Detecting SmokeLoader Campaign: UAC-0006 Keep Targeting Ukrainian Financial Institutions in a Series of Phishing Attacks

By Daryna Olyniychuk

Published: 2023-07-24 · Archived: 2026-04-05 18:54:29 UTC

UAC-0006 hacking collective is on the rise, actively targeting Ukrainian organizations with SmokeLoader malware in a long-lasting campaign aimed at financial profits. The latest CERT-UA cybersecurity alert details that the hacking group has launched a third massive cyber-attack in a row, severely threatening the banking systems across the country.

Analyzing UAC-0006 Phishing Campaign Aimed at SmokeLoader Distribution

In the wake of the UAC-0006 offensive operation in mid-July 2023, adversaries persistently target the Ukrainian financial sector with a third consecutive attack in the last ten days, utilizing a phishing vector to deliver SmokeLoader malware.

Detailed analysis by CERT-UA reveals that the latest attack involves the use of a dedicated ZIP polyglot file, whose contents vary based on the extracting program. If WinRAR is utilized, the ZIP polyglot would contain either a *.pdf* or *.docx* extension, leading to a sequence of JavaScript downloader, SFX-archive, BAT script, and decoy files, enticing victims with financial-themed lures, particularly related to payment instructions from Privat Bank, one of Ukraine's largest banks.

With more than 1000 devices currently enslaved to the botnet, CERT-UA states with a high level of confidence that the adversaries are leveraging compromised authentication data from previous attacks to execute large-scale phishing email campaigns.

As the malicious activities of UAC-0006 escalate, CERT-UA anticipates a notable surge in cyber fraud targeting remote banking systems. To counter these threats, defenders strongly recommend implementing mitigation measures such as restricting the use of utilities like wscript.exe, cscript.exe, powershell.exe, and mshta.exe while implementing outgoing information flow filtering.

Detecting SmokeLoader Campaing by UAC-0006 Detailedi n CERT-UA#7065, CERT-UA#7076 Alerts

To assist cyber defenders in thwarting malicious activity aimed at SmokeLoader infections, SOC Prime Platform for collective cyber defense provides a set of curated Sigma rules aimed at UAC-0006 attack detection.

Press the **Explore Detections** button below to grab an extensive batch of dedicated Sigma rules allowing security professionals timely identify relevant TTPs leveraged by the UAC-0006 collective. To streamline the SOC content search, apply the corresponding tags "UAC-0006", "CERT-UA#7065", "CERT-UA#7066," or "SmokeLoader" to

select detection algorithms enhanced with cyber threat context and automatically convertible to dozens of SIEM, EDR, XDR formats.

Explore Detections

Security engineers can also rely on Uncoder AI to seamlessly hunt for IOCs listed in recommended CERT-UA#6613, CERT-UA#6757, CERT-UA#6999 alerts 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 the latest 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:
