UAC-0255 Attack Detection: Threat Actors Impersonate CERT-UA to Infect Ukrainian Public and Private Sector Organizations With AGEWHEEZE RAT

By Daryna Olyniychuk

Published: 2026-04-01 · Archived: 2026-04-10 02:01:45 UTC

Phishing remains one of the most effective tools in the cybercriminal arsenal, especially when threat actors abuse the credibility of trusted institutions and familiar digital services to increase victim interaction. In late March 2026, CERT-UA revealed a phishing campaign tracked as UAC-0255 in which attackers impersonated the agency and attempted to infect organizations across Ukraine's public and private sectors with the AGEWHEEZE RAT.

Detect UAC-0255 Attacks Covered in CERT-UA#21075

Europol notes that phishing remains the main distribution vector for data-stealing malware, reflecting how email- and URL-driven social engineering remains central to malware delivery. The same pattern is visible across the phishing activity CERT-UA has been documenting against Ukraine throughout 2026.

Earlier this year, CERT-UA reported a UAC-0190 campaign targeting the Ukrainian Armed Forces with the PLUGGYAPE backdoor, and later disclosed UAC-0252 activity in which emails impersonating central executive authorities and regional administrations lured victims into running SHADOWSNIFF and SALATSTEALER payloads. The latest UAC-0255 attack covered in CERT-UA#21075 alert fits the same broader trend, with threat actors now abusing CERT-UA's own identity to make the lure more convincing and expand targeting across both public and private sector organizations.

Register for the SOC Prime Platform to proactively detect UAC-0255 and similar attacks at the earliest stages possible. Just press **Explore Detections** below and access a relevant detection rule stack, enriched with AI-native CTI, mapped to the MITRE ATT&CK® framework, and compatible with multiple SIEM, EDR, and Data Lake technologies.

Explore Detections

Security experts can also use the "CERT-UA#21075" tag based on the relevant CERT-UA alert identifier to search for the detection stack directly and track any content changes. For more rules to detect adversary-related attacks, cyber defenders can search the Threat Detection Marketplace library using the "UAC-0255" tag.

Cybersecurity professionals can also rely on Uncoder AI to analyze threat intelligence in real time, generate Attack Flows, Sigma rules, simulations and validations, design detections in 56 languages, and create custom agentic workflows. Visit https://socprime.ai/ to learn more.

Analyzing UAC-0255 Attacks Impersonating CERT-UA to Deploy AGEWHEEZE

On March 26–27, 2026, CERT-UA identified a phishing campaign in which attackers impersonated the agency and urged recipients to download password-protected archives from the *Files.fm* service, including "*CERT_UA_protection_tool.zip*" and "*protection_tool.zip*." The archives contained malicious content presented as specialized software to be installed by targeted organizations.

Malicious emails were distributed broadly across Ukraine and targeted government organizations, medical centers, security firms, educational institutions, financial organizations, software development companies, and other entities, highlighting the campaign's reach across both public and private sectors.

CERT-UA#21075 alert also details the discovery of the fraudulent website *cert-ua[.]tech*, which reused materials from the official cert.gov.ua website and included instructions for downloading the fake protection tool. This helped the attackers reinforce the legitimacy of the lure and increase the chances of user interaction by abusing trust in Ukraine's Computer Emergency Response Team.

The executable offered for installation was determined to be a multifunctional remote access malware strain tracked by CERT-UA as AGEWHEEZE. AGEWHEEZE is a Go-based RAT that supports a broad set of remote administration capabilities. In addition to standard functions such as command execution and file management, the malware can stream screen content, emulate mouse and keyboard input, interact with the clipboard, manage processes and services, and open URLs on the compromised host.

The malware's command-and-control infrastructure was hosted on the network of French provider OVH (AS16276). On port 8443/tcp, researchers observed a web page titled "The Cult" containing an authentication form, while the HTML source included russian-language strings noting about blocked access to the service. CERT-UA also found that the associated self-signed SSL certificate had been created on March 18, 2026, and that the Organization field contained the value "TVisor."

During a review of the AI-generated *cert-ua[.]tech* website, CERT-UA found embedded references to the CyberSerp Telegram channel, including the phrase "*With Love, CYBER SERP.*" On March 28, 2026, the same Telegram channel publicly claimed responsibility for the attack, helping remove uncertainty around the technical attribution. Based on these findings, CERT-UA assigned the activity the identifier UAC-0255.

Despite the breadth of targeting, CERT-UA assessed the attack as unsuccessful. Investigators identified only several infected personal devices belonging to employees of educational institutions, and the response team provided the necessary practical and methodological assistance.

MITRE ATT&CK Context

Leveraging MITRE ATT&CK offers in-depth insight into the latest UAC-0255 phishing campaign impersonating CERT-UA. The table below displays all relevant Sigma rules mapped to the associated ATT&CK tactics, techniques, and sub-techniques.

Tactics	Techniques	Sigma Rules

Initial Access	Phishing: Spearphishing Attachment (T1566)	Possible Opening Password Protected RAR Archive (via registry_event)
Execution	Scheduled Task/Job: Scheduled Task (T1053.005)	Suspicious Scheduled Task (via audit) Suspicious Scheduled Task Files Access via Rare Image (via file_event)
Defense Evasion	Obfuscated Files or Information (T1027)	Possible Opening Password Protected RAR Archive (via registry_event)
Command and Control	Application Layer Protocol: Web Protocols (T1071.001)	Possible Data Infiltration / Exfiltration / C2 via Third Party Services / Tools (via dns) Possible Data Infiltration / Exfiltration / C2 via Third Party Services / Tools (via proxy)
	Ingress Tool Transfer (T1105)	Possible Data Infiltration / Exfiltration / C2 via Third Party Services / Tools (via dns) Possible Data Infiltration / Exfiltration / C2 via Third Party Services / Tools (via proxy)
