SmokeLoader Malware Detection: UAC-0006 Hackers Launch a Wave of Phishing Attacks Against Ukraine Targeting Accountants

By Veronika Zahorulko

Published: 2023-10-09 · Archived: 2026-04-05 16:39:21 UTC

In early October 2023, the UAC-0006 group was observed behind a series of at least four cyber attacks targeting Ukraine, as CERT-UA researchers report. Attackers applied a similar adversary toolkit as in previous campaigns, leveraging SmokeLoader in the latest phishing operation.

SmokeLoader Delivery: UAC-0006 Attack Analysis

On October 6, 2023, CERT-UA released four alerts notifying the peer community of a surge of phishing activity targeting Ukrainian accountants linked to the financially motivated UAC-0006 group. During this ongoing campaign, hackers leverage compromised legitimate email accounts to send phishing emails to potential victims. Also, UAC-0006 drops SmokeLoader in multiple ways, leveraging lure PDF or ZIP attachments. Opening the latter triggers JavaScript loaders or batch files that lead to running an executable file containing SmokeLoader malware. Notably, the remote access server is hosted on a russia-linked resource.

The UAC-0006 threat actors were in the spotlight in the cyber threatscape in early May 2023 and later on, in mid-July, exploiting the phishing attack vector and spreading SmokeLoader.

In the latest attacks, the UAC-0006 gang targets the personal computers of accountants striving to steal authentication data and change the details of financial documents within remote banking systems in order to send unauthorized payments. Throughout August-September 2023, adversaries made attempts to steal up to tens of millions of hryvnias.

To protect corporate networks against financial cybercrimes, CERT-UA researchers recommend applying reliable security software, restricting the launch of wscript.exe, cscript.exe, powershell.exe, mshta.exe, and similar tools, along with filtering outbound information flows.

Also, banking institutions are strongly recommended to ensure they apply basic anti-fraud practices and relevant security settings related to the payment transactions to a new counterparty, an amount exceeding the limit, and access restrictions to the client’s bank according to the list of trusted IP addresses.

Detect UAC-0006 Attacks Using SmokeLoader Highlighted in the Latest CERT-UA Alerts

With the overwhelming volumes of phishing attacks and the escalating risks of financial cybercrimes, progressive organizations are looking for ways to protect their accounting systems against intrusions. In response to emerging and existing threats of such kind, SOC Prime Platform equips defenders with innovative solutions to risk-optimize the organization’s cybersecurity posture. SOC Prime team provides security teams with behavior-based Sigma

rules to detect the ongoing malicious activity of the UAC-0006 hackers taking advantage of SmokeLoader malware. Security engineers can look for this detection content using any of the custom tags based on the CERT-UA alert IDs (“CERT-UA#7648”, “CERT-UA#7688”, “CERT-UA#7699”, “CERT-UA#7705”). Follow the link below to reach relevant Sigma rules convertible to the popular cloud and on-prem security solutions on the fly:

Sigma rules to detect ongoing attacks by UAC-0006 spreading SmokeLoader

In addition, cybersecurity experts can enhance their detection and hunting capabilities by leveraging other collections of Sigma rules for SmokeLoader detection and those to proactively defend against attacks by the UAC-0006 actors. Click the **Explore Detections** button below to drill down to the SOC content items filtered by a relevant tag (“UAC-0006”). All Sigma rules are aligned with the MITRE ATT&CK® framework and accompanied by threat intel, helping you explore all the ins and outs of the cyber threat context.

Explore Detections

Alternatively, teams can explore 30+ Sigma rules to detect SmokeLoader.

SOC Prime’s Uncoder AI can also be used to hunt for relevant IOCs provided by CERT-UA by creating custom queries and automatically running them in your cloud environment.

 Use Uncoder AI to generate custom IOC queries for UAC-0006 attack detection.

MITRE ATT&CK Context

Cyber defenders can also check out the comprehensive cyber threat context behind the wave of cyber-attacks by UAC-0006 covered in CERT-UA#7648, CERT-UA#7688, CERT-UA#7699, CERT-UA#7705 alerts. Check out the table below to find the list of all applicable adversary tactics, techniques, and sub-techniques linked to the relevant Sigma rules for in-depth threat research:
