SmokeLoader Malware Detection: UAC-0006 Group Reemerges to Launch Phishing Attacks Against Ukraine Using Financial Subject Lures

By Veronika Zahorulko

Published: 2023-05-09 · Archived: 2026-04-05 16:31:53 UTC

The financially-motivated hacking collective tracked as UAC-0006 comes back to the cyber threat arena exploiting the phishing attack vector and distributing the SmokeLoader malware. According to the latest CERT-UA cybersecurity alert, threat actors massively distribute phishing emails exploiting the compromised accounts with the financially related email subject and using a malicious ZIP attachment to deploy malware on the targeted systems.

UAC-0006 Phishing Attack Analysis Spreading SmokeLoader

On May 5, 2023, CERT-UA cybersecurity researchers issued a novel CERT-UA#6613 alert covering the ongoing adversary campaigns of a notorious financially-motivated hacking group known as UAC-0006. By exploiting the malicious archive attached to phishing emails, threat actors deploy the SmokeLoader malware samples on the compromised systems. The archive is a polyglot file containing a document lure and a JavaScript code, which downloads and launches the executable file *portable.exe* via PowerShell. The latter launches the SmokeLoader malware to spread the infection further.

The UAC-0006 hacking collective behind the ongoing campaign has been in the limelight in the cyber threat arena since 2013 and up to July 2021. The group commonly uses JavaScript file uploaders at the initial attack stage. The typical adversary behavioral patterns involve gaining access to remote banking services, stealing authentication credentials, like passwords, keys or certificates, and performing unsanctioned payments, for instance, via running the HVNC bot directly from the compromised systems.

The recommended mitigation measures that help minimize the threat involve blocking the Windows Script Host on the potentially compromised computers. To enable this mitigation configuration, CERT-UA researchers suggest adding the “Enabled” property with the DWORD type and value “0” to the registry branch *{HKEY_CURRENT_USER,HKEY_LOCAL_MACHINE}\Software\Microsoft\Windows Script Host\Settings.*

Detecting SmokeLoader Malware Spread by the UAC-0006 Group and Covered in the CERT-UA#6613 Alert

With the ever-increasing volume and sophistication of phishing attacks launched by russia-affiliated actors against Ukrainian entities, organizations require a source of reliable detection content to proactively withstand possible intrusions. SOC Prime´s Detection as Code Platform aggregates a list of curated Sigma rules addressing

adversaries TTPs covered in CERT-UA inquiries. All the detection content is compatible with 28+ SIEM, EDR, and XDR solutions and mapped to the MITRE ATT&CK framework v12.

Hit the **Explore Detections** button below and dive into dedication detection content identifying the latest SmokeLoader campaign by UAC-0006. All the rules are enriched with relevant metadata, including ATT&CK references and CTI links. To streamline the content search, SOC Prime Platform supports filtering by the custom tag “CERT-UA#6613” and a broader tage “UAC-0006” based on the alert and group identifiers.

Explore Detections

Security practitioners can also streamline their threat hunting operations by searching for IoCs linked to the latest UAC-0006 campaign against Ukrainian organizations using Uncoder.IO. Just paste the IoCs listed in the latest CERT-UA report into the tool and easily convert it to performance-optimized query in a matter of seconds.


IOCs from the CERT-UA#6613 to detect UAC-0006-related threats via Uncoder.IO

MITRE ATT&CK Context

To delve into the context behind the ongoing UAC-0006 phishing attacks leveraging SmokeLoader malware, all the above-referenced Sigma rules are tagged with ATT&CK v12 addressing the relevant tactics and techniques:
