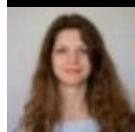


UAC-0185 aka UNC4221 Attack Detection: Hackers Target the Ukrainian Defense Forces and Military-Industrial Complex

 socprime.com/blog/uac-0185-aka-unc4221-attack-detection/



WRITTEN BY

Veronika Telychko

Technical Writer

[post-views]

December 09, 2024 · 4 min read

Since Russia launched its full-scale invasion of Ukraine, defense organizations have been heavily targeted by multiple hacking groups via the phishing attack vector. CERT-UA researchers recently shed light on the latest attacks by UAC-0185 (aka UNC4221) targeting

Ukrainian organizations within the defense-industrial sector. [The new CERT-UA alert](#) covers cyber attacks using email spoofing and masquerading the sender as the Ukrainian Union of Industrialists and Entrepreneurs (UUIE).

Detect UAC-0185 aka UNC4221 Attacks Covered in the CERT-UA#12414 Alert

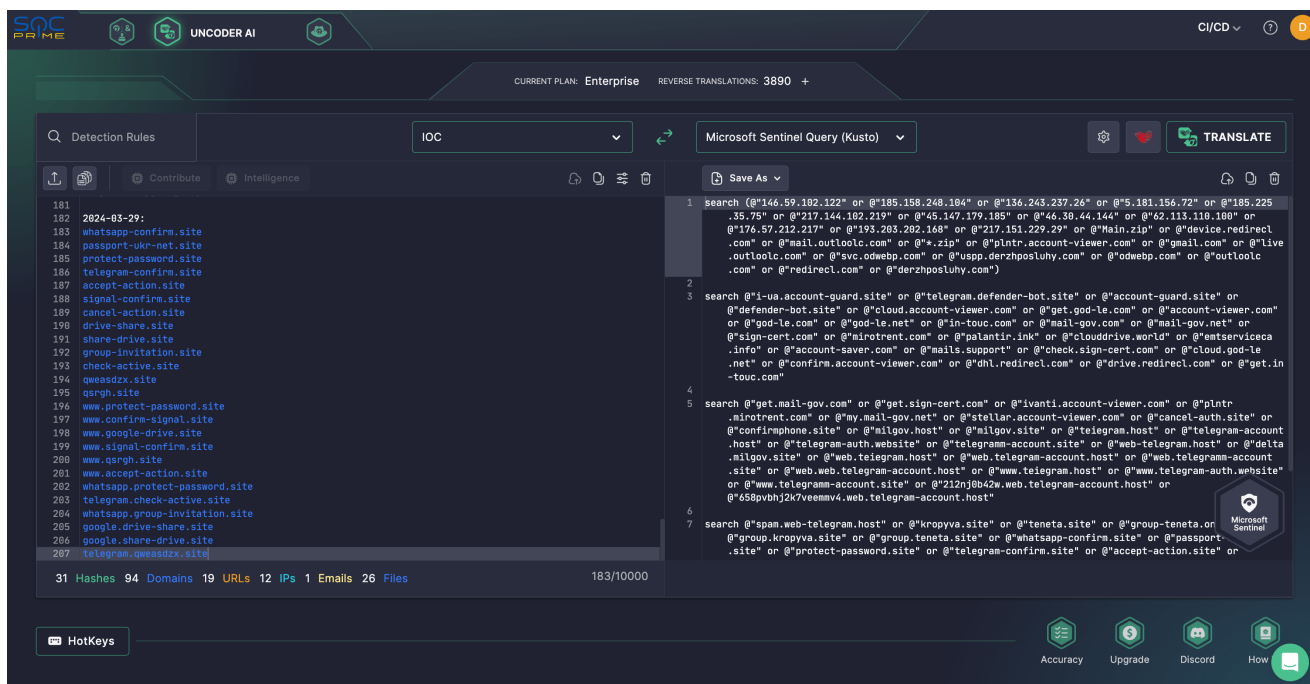
On December 7, 2024, CERT-UA issued a new security [CERT-UA#12414 heads-up](#) notifying cyber defenders of a series of phishing attacks against Ukrainian defense organizations and masquerading the sender as UUIE. To help progressive organizations withstand emerging cyber attacks that have increased in volume and sophistication since [the onset of russia's full-fledged war against Ukraine](#), SOC Prime Platform for collective cyber defense helps security teams adopt a proactive cybersecurity strategy and stay ahead of offensive forces.

Click **Explore Detections** below to reach the dedicated collection of SOC content to proactively thwart cyber attacks by the UAC-0185 (aka UNC4221) group covered in the latest CERT-UA alert. All detection algorithms are mapped to [MITRE ATT&CK®](#) and enriched with actionable CTI to ensure an in-depth threat investigation and enhanced defenses.

[Explore Detections](#)

Alternatively, cyber defenders might search for detection rules addressing hacking group TTPs with a corresponding [“UAC-0185”](#) tag in the Threat Detection Marketplace.

To proceed with the investigation, security professionals might launch instant hunts using the IOCs provided in the corresponding [CERT-UA#12414](#) alert. Rely on SOC Prime's [Uncoder AI](#) to create custom IOC-based queries in a matter of seconds and automatically work with them in your chosen SIEM or EDR environment.



UAC-0185 aka UNC4221 Attack Analysis

On December 4, 2024, CERT-UA received information from MIL.CERT-UA regarding the mass email distribution leveraging phishing lures to encourage recipients to open the email contents. Those emails impersonated the sender as the UUIE and were disguised as invitations to the corresponding conference focused on transitioning Ukraine's defense industry products to NATO technical standards. The research into the malicious activity has uncovered that the UAC-0185, also known as UNC4221, can be attributed to the corresponding phishing campaign.

The hacking collective behind attacks covered in the CERT-UA#12414 alert has been active in the cyber threat arena since at least 2022. Adversaries are primarily involved in credential theft via popular messaging applications like Signal, Telegram, and WhatsApp, as well as military systems such as DELTA, TENETA, and Kropyva. Additionally, the group conducts limited cyber attacks aimed at gaining unauthorized remote access to the computers of employees related to the military-industrial sector and the Defense Forces of Ukraine. UAC-0185 commonly employs custom tools, including MESHAGENT and UltraVNC.

Emails contained a lure hyperlink to attract the victims' attention and click it. Once clicked, it triggered the download of a shortcut file onto the targeted computer. Opening this LNK file initiated the download and execution of an HTA file via the mshta.exe utility. The HTA file contained JavaScript code designed to run two PowerShell commands. One command downloaded and opened a decoy document resembling a letter from UUIE, while the other downloaded a file named "Front.png." The latter was a ZIP archive containing three malicious files. By extracting the archive, one of the files dubbed "Main.bat" was executed.

The BAT file moved another file named “Registry.hta” to the startup directory, executed it, and deleted some downloaded files. Finally, the above-mentioned HTA file launched an executable one identified as a remote control program, MESHAGENT. Further analysis uncovered additional files and adversary infrastructure linked to cyber attacks dating back to early 2023.

MITRE ATT&CK Context

Leveraging MITRE ATT&CK provides extensive visibility into the behavior patterns of the latest UAC-0185 malicious activity against Ukrainian defense forces and the military. Explore the table below for the complete 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)	An Archive Was Extracted To Suspicious Directory Using Powershell (via powershell)
		Download or Upload via Powershell (via cmdline)
		Possible Execution by Use of Short Script Name (via cmdline)
	Command and Scripting Interpreter: Windows Command Shell (T1059.003)	Possible Execution by Use of Short Script Name (via cmdline)
	Command and Scripting Interpreter: Visual Basic (T1059.005)	Possible Execution by Use of Short Script Name (via cmdline)
Persistence	Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder (T1547.001)	Suspicious Binary / Scripts in Autostart Location (via file_event)
Defense Evasion	System Binary Proxy Execution (T1218)	Suspicious LOLBAS MSHTA Defense Evasion Behavior by Detection of Associated Commands (via process_creation)

Possible LOLBAS Chain (via cmdline)

Impair Defenses: Disable or
Modify System Firewall
(T1562.004)

Advfirewall Rule With Action Allow Created
For Binary In Suspicious Location (via
cmdline)

Command
and
Control

Ingress Tool Transfer (T1105)

Download or Upload via Powershell (via
cmdline)