IMPORTANT CYBERSECURITY NEWS: SOPHISTICATED PHISHING CAMPAIGN DEPLOYS HAVOC FRAMEWORK VIA SHAREPOINT C2

Vairav Cyber Security News Report

Date: March 04, 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

A newly uncovered phishing campaign is leveraging ClickFix tactics and modified open-source tools to deliver a customized Havoc C2 framework via SharePoint abuse. The campaign, active as of March 2025, deceives victims into executing malicious PowerShell commands, leading to multi-stage infection and persistent access. Attackers exploit Microsoft Graph API endpoints to mask command-and-control (C2) traffic, evading traditional security defenses. This evolving attack highlights the growing sophistication of social engineering combined with cloud service abuse.

INCIDENT ANALYSIS

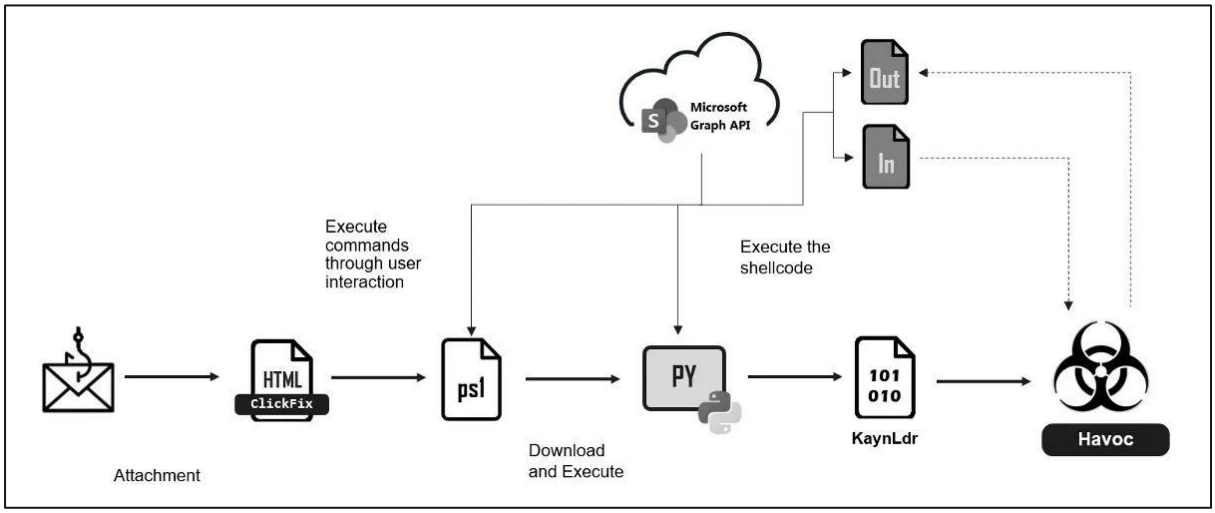

Figure 1: ClickFix Attack flow

Threat actors initiate the attack with a phishing email posing as an urgent document notification, containing an HTML file (Documents.html). Victims who open the file see a fabricated error message instructing them to copy-paste a PowerShell command into their terminal, a tactic known as ClickFix.

Once executed, the PowerShell script retrieves additional payloads from an attacker-controlled SharePoint URL, performing sandbox checks before executing the next-stage Python shellcode loader. The attack ultimately deploys a modified Havoc framework DLL, using Microsoft Graph API and SharePoint for C2 communication.

- Havoc malware communicates via SharePoint, creating hidden files for encrypted data exchange.

- Victim metadata (hostname, IP, OS details, privilege status) is exfiltrated using AES-256 encryption.
- Over 50 commands supported, including file exfiltration, lateral movement, and Kerberos ticket manipulation.
- By leveraging trusted cloud services, attackers blend malicious traffic with legitimate Office 365 requests, making detection difficult.

The weaponization of SharePoint and Microsoft Graph API for covert C2 operations underscores the evolving nature of cloud-based attacks. As offensive security tools like Havoc gain popularity, organizations must adopt proactive monitoring and cloud security measures to defend against stealthy phishing campaigns.

RECOMMENDED ACTIONS

- Educate employees on phishing tactics that involve executing terminal commands.
- Limit use of PowerShell in non-admin contexts to mitigate execution of malicious scripts.
- Detect unusual file creation patterns that may indicate abuse of Microsoft Graph API.
- Use Fortinet's IPS signatures and Content Disarm and Reconstruction (CDR) services to block malicious scripts and payloads.
- Continuously track API-driven C2 channels within SharePoint and Office 365 environments.

RESOURCES

https://cybersecuritynews.com/clickfix-tactic-to-attack-windows-machine/

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