UAC-0063 Attack Detection: Hackers Target Ukrainian Research Institutions Using HATVIBE, CHERRYSPY, and CVE-2024-23692

socprime.com/blog/uac-0063-attack-detection-hackers-target-ukrainian-research-institutions-using-hatvibe-cherryspy-and-cve-2024-23692/

Veronika Telychko

Since the outbreak of the full-scale war in Ukraine, cyber defenders have identified the growing volumes of cyber-espionage campaigns aimed at collecting intelligence from the Ukrainian state bodies. Further, the same tactics, techniques, and procedures are applied to target broader geography, including North America, Europe, and Asia. Precisely, in May 2023, the UAC-0063 group launched a cyber-espionage campaign targeting Ukraine, Central Asia, Israel, and India. And now, the most recent alert by CERT-UA warns cyber defenders about the ongoing offensive operation against Ukrainian research institutions orchestrated by the same hacking collective.

Detect UAC-0063 Activity Covered in the CERT-UA#10356 Alert

The UAC-0063 group is back in the cyber threat arena, targeting the academic sector in Ukraine. The group's capability to experiment with diverse adversary toolkits and multiple infection vectors at the initial attack flow underscores the need for proactive defense. SOC Prime's Platform for collective cyber defense curates a complete product suite for AI-powered Detection Engineering, Automated Threat Hunting, and Detection Stack Validation, enabling organizations to timely spot intrusions and risk-optimize their cybersecurity posture. By following the link below, security experts can instantly reach the comprehensive detection stack addressing the latest UAC-0063 adversary activity and filtered by the "CERT-UA#10356" tag based on the alert ID.

Sigma rules for UAC-0063 attack detection based on the CERT-UA#10356 alert

All detection algorithms are mapped to the MITRE ATT&CK® framework, enriched with actionable CTI and metadata, and are ready to deploy into dozens of cloud-native and on-prem security analytics platforms.

To proactively defend against the latest and evergreen cyber attacks attributed to UAC-0063, security engineers can also access more relevant SOC content by clicking the **Explore Detections** button below.

Explore Detections

CERT-UA has provided a collection of IOCs to detect threats related to the recent activity of the UAC-0063 group. By relying on SOC Prime's Uncoder AI, defenders can simplify IOC matching by instantly converting relevant threat intelligence into custom performance-optimized queries tailored for the language format of the chosen SIEM or EDR and ready to hunt in the selected environment.


Use Uncoder AI to hunt for IOCs linked to the UAC-0063 activity from CERT-UA#10356 alert

UAC-0063 Latest Activity Analysis

CERT-UA researchers have uncovered a new malicious campaign attributed to the UAC-0063 hacking collective. Adversaries launched an attack against Ukrainian research institutions on July 8, 2024, leveraging the HATVIBE and CHERRYSPY malware.

At the initial infection stage, attackers who have access to an employee's email account send a copy of a recently sent email to dozens of recipients, including the original sender. Notably, the original attachment is replaced with another document containing a macro.

By opening the DOCX file and activating the macro, another file with a macro will be generated and opened on the computer. The latter, in turn, will create and open an encoded HTA file of the HATVIBE "RecordsService" malware, along with a scheduled task file "C:\Windows\System32\Tasks\vManage\StandaloneService" designed to launch the malicious sample.

Further, adversaries download a Python interpreter and the CHERRYSPY malware into the “C: ProgramDataPython” directory, relying on technical capabilities for hidden remote control of the computer. Unlike the previous malware version, which was obfuscated with pyArmor, the latest iteration was compiled into a .pyd (DLL) file.

Notably, the recently observed activity of the UAC-0063 actors could be affiliated with the APT28 group (UAC-0001), which is directly linked to the Main Directorate of the General Staff of russia’s Armed Forces. Additionally, a DOCX file with a similar macro was found on VirusTotal, uploaded from Armenia on July 16, 2024. The lure content of this file contains text addressed to the Department of Defense Policy of the Ministry of Defense of the Republic of Armenia on behalf of the Department of International Military Cooperation of the Ministry of Defense of the Kyrgyz Republic.

Moreover, during June 2024, defenders observed multiple instances of installing the HATVIBE backdoor through HFS HTTP File Server vulnerability (probably CVE-2024-23692) exploitation. This showcases that the UAC-0063 group applies diverse attack vectors for initial compromise.

To minimize the risks of UAC-0063 intrusions, defenders strongly recommend enabling two-factor authentication for email accounts, applying policies to block the execution of macros, mshta.exe, and other potentially hazardous software, including the Python interpreter, and following industry best practices and recommendations typical for the current cyber threat landscape.

MITRE ATT&CK Context

Leveraging MITRE ATT&CK provides extensive visibility into the behavior patterns related to the latest UAC-0063 attack against Ukrainian research institutions. 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
Initial Access	Phishing: Spearphishing Attachment (T1566.001)	Unusual Library Loading in Office Process (via image_load)
	Exploit Public-Facing Application (T1190)	Possible CVE-2024-23692 (Unauthenticated RCE Flaw in Rejetto HTTP File Server) RCE Exploitation Attempt (via webserver)
Execution	Scheduled Task/Job: Scheduled Task (T1053.005)	Suspicious Scheduled Task (via audit)
		Suspicious Svchost LoLBin Execution (via cmdline)
		Suspicious Scheduled Task Files Access via Rare Image (via file_event)
	Command and Scripting Interpreter: Visual Basic (T1059.005)	Unusual Library Loading in Office Process (via image_load)
	Command and Scripting Interpreter: Python (T1059.006)	Python File Created In Unusual Directory (via file_event)
		Python Execution from Suspicious Folders (via cmdline)
Defense Evasion	System Binary Proxy Execution: Mshta (T1218.005)	Suspicious Mshta Execution Without HTA File (via cmdline)
	Modify Registry (T1112)	Suspicious Operations on Visual Basic Object Model Settings [VBOM] (via registry_event)

Table of Contents