BREAKING CYBERSECURITY NEWS: MICROSOFT DISRUPTS MASSIVE GITHUB-BASED MALVERTISING CAMPAIGN TARGETING MILLION DEVICES

Vairav Cyber Security News Report

Date: March 07, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

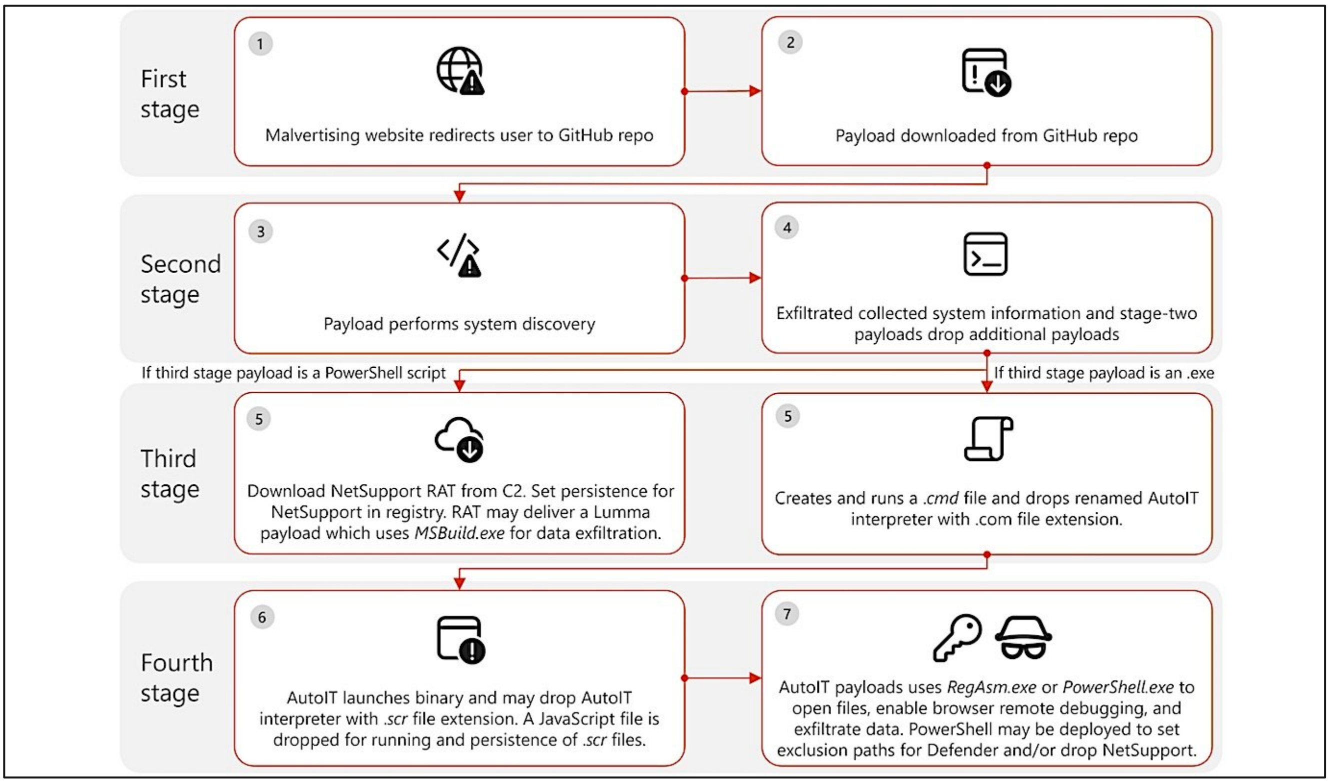
Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Microsoft has dismantled a large-scale malvertising campaign that exploited GitHub repositories to infect nearly one million devices worldwide. The attack chain, linked to Storm-0408, involved pirated streaming websites embedding malicious ads that redirected victims to GitHub-hosted malware. The malware executed multi-stage payloads, including NetSupport RAT, Lumma Stealer, and Doenerium Infostealer, to exfiltrate sensitive data and establish remote access. Microsoft has removed undisclosed GitHub repositories and observed Dropbox and Discord being used as alternative payload hosts**,** highlighting the indiscriminate nature of this attack.

INCIDENT ANALYSIS


First stage
Second stage
Third stage
Fourth stage
If third stage payload is a PowerShell script
If third stage payload is an .exe

1 Malvertising website redirects user to GitHub repo

2 Payload downloaded from GitHub repo

3 Payload performs system discovery

4 Exfiltrated collected system information and stage-two payloads drop additional payloads

5 Download NetSupport RAT from C2. Set persistence for NetSupport in registry. RAT may deliver a Lumma payload which uses *MSBuild.exe* for data exfiltration.

5 Creates and runs a *.cmd* file and drops renamed AutoIT interpreter with .com file extension.

6 AutoIT launches binary and may drop AutoIT interpreter with *.scr* file extension. A JavaScript file is dropped for running and persistence of *.scr* files.

7 AutoIT payloads uses *RegAsm.exe* or *PowerShell.exe* to open files, enable browser remote debugging, and exfiltrate data. PowerShell may be deployed to set exclusion paths for Defender and/or drop NetSupport.

Figure 1: Attack stages

The campaign began in December 2024, when Microsoft's threat analysts detected devices downloading malware from GitHub repositories.

- Attackers injected malicious ads into pirated streaming websites, redirecting users through multiple malicious domains before landing on infected GitHub repositories.
- The first-stage malware performed system discovery, collecting details like OS, memory, screen resolution, and user paths before fetching additional payloads.

- The third-stage payload, a PowerShell script, installed NetSupport RAT, providing remote control over the victim's machine.
- Attackers also deployed Lumma Stealer and Doenerium, targeting stored browser credentials, system files, and sensitive user data.
- AutoIt scripts were used to evade detection, modify Windows Defender settings, and establish persistence.
- Beyond GitHub, Dropbox and Discord were also used to host malware payloads, expanding the attack's reach across multiple platforms.

The campaign targeted both enterprise and consumer devices, affecting various industries worldwide. Microsoft's disruption of GitHub repositories helped mitigate the attack, but the continued use of alternative hosting platforms suggests the threat actors remain active. Microsoft's takedown of malicious GitHub repositories represents a major step in curbing malvertising threats. However, with attackers shifting to Dropbox, Discord, and alternative hosting platforms**,** organizations must remain vigilant against multi-stage malware that leverages trusted cloud services to bypass traditional security measures**.**

RECOMMENDED ACTIONS

- Avoid downloading files from unverified sources, especially from GitHub, Dropbox, and Discord links shared on pirated streaming sites.
- Monitor PowerShell activity for unusual script executions that may indicate malicious registry modifications or persistence mechanisms.
- Enhance endpoint security with behavior-based detections to identify multi-stage malware infections.
- Block known malicious domains associated with malvertising campaigns in enterprise security policies.
- Enable Windows Defender tamper protection to prevent exclusion path abuse by malicious payloads.
- Educate employees about malvertising risks and the dangers of downloading software from unofficial sources

RESOURCES

https://www.bleepingcomputer.com/news/security/microsoft-says-malvertising-campaign-impacted-1-million-pcs/

https://www.microsoft.com/en-us/security/blog/2025/03/06/malvertising-campaign-leads-to-info-stealers-hosted-on-github/

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