Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

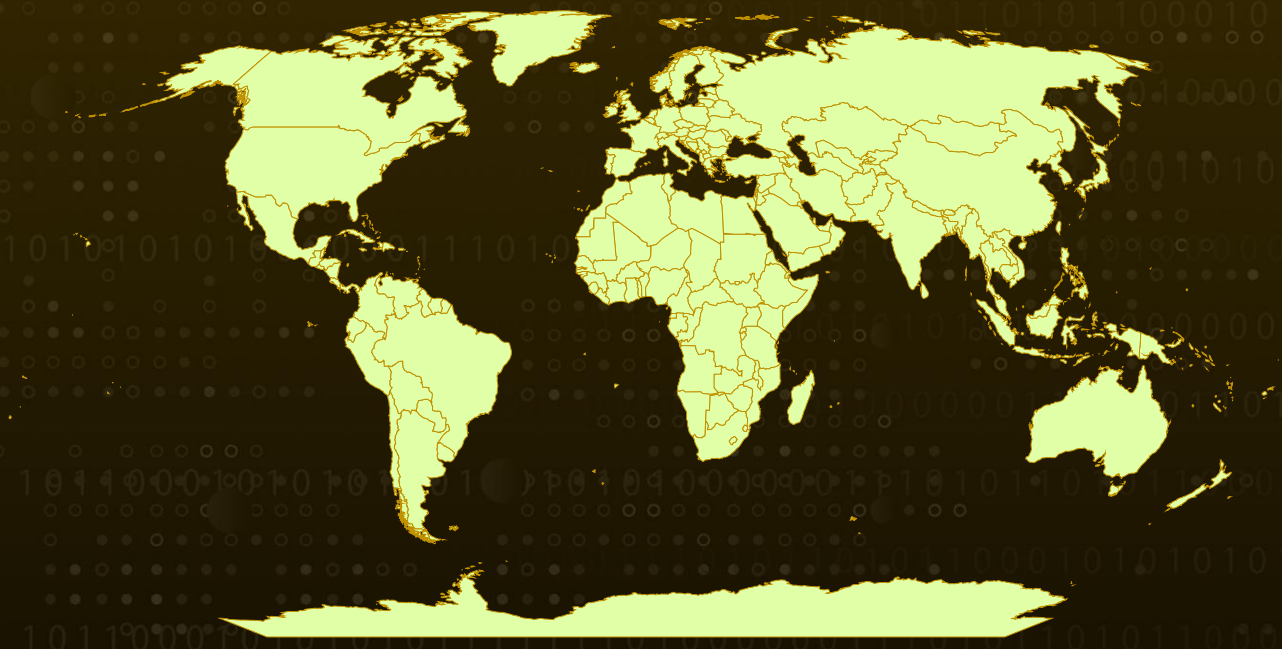
ClickFix Deception: Hackers Use SharePoint and Graph API to Deploy Havoc Malware

Date of Publication	Admiralty Code	TA Number
March 4, 2025	A1	TA2025063

Summary

Attack Discovered: January 2025
Targeted Countries: Worldwide
Affected Platforms: Microsoft Windows
Malware: Havoc Demon, KaynLdr
Attack: A recently discovered ClickFix phishing campaign is luring victims into running malicious PowerShell commands, which ultimately deploy the Havoc framework to establish remote access on compromised devices. Havoc, an open-source tool available on GitHub, allows attackers to easily modify its code, helping them evade detection. To conceal their malware delivery process, the threat actors host each infection stage on a SharePoint site, leveraging a modified version of Havoc Demon for stealth. Once successfully deployed, the attackers gain full control over infected systems, enabling them to execute further malicious actions undetected.

Attack Regions



Attack Details

#1 A newly uncovered phishing campaign is using ClickFix and a multi-stage malware infection chain to deploy a modified Havoc Demon Agent, an open-source command-and-control (C2) framework. The attackers cleverly host different malware stages on SharePoint and exploit the Microsoft Graph API to hide their C2 communications within trusted Microsoft services, making detection and blocking significantly harder.

#2 The attack begins with a phishing email carrying a malicious HTML attachment that leverages the ClickFix technique—a social engineering trick where attackers display fake errors and prompt users to "fix" them by clicking a button or following specific instructions. In this case, the fake error message deceives victims into copying and executing a malicious PowerShell command. This script, hosted on SharePoint and controlled by the attackers, first checks if it is running in a sandboxed environment by verifying the number of domain computers. It then deletes specific Windows registry entries.

#3 If pythonw.exe is missing, the script automatically downloads and installs a Python interpreter before retrieving and executing a Python-based shellcode loader, KaynLdr. This loader reflectively loads an embedded DLL, making analysis more difficult by using API hashing with a modified DJB2 algorithm. It also relies on ntdll APIs for memory allocation and execution, ultimately launching the embedded payload through the "call rax" instruction.

#4 Once deployed, the Havoc Demon Agent executes its initialization routine and uses the same API hashing technique as KaynLdr to resolve critical functions. The malware modifies the TransportSend function to facilitate C2 communication through two files used to send requests and to receive responses. By leveraging the Microsoft Graph API, the malware fetches commands, executes them, and then immediately erases the contents to avoid detection.

#5 The modified Havoc Demon Agent supports a wide range of malicious activities, including data exfiltration, file manipulation, command execution, privilege escalation, and Kerberos attacks.

#6 This campaign highlights a growing trend where threat actors abuse open-source tools and trusted cloud services to avoid detection. By embedding their malware within SharePoint and Microsoft Graph API, they create a stealthy and persistent infection chain. Organizations must stay vigilant against phishing attempts and avoid executing unverified scripts.

Recommendations

Enhance Email Security: Implement robust email filtering to block phishing emails impersonating trusted entities. Use email authentication mechanisms like DMARC, SPF, and DKIM to prevent spoofed emails. Educate employees on identifying phishing attempts.

Restrict Execution of Untrusted Files: To minimize the risk of malware infections, allow only trusted applications and scripts to run using application whitelisting. Block unauthorized PowerShell commands and enforce strict execution policies to prevent attackers from running malicious scripts.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Monitor and Restrict Unauthorized Activity: Regularly monitor SharePoint for unusual file creation patterns that could indicate malware staging or unauthorized access. Additionally, restrict PowerShell execution for non-administrative users to prevent attackers from running malicious scripts and gaining control over systems. Secure Microsoft Graph API by enforcing strict access controls, monitoring API requests for anomalies, and restricting permissions to only essential functions to prevent abuse in C2 communications.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0008** Lateral Movement	**TA0011** Command and Control
T1566 Phishing	**T1566.001** Spearphishing Attachment	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1059.006 Python	**T1033** System Owner/User Discovery	**T1082** System Information Discovery	**T1053** Scheduled Task/Job

T1140 Deobfuscate/Decode Files or Information	**T1027** Obfuscated Files or Information	**T1558** Steal or Forge Kerberos Tickets	**T1083** File and Directory Discovery
T1057 Process Discovery	**T1012** Query Registry	**T1134** Access Token Manipulation	**T1070** Indicator Removal
T1021 Remote Services	**T1564** Hide Artifacts	**T1204** User Execution	**T1204.002** Malicious File
T1036 Masquerading	**T1132** Data Encoding	**T1132.001** Standard Encoding	**T1497** Virtualization/Sandbox Evasion

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	hao771[.]sharepoint[.]com
SHA256	51796effe230d9eca8ec33eb17de9c27e9e96ab52e788e3a9965528be2902330, 989f58c86343704f143c0d9e16893fad98843b932740b113e8b2f8376859d2dd, A5210aaa9eb51e866d9c2ef17f55c0526732eacb1a412b910394b6b51246b7da, cc151456cf7df7ff43113e5f82c4ce89434ab40e68cd6fb362e4ae4f70ce65b3

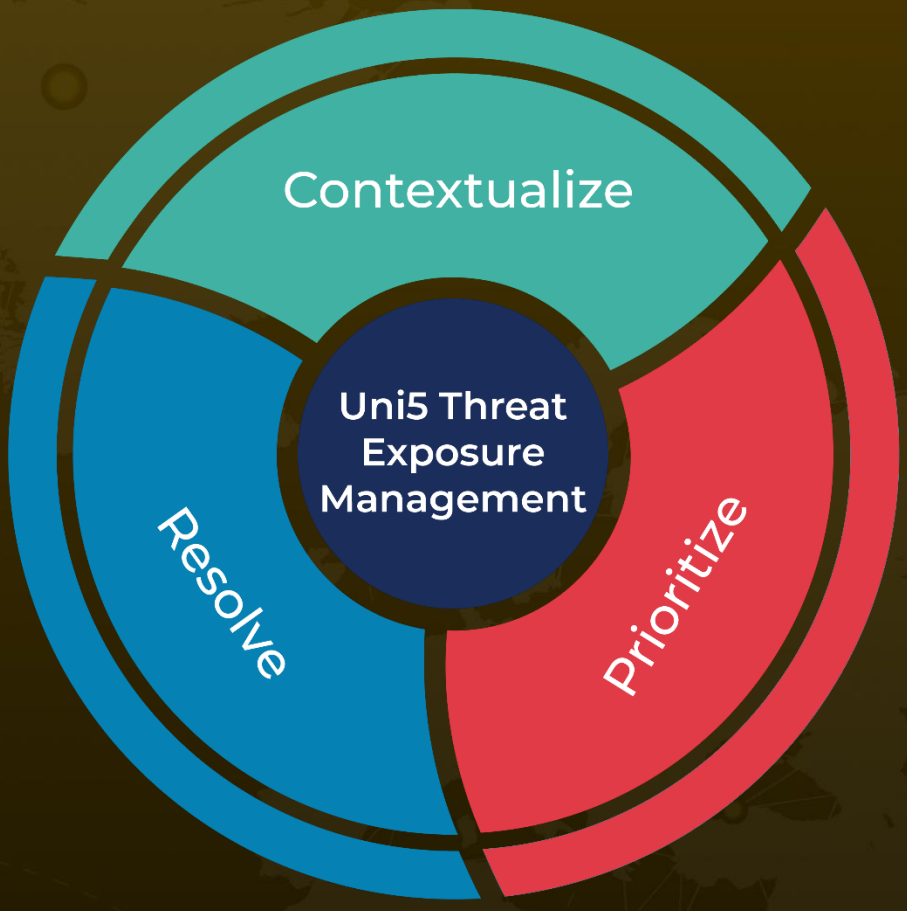
References

https://www.fortinet.com/blog/threat-research/havoc-sharepoint-with-microsoft-graph-api-turns-into-fud-c2

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 4, 2025 • 4:50 AM

More at www.hivepro.com