Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

VIPKeyLogger: A New Infostealer in Phishing Attacks

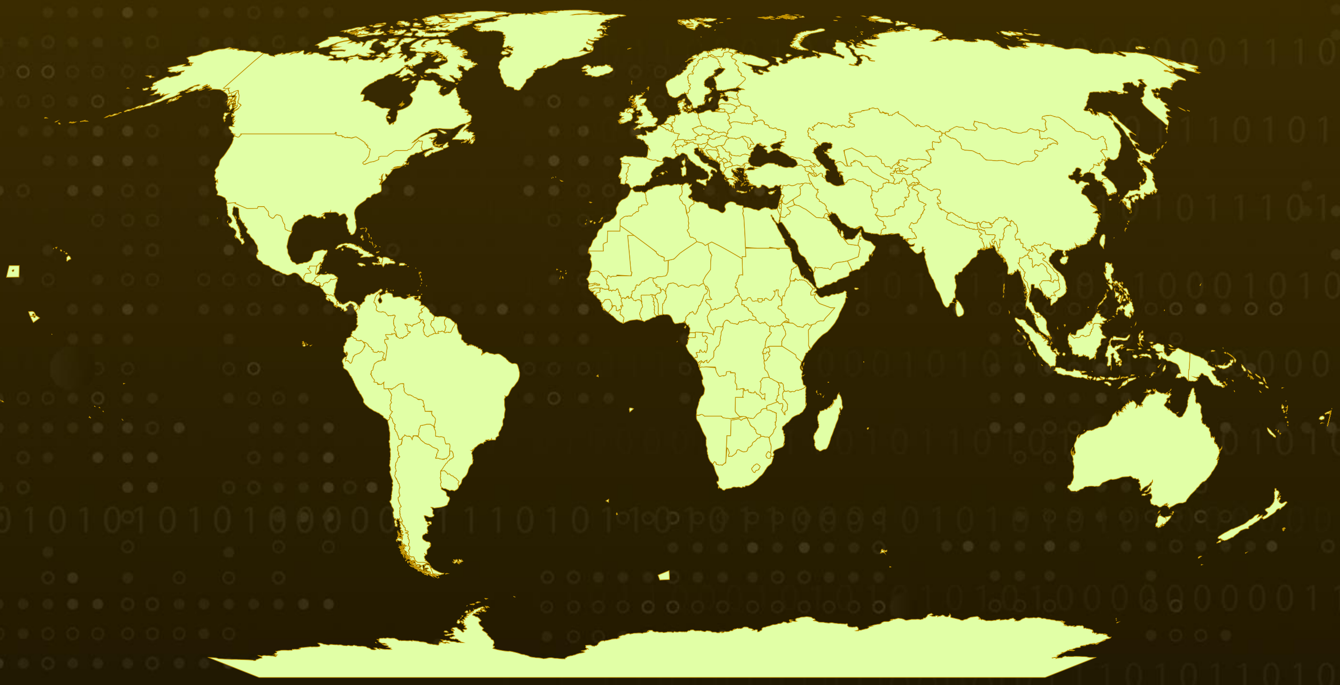
Date of Publication	Admiralty Code	TA Number
December 17, 2024	A1	TA2024463

Summary

First Seen: August 9, 2024
Targeted Countries: Worldwide
Malware: VIPKeyLogger
Affected Platform: Windows

Attack: VIPKeyLogger is a newly identified infostealer malware similar to Snake Keylogger, spreading through phishing emails with malicious Microsoft 365 attachments. It uses RTF files to download a .NET payload, enabling keylogging, data exfiltration, and persistence. The malware evades detection by obfuscation techniques and deletes itself after execution. Stolen data is sent to the attacker's server via Telegram, posing risks of identity theft and unauthorized access.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	Kubernetes Image Builder	✗	✓	✓

Attack Details

#1

VIPKeyLogger is a newly discovered infostealer malware that shares similarities with the well-known Snake Keylogger. It primarily targets victims through phishing emails containing malicious attachments, often disguised as Microsoft 365-related files to trick users into opening them. Once the attachment is accessed, the malware initiates a sophisticated infection chain designed to steal sensitive information, including login credentials and system data.

#2

The malware exploits vulnerabilities in Microsoft Office files, particularly CVE-2017-11882, to execute its payload. It leverages RTF (Rich Text Format) files containing encoded object data to download additional payloads from a remote server. When the RTF attachment is opened, it triggers the download of a .NET executable file, which installs the VIPKeyLogger malware. This executable facilitates keylogging and data exfiltration while maintaining persistence on the compromised system.

#3

VIPKeyLogger captures keystrokes, login credentials, and other system-related information. It employs various obfuscation techniques to evade detection by traditional security software. Additionally, the malware often executes from temporary or startup folders to maintain persistence and deletes itself after execution to reduce its footprint on the infected system.

#4

The stolen data is sent to the attacker’s command-and-control server using Telegram, which complicates detection efforts. This exfiltrated data can be exploited for identity theft, unauthorized account access, and other malicious activities.

Recommendations

Email Security Controls: Implement advanced email filtering solutions to detect and block malicious attachments, such as RTF files with embedded encoded objects. Enable attachment scanning and sandboxing to analyze potentially harmful files before they reach end-users. Block or quarantine emails containing uncommon file types, such as .rtf or .exe, if these are not typically used in your organization.

Endpoint Protection and Monitoring: Deploy Endpoint Detection and Response (EDR) solutions to monitor, detect, and respond to suspicious behaviors such as unauthorized processes, keylogging activities, or unusual system changes. Enable behavioral analysis to detect obfuscated malware or processes that attempt to establish persistence in temporary or startup folders.

Patch and Update Systems: Ensure all operating systems, software, and security solutions are up to date with the latest patches to mitigate vulnerabilities exploited by malware. Prioritize updates for Microsoft Office and other document-handling applications to close potential security loopholes used by malicious attachments.

Restrict Macro and Script Execution: Disable macros and scripting by default in Microsoft Office applications unless absolutely necessary. Implement group policies to restrict the execution of .exe files from temporary or startup directories to limit the malware's ability to execute and persist on infected systems.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	**TA0042** Resource Development	**TA0001** Initial Access	**TA0002** Execution
TA0007 Discovery	**TA0010** Exfiltration	**TA0009** Collection	**TA0011** Command and Control
TA0003 Persistence	**TA0006** Credential Access	**T1041** Exfiltration Over C2 Channel	**T1027** Obfuscated Files or Information
T1219 Remote Access Software	**T1059** Command and Scripting Interpreter	**T1588.006** Vulnerabilities	**T1588** Obtain Capabilities
T1566.001 Spearphishing Attachment	**T1566** Phishing	**T1204** User Execution	**T1564** Hide Artifacts

T1115 Clipboard Data	**T1113** Screen Capture	**T1204.002** Malicious File	**T1217** Browser Information Discovery
T1056.001 Keylogging	**T1056** Input Capture	**T1539** Steal Web Session Cookie	**T1070** Indicator Removal

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	A7fb35d35eb23fe3b4358e3c843f5982a161534e, 2830f9d5f41bbecd2ae105ed0b9a8d49327c8594
URLs	hxxp[://]87.120.84[.]39/txt/xXdquUOrM1vD3An.exe, hxxp[://]51.38.247[.]67:8081/_send_.php?L, hxxp[://]varders.kozow[.]com:8081, hxxp[://]aborters.duckdns[.]org:8081, hxxp[://]anotherarmy.dns[.]army:8081, hxxp[://]mail.jhxkgroup[.]online

Patch Link

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882

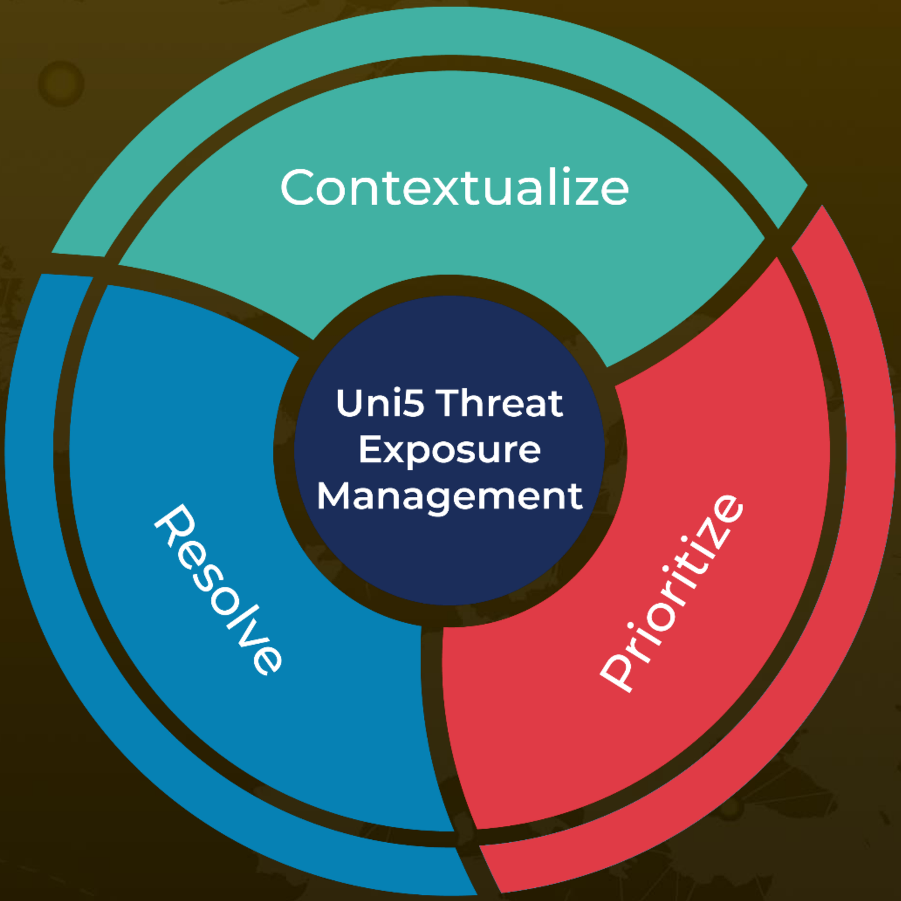
References

https://www.forcepoint.com/blog/x-labs/vipkeylogger-infostealer-malware

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

December 17, 2024 • 7:30 AM

More at www.hivepro.com