SmokeLoader Detection: UAC-0006 Group Launches a New Phishing Campaign Against Ukraine

By Veronika Zahorulko

Published: 2023-07-13 · Archived: 2026-04-02 11:36:03 UTC

Heads up! Cyber defenders are notified of a new wave of phishing attacks leveraging the invoice-relate email subjects with the infection chain triggered by opening a malicious VBS file, which leads to spreading SmokeLoader malware on the affected devices. According to the investigation, the malicious activity can be attributed to the financially-motivated UAC-0006 hacking gang which was observed in earlier attacks against Ukraine also using the same malicious strains and the phishing attack vector.

Analysis of UAC-0006 Offensive Operations Spreading SmokeLoader Malware

Slightly more than one month after phishing attacks by UAC-0006 financially-motivated hackers targeting Ukraine, CERT-UA researchers revealed another campaign abusing financial subject lures and also distributing SmokeLoader malware. Hackers massively spread emails with invoice-related subjects and attachments that contain a VBS file intended to install and run SmokeLoader malware on the impacted devices.

In this campaign covered in the novel CERT-UA#6999 alert, the malware configuration file contains 45 domain names, 5 of which use the A record and are linked to the russian provider. To maintain persistence, the malware iteration used in these attacks is capable of defining the current A records for domain names by connecting to the corresponding DNS server. UAC-0006 adversaries apply the compromised email accounts similarly to their behavior patterns observed in the previous campaigns against Ukraine.

As potential mitigation measures, defenders recommend restricting the use of Windows Script Host and PowerShell to minimize the threat.

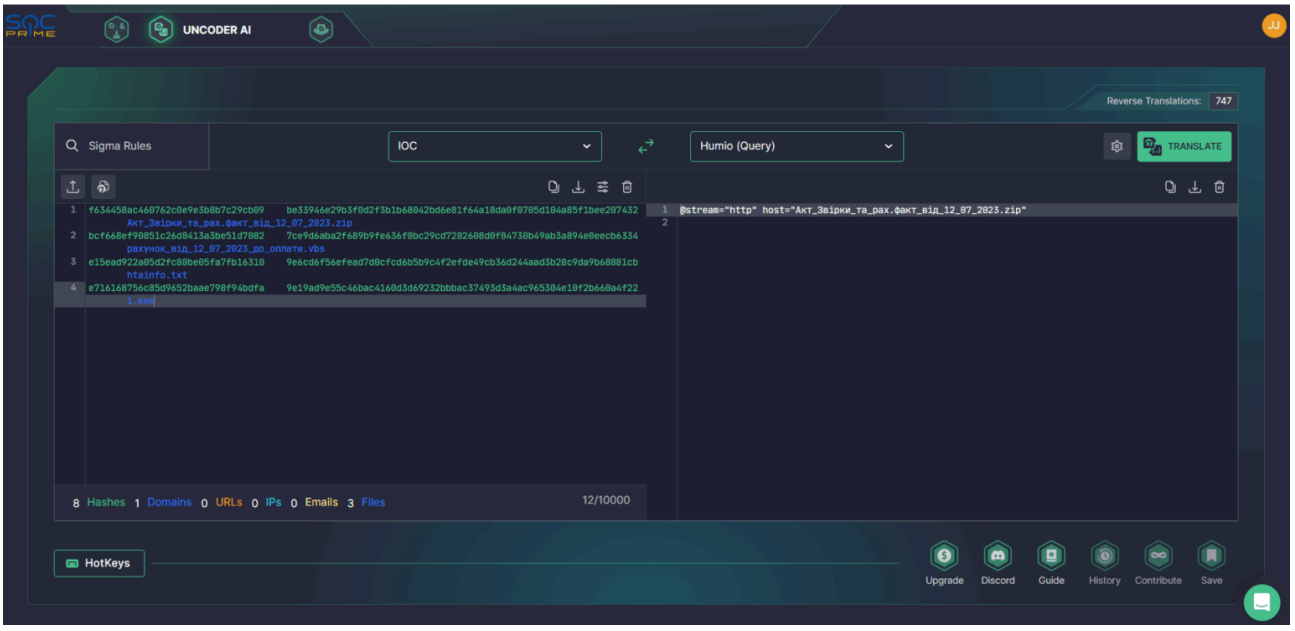
Detecting UAC-0006 Activity Covered in the CERT-UA#6999 Alert

The increasing volumes of offensive operations linked to UAC-0006 require ultra-responsiveness from cyber defenders to timely thwart the related attacks. SOC Prime Platform for collective cyber defense delivers curated Sigma rules to help organizations proactively defend against the group’s attacks massively distributing SmokeLoader and timely identify relevant adversary TTPs.

Hit the **Explore Detections** button below to obtain the entire list of Sigma rules for UAC-0006 attack detection mentioned in the CERT-UA#6999 alert. To accelerate the SOC content search, apply the relevant tags “UAC-0006” or “CERT-UA#6999”. All detection algorithms are enhanced by cyber threat context and can be automatically converted to dozens of language formats in use.

Explore Detections

Security engineers can also leverage Uncoder AI to instantly hunt for IOC listed in the CERT-UA#6999 alert by creating custom IOC queries and running them in the selected environment on the fly.



MITRE ATT&CK Context

Cyber defenders can also gain insights into the context behind phishing attacks by UAC-0006 in more detail by exploring the table below, which provides the list of relevant adversary tactics and techniques as per ATT&CK:

Source: https://socprime.com/blog/smokeloader-detection-uac-0006-group-launches-a-new-phishing-campaign-against-ukraine/