Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

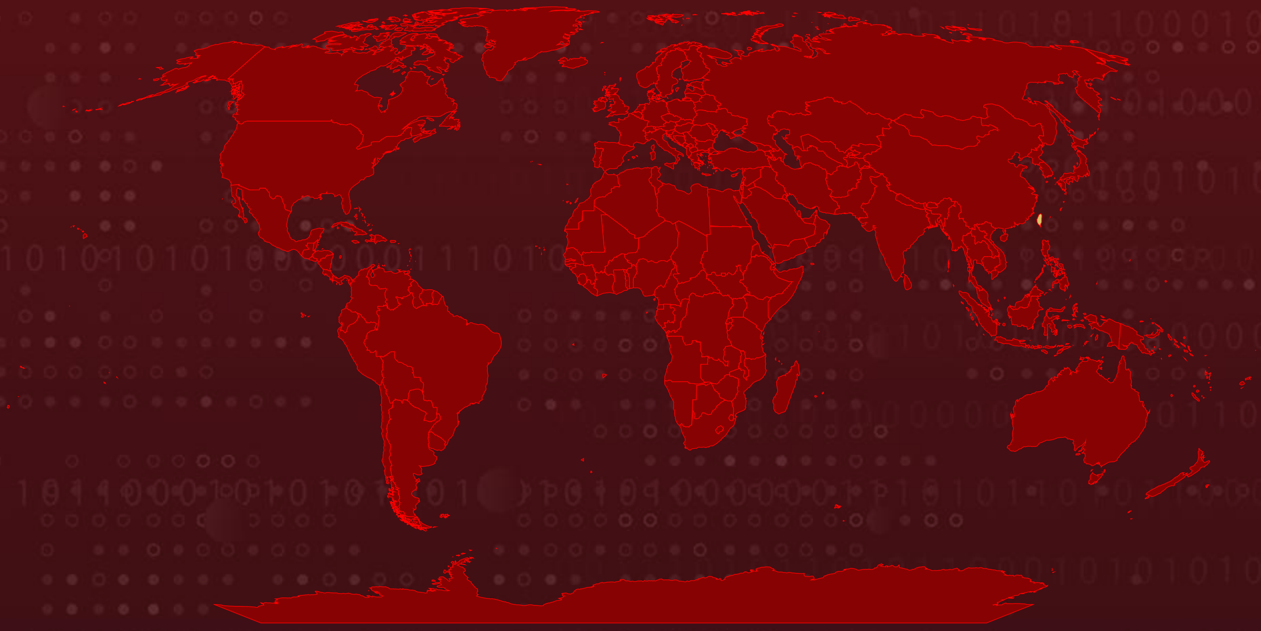
SmokeLoader Strikes Taiwan: Unveiling a Modular Malware's Sophisticated Attack Chain

Date of Publication	Admiralty Code	TA Number
December 3, 2024	A1	TA2024448

Summary

Attack Discovered: September 2024
Targeted Countries: Taiwan
Targeted Industries: Manufacturing, Healthcare and Information Technology
Affected Platforms: Microsoft Windows
Malware: SmokeLoader malware
Attack: A recent campaign has surfaced, deploying SmokeLoader malware to target organizations in Taiwan. Known for its versatility and sophisticated evasion capabilities, SmokeLoader continues to demonstrate its adaptability in the cyber threat landscape. While typically used as a downloader to deliver secondary payloads, this campaign highlights a more direct approach, SmokeLoader independently conducts the attack by fetching additional plugins from its command-and-control (C2) server, reinforcing its role as both an initial access vector and an operational threat.

Attack Regions



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2017-0199	Microsoft Office and WordPad Remote Code Execution Vulnerability	Microsoft Office and WordPad	✓	✓	✓
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	Microsoft Office	✗	✓	✓

Attack Details

#1 In September 2024, a sophisticated cyber campaign targeted Taiwanese companies across manufacturing, healthcare, and IT sectors, deploying the infamous SmokeLoader malware. Known for its modularity and advanced evasion tactics, SmokeLoader showcased its adaptability by executing the attack autonomously using plugins downloaded from its command-and-control (C2) servers. The attack began with carefully crafted phishing emails masquerading as business correspondence, falsely claiming to include quotations with special instructions.

#2 The attackers exploited two longstanding Microsoft Office vulnerabilities—CVE-2017-0199 and CVE-2017-11882—to initiate their attack chain. CVE-2017-0199 leveraged OLE2-embedded link objects to automatically download and execute malicious files when victims opened the document. Meanwhile, CVE-2017-11882, a remote code execution vulnerability in the equation editor, enabled attackers to decrypt and execute payloads that retrieved a VBS file through the URLDownloadToFile function. These vulnerabilities acted as entry points, paving the way for further exploitation using obfuscated VBS scripts and PowerShell commands to deliver the AndeLoader malware loader.

#3 Once deployed, AndeLoader downloaded an image embedded with encoded injector data using steganographic techniques. This concealed data was extracted, decoded, and executed, enabling SmokeLoader to embed itself into legitimate processes. By operating in-memory and injecting itself into trusted system processes, SmokeLoader avoided detection while maintaining persistence and operational control.

#4 The final payload was a set of nine plugins designed for targeted data collection and exfiltration. These plugins zeroed in on widely used applications, including web browsers, email clients, and FTP tools such as Firefox, Chrome, Edge, Outlook, and Thunderbird. For instance, Plugin 4 and fgclearcookies disrupted user sessions by deleting cookies, forcing victims to re-enter sensitive credentials. Plugin 5 intercepted data from email and FTP clients by hooking API functions. Similarly, Plugin 7 introduced keylogging capabilities, injecting shellcode into explorer.exe or other processes to capture user inputs by hooking critical system APIs.

#5 SmokeLoader's modular framework allowed attackers to customize its behavior through plugins, replacing traditional monolithic payloads. This flexibility not only enhanced its effectiveness but also posed significant challenges for defenders attempting to detect and neutralize it. As cybercriminals continue to refine their tactics, the need for vigilant monitoring and adaptive defenses is essential.

Recommendations

Patch and Update Systems Regularly: Apply the latest security patches to Microsoft Office and other critical software to protect against vulnerabilities like CVE-2017-0199 and CVE-2017-11882. Maintain a robust patch management process to ensure all systems are up-to-date.

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Monitor for Malicious Activity: Use endpoint detection and response (EDR) tools to identify and block suspicious scripts such as malicious VBScript and PowerShell commands. Deploy network monitoring solutions to detect unusual HTTP PUT requests or connections to command-and-control (C2) servers.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0011 Command and Control
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1566 Phishing	T1566.001 Spearphishing Attachment
T1059 Command and Scripting Interpreter	T1059.005 Visual Basic	T1059.001 PowerShell	T1027 Obfuscated Files or Information
T1001 Data Obfuscation	T1001.002 Steganography	T1132 Data Encoding	T1132.001 Standard Encoding
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1552 Unsecured Credentials	T1552.001 Credentials In Files
T1539 Steal Web Session Cookie	T1190 Exploit Public-Facing Application	T1057 Process Discovery	T1106 Native API

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	198[.]23[.]188[.]147, 77[.]232[.]41[.]29, 91[.]183[.]104[.]24, 185[.]228[.]234[.]237

TYPE	VALUE
SHA256	3e523ed80dbb592b1ff8c3345c3cd231ddd5a06e1af4c7b7d1f7f81249d0c4a3, ad657479d9f6322daba65638523d65631ff83ba5a717261acb5a53fd48e52209, 8dc06fdc2897d7c3438105ea0a39d2074774f80e051007fe7799b8195580ad2f, fbe226dd0130c3c0c4db9d125cd25eca3c8e310dae8127d15c8be18041d41cd6, 392d201120936c1f0e77bdb4b490f2825c1e6f584f18055c742b36250f89566b, e29c269a4c3ee4bbd673bfe0d24ca7d131d9221607e26a60989e81d8ffc17095, 00874ab2a91433dfbfdc9ee6ade6173f3280737fc81505504ace11273f640610, 1a1c8cdac1c3cbae5f1140e850ee06b414259876dab97152669f7c0f93469b13, 5dc92a6ed1ef2a5d9cf2a112532ad2c9fd70bff727e4cb60cd5d9c4966f2f77f, a334ba0d8ac0676d09e41aa273589ee27338c44a09109a4d5defa45f1d9bd82b, 35e55053bed6b3c1027a3e7c140e67303e01e8fcbf42abac27b8e9df2a090ee3, 858d26e697bc60b642e5d92922b625f58532fc06f028962d8add5fa497981f33, 7f9909677c290b98541be176251eca34b9f3d36555669a2639130adb97ca6958, f4b16c3f8bff445fdcd9d7edb5883d20d7663c3744e137439fa961736d0a9471, fb6ef14ac4cebf87f937f15553575f0f62ac62df917b490f602025a0985addd1, 9dea895b5b1c03caa2b838b8def4e082392851325794c3bd2eb5ca7372d8e09c, cfe7f6c1c0560bd56cd2df856d459b7fe7fd63b2f635c35151f61d4d04ce4162, a4ec792538455fb56f0b89ae10ddd0b2504afba092ba5cfa2083cf61b5fac0ef, cb92d320fc9bc674e8d37ceeebf0363f8e96dd67ef4ef543b3348f96ef567e5f, eb8381b156aad734ef3a0328b4985ed1edeca1c8d79d66e094598f8c6992ac71, e3e7a3d0ba55b8dbbe3633b1dad0a3bbf4eada72dd8df3f7b1bc76a692862f23, ea3b07a2356a7bfb92144f621ba551677a138c31d684072d69a4d37c1a378bb3,

TYPE	VALUE
SHA256	7ab20d40431b990a9a44e96dc53519f0af72eaf56c4b20f8995f95a48039bf67, bdb897e6a8bfc21302ae1ac254b1b2e779684fe75b2b824cb24c80c775898940, F7544f07b4468e38e36607b5ac5b3835eac1487e7d16dd52ca882b3d021c19b6

Patch Links

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0199

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

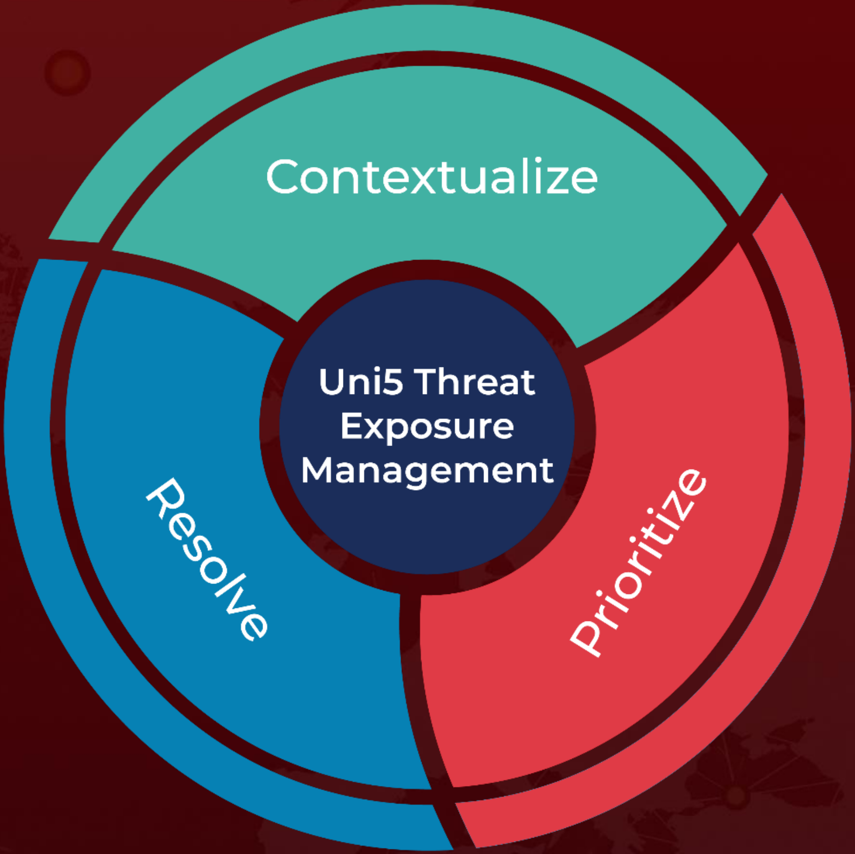
References

https://www.fortinet.com/blog/threat-research/sophisticated-attack-targets-taiwan-with-smokeloader

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 3, 2024 • 11:40 PM

More at www.hivepro.com