allies have become targets of diverse malicious campaigns launched by multiple hacking collectives. Threat actors frequently leverage phishing attack vectors to perform their adversary campaigns, like in December 2022's cyber attacks distributing DolphinCape and FateGrab/StealDeal malware.

On February 1, 2023, CERT-UA cybersecurity researchers issued a novel CERT-UA#5909 alert, in which they drew the defenders' attention to a fake webpage prompting targeted users to download software disguised as virus-scanning utilities. Hackers apply this fraudulent web page, which impersonates an official web resource of the Ministry of Foreign Affairs of Ukraine, as a lure to spread malware on the compromised systems. The hacking collective behind these attacks might include russia-linked cybercriminals.

UAC-0114/Winter Vivern Activity: Analysis of the Latest Campaign Targeting State Bodies

Hard on the heels of yet another malicious campaign by the notorious russia-backed Sandworm APT group (aka UAC-0082), Ukrainian state bodies are again under phishing attacks along with the government organizations of the Republic of Poland.

The latest CERT-UA#5909 alert details the ongoing malicious campaign targeting Ukrainian and Polish government organizations. In this cyber attack, hackers take advantage of a fake web page masquerading as the official web resource of the Ukrainian state bodies to lure victims into downloading malicious software.

The infection chain starts by following a lure link to the fake virus-scanning software, which results in downloading the malicious “Protector.bat” file. The latter launches a set of PowerShell scripts, one of which applies a recursive search algorithm to browse the desktop catalog for files with specific extensions, including .edb, .ems, .eme, .emz, .key, etc. The latter script is also capable of screen capturing and further data exfiltration via HTTP. Adversaries also leverage a set of malware persistence techniques using scheduled tasks, which poses a challenge to attack detection.

Cooperation with CERT Polska and CSIRT MON enabled cyber defenders to uncover similar phishing web resources impersonating official web pages of Ukrainian and Polish government entities, including the Ministry of Foreign Affairs of Ukraine, The Security Service of Ukraine (SBU), and the Polish Police. Notably, in June 2022, a similar phishing web page masqueraded as the UI of the mail service of the Ministry of Defence of Ukraine.

The malicious activity is being tracked as UAC-0114, attributed to the Winter Vivern hacking collective. The adversary TTPs leveraged in these phishing campaigns are quite common, including the use of PowerShell scripts and the email subject lure related to malware scanning. It is also highly likely that the above-mentioned hacking group involves russian-speaking members since one of the applied malware, APERETIF software, includes a code line typical of russia-affiliated adversary behavior patterns.

Detecting the Malicious activity of UAC-0114 Covered in the CERT-UA#5909 Alert

SOC Prime stays on the frontline helping Ukraine and its allies proactively defend against russia-affiliated malicious activity. SOC Prime’s Detection as Code platform curates a batch of Sigma rules to help teams timely identify the presence of malware related to the recent phishing campaign by the UAC-0114 group covered in the dedicated CERT-UA#5909 alert. All detections are aligned with the MITRE ATT&CK® framework v12 and are compatible with the industry-leading SIEM, EDR, and XDR technologies.

Click the **Explore Detections** button for access to a comprehensive list of Sigma rules to detect TTPs typical of the UAC-0114 group, which is behind phishing attacks against Ukraine and Poland. For streamlined content search, all detection algorithms are filtered by the corresponding custom tags “CERT-UA#5909” and “UAC-0114” based on the CERT-UA alert and group identifiers. Also, security engineers can drill down to relevant cyber threat context, including ATT&CK and CTI references, mitigations, and operational metadata, to facilitate their threat research.

Explore Detections

To make the most of IOC-based threat hunting and shave seconds off ad-hoc manual tasks, security engineers can instantly generate IOC queries associated with the ongoing attacks by UAC-0114 threat actors via Uncoder CTI. Paste file, host, or network IOCs from the relevant CERT-UA#5909 alert, build custom IOC queries on the fly, and you’re all set to search for related threats in your selected SIEM or XDR environment.

Uncoder CTI: IOC queries from CERT-UA#5909 alert

MITRE ATT&CK Context

For in-depth context behind the latest phishing campaign by the UAC-0114 aka Winter Vivern group, all dedicated Sigma rules are mapped to ATT&CK addressing relevant tactics and techniques:

Tactics	Techniques	Sigma Rule
Command and Control	Ingress Tool Transfer (T1105)	Download or Upload via Powershell (via cmdline)
Execution	Command and Scripting Interpreter (T1059)	The Possibility of Execution Through Hidden PowerShell Command Lines (via cmdline) Environment Variables in Command Line Arguments (via cmdline) Call Suspicious .NET Classes/Methods from Powershell CommandLine (via process_creation) Call Suspicious .NET Methods from Powershell (via powershell) Suspicious Usage of Invoke-RestMethod (via powershell) Download or Upload via Powershell (via cmdline)
Scheduled Task/Job (T1053)	Possible Actor Activity by Scheduled Task Pointing to Suspicious Directory (via process_creation) Possible Schtasks or AT Usage for Persistence (via cmdline)	
Defense Evasion	Hide Artifacts (T1564)	Suspicious Files in Public User Profile (via file_event)
Exfiltration	Automated Exfiltration (T1020)	Suspicious Usage of Invoke-RestMethod (via powershell)