Unit 42 Collaborative Research With Ukraine's Cyber Agency To Uncover the Smoke Loader Backdoor

By Unit 42

Published: 2024-03-19 · Archived: 2026-04-02 10:53:19 UTC

Executive Summary

This article announces the publication of our first collaborative effort with the State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine (SCPC SSSCIP). This collaborative research focuses on recent Smoke Loader malware activity observed throughout Ukraine from May to November 2023 from a group the CERT-UA designates as UAC-0006.

Unit 42 has been collaborating with Ukraine for many years to share actionable intelligence and expertise. As the war in Ukraine enters its third year, Ukraine faces an all-time high in both volume and severity of cyberattacks. Global threat actors, including nation-states, cybercriminals and hacktivist groups, are seizing the opportunity presented by the Ukraine conflict for their malicious purposes. The SCPC SSSCIP has identified Smoke Loader as a prominent type of malware used in recent attacks.

Also known as Dofoil or Sharik, Smoke Loader is a backdoor targeting systems running Microsoft Windows. Threat actors have advertised this threat on underground forums since 2011. Primarily a loader with added information-stealing capabilities, Smoke Loader has been linked to Russian cybercrime operations and is readily available on Russian cybercrime forums.

Ukrainian officials have highlighted a surge in Smoke Loader attacks targeting the country's financial institutions and government organizations. While Ukraine has seen a rise in Smoke Loader attacks, this malware remains a global threat and continues to be seen in multiple campaigns targeting other countries. However, this surge of attacks suggests a coordinated effort to disrupt Ukrainian systems and extract valuable data.

While Smoke Loader can be distributed through web-based vectors, attacks using this malware against Ukraine have been detected in malicious emails from phishing campaigns. The SCPC SSSCIP report provides detailed analysis on 23 waves of email-based attacks from May 10-Nov. 23, 2023. This report is most beneficial to security professionals who study trends in attack chains, analyze malware or are interested in deep technical analysis and detailed indicators of compromise.

To review the technical aspects of these Smoke Loader campaigns in Ukraine, refer to the SCPC SSSCIP report.

Readers can prevent Smoke Loader and similar malware attacks by prioritizing security measures and cultivating smart online habits. Be extremely cautious when opening email attachments or clicking links, especially from unknown senders. Stick to trusted websites for downloads. Create strong, unique passwords for online accounts, and stay informed of current cybersecurity threats. These measures can significantly reduce the risk of falling victim to malware like Smoke Loader.

Palo Alto Networks customers are better protected from the Smoke Loader samples in the SCPC SSSCIP report through Cortex XDR and XSIAM, as well as through our Next-Generation Firewall with Cloud-Delivered Security Services, including Advanced WildFire, DNS Security, Advanced Threat Prevention and Advanced URL Filtering.

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

The UAC-0006 Group

On May 5, 2023, CERT-UA issued alert CERT-UA#6613, its first notification of Smoke Loader activity under the UAC-0006 identifier. Throughout the remainder of 2023, the CERT-UA published five additional notices on the UAC-0006 group.

According to CERT-UA, the UAC-0006 group ranked first in the category of financial crimes as of December 2023. UAC-0006 uses Smoke Loader to download other malware, and the group uses this additional malware in attempts to steal funds from Ukrainian enterprises. These attempts represent a significant potential for financial loss.

While CERT-UA has not confirmed a specific threat actor behind these Smoke Loader attacks, various sources suspect UAC-0006 might be associated with Russian cybercrime.

Conclusion

Palo Alto Networks collaborated with the SCPC SSSCIP to provide actionable threat intelligence to mitigate Smoke Loader attacks targeting Ukrainian organizations. Our joint research provides valuable insight into how attackers leverage Smoke Loader in real-world campaigns. This includes understanding initial attack vectors, types of secondary payloads and the overall objective of the attackers. Our research was used to help develop our mutual defenses and to disrupt the entire attack chain.

For a deeper understanding of the technical aspects of UAC-0006 Smoke Loader campaigns in Ukraine, read the SCPC SSSCIP report.

A crucial element of defense against Smoke Loader is prioritizing security measures and cultivating smart online habits. Be extremely cautious when opening email attachments or clicking links, especially from unknown senders. Stick to trusted websites for downloads, and create strong, unique passwords for all online accounts. Stay informed on current cybersecurity threats. Such vigilance should significantly reduce the risk of falling victim to malware like Smoke Loader.

Palo Alto Networks customers are better protected from Smoke Loader through Cortex XDR and XSIAM, as well as through our Next-Generation Firewall with Cloud-Delivered Security Services, including Advanced WildFire, DNS Security, Advanced Threat Prevention and Advanced URL Filtering.

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.
