IMPORTANT CYBERSECURITY NEWS: ASYNCRAT DEPLOYMENT IN NEW MALWARE CAMPAIGN

Vairav Cyber Security News Report

Date: February 24, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Cyble Research and Intelligence Labs (CRIL) has identified a new malware campaign leveraging Null-AMSI to bypass Windows security defenses and deploy AsyncRAT, a powerful remote access trojan (RAT). This attack method enables stealthy execution of malicious payloads while avoiding detection by antivirus and endpoint security solutions. The campaign tricks users into executing malicious LNK files disguised as wallpapers featuring animated characters. Upon execution, obfuscated PowerShell scripts retrieve additional payloads, which are executed directly in memory, leaving minimal forensic traces.

INCIDENT ANALYSIS

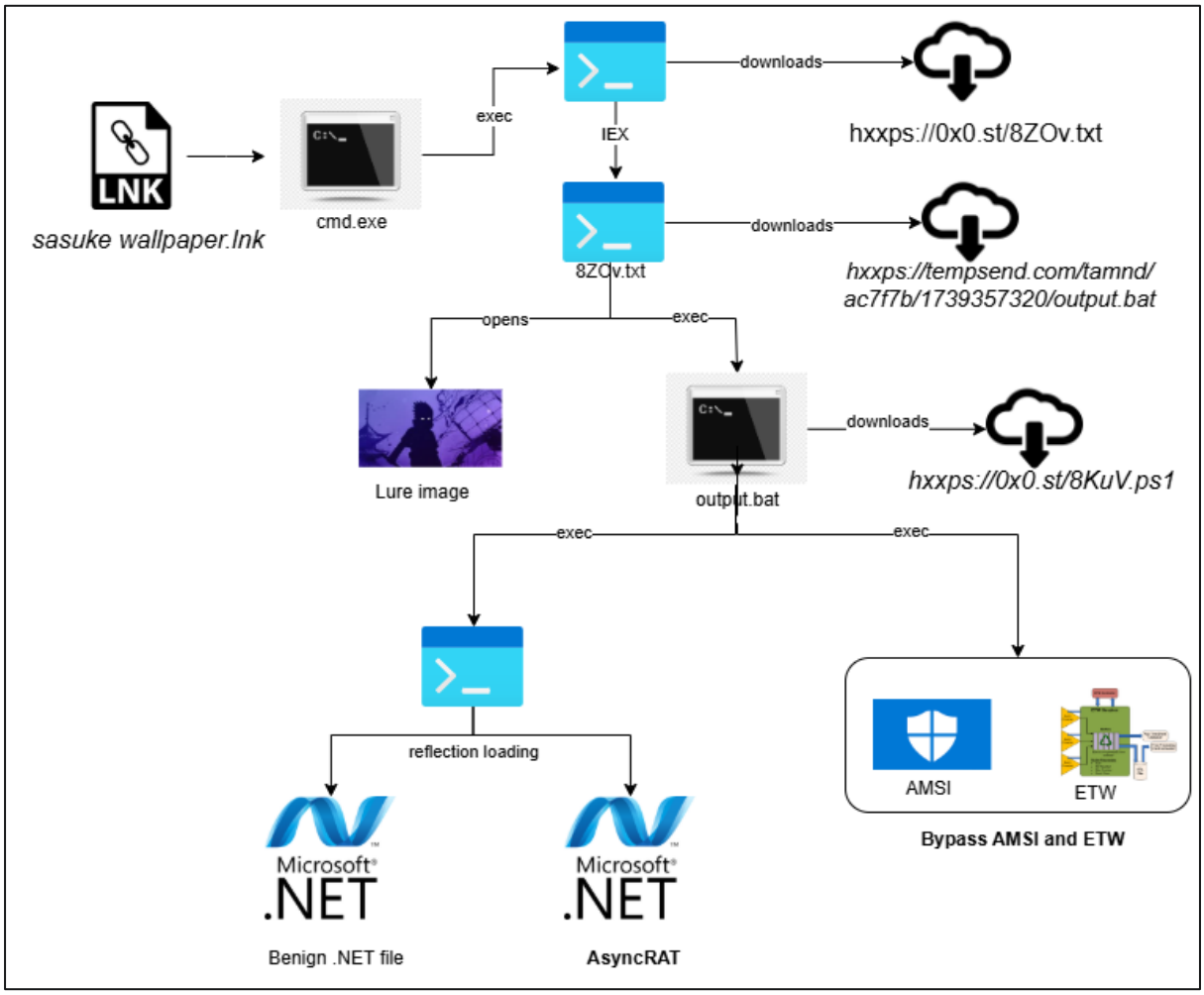

Figure 1: Infection Chain

The attack chain begins with LNK files disguised as attractive wallpapers containing malicious PowerShell scripts. Once executed, these scripts fetch additional payloads from a remote server, initiating a multi-stage execution process that remains entirely in memory.

The Null-AMSI tool is utilized to bypass AMSI and ETW protections, preventing security solutions from scanning the malicious scripts and ensuring stealthy execution. The attackers also use AES encryption and GZIP compression to further obfuscate their payloads, making detection and static analysis difficult.

Upon successful execution, AsyncRAT is loaded into memory using reflection techniques, granting the attacker full remote control of the infected system. This RAT poses a significant cybersecurity risk to organizations and individuals, enabling:

- Keystroke logging and credential theft
- Remote command execution for further exploitation
- Exfiltration of sensitive files and system information
- Persistence mechanisms to maintain long-term access
- Deployment of additional malware, escalating the attack's impact

This campaign poses a critical security threat, as the combination of AMSI bypass, in-memory execution, and strong encryption techniques makes detection extremely challenging.

RECOMMENDED ACTIONS

To mitigate the risks associated with this campaign, organizations should implement the following security measures:

- Restrict LNK file execution from untrusted sources to prevent initial access.
- Enable advanced threat detection tools capable of identifying AMSI bypass attempts and in-memory execution.
- Regularly update endpoint protection to detect and block AsyncRAT and other remote access trojans.
- Monitor PowerShell activity for obfuscated or unusual scripts using PowerShell logging and script block auditing.
- Disable script execution policies for non-administrative users to minimize risk exposure.
- Implement strict email security controls to block phishing emails by distributing malicious LNK files.
- Educate employees on social engineering tactics to prevent them from downloading and executing unknown files.

RESOURCES

https://securityonline.info/security-alert-asyncrat-malware-evades-detection-with-null-amsi/

https://cyble.com/blog/null-amsi-evading-security-to-deploy-asyncrat/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com