Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

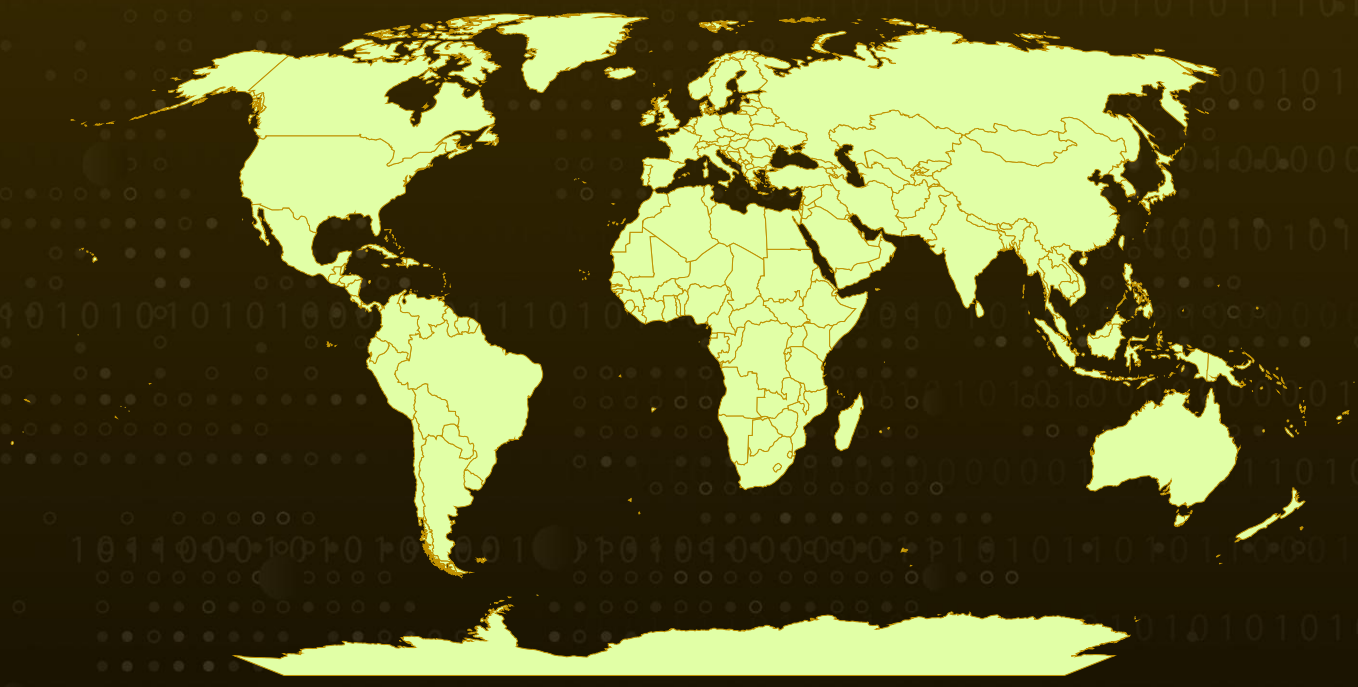
Lumma Stealer Strikes Again with Fake CAPTCHAs and Advanced Evasion

Date of Publication	Admiralty Code	TA Number
January 27, 2025	A1	TA2025021

Summary

Attack Discovered: January 2025
Targeted Countries: Worldwide
Affected Industries: Healthcare, Banking, Marketing, Telecom Industry
Affected Platform: Windows
Malware: Lumma Stealer
Attack: A new Lumma Stealer campaign has emerged, using fake CAPTCHAs, malvertising, and sophisticated payloads to target Windows users worldwide. The attackers employ deceptive tactics, including an infection chain that tricks victims into executing clipboard commands via the Windows Run prompt, effectively bypassing conventional defenses. Notably, one payload leverages code from an open-source tool to bypass the Windows Antimalware Scan Interface (AMSI), disabling malware protections and enabling the attackers to operate undetected within compromised systems.

Attack Regions



Attack Details

#1 A global malware campaign has surfaced, leveraging Lumma Stealer, a malware-as-a-service (MaaS) platform active since 2022 with victims targeted in Argentina, Colombia, the United States, the Philippines, and other countries around the world. This campaign specifically targets industries such as healthcare, banking, and marketing, employing a mix of deceptive techniques to evade detection. Attackers rely on advanced tactics like PowerShell one-liners and open-source code snippets to bypass security measures. To complicate matters further, they introduce new payloads and malvertising websites, making it increasingly challenging for defenders to detect and counter the attacks.

#2 Since August 2024, fake CAPTCHA pages have become a central element of these attacks. These pages use social engineering to trick victims into executing malicious commands outside their web browsers. Victims are prompted to open the Windows Run dialog, paste clipboard content, and press ENTER.

#3 Behind the scenes, the CAPTCHA's JavaScript stealthily inserts commands into the clipboard. These commands utilize Windows' trusted mshta.exe tool to download and execute a remote HTA file. This method, known as Living Off the Land Binary (LOLBIN), exploits legitimate system binaries to bypass browser-based defenses and execute malicious actions outside the browser's security context.

#4 The payloads delivered through this campaign often disguise their intent using deceptive file extensions but hide malicious JavaScript snippets. These scripts initiate additional attack stages, including the use of PowerShell commands to decode base64-encoded data and download further payloads. Advanced payloads employ obfuscation techniques like mathematical operations, XOR encoding, and base64 decoding to hide malicious behavior.

#5 In one instance, a script disables the Windows Antimalware Scan Interface (AMSI) by removing the "AmsiScanBuffer" string from the clr.dll module. Using publicly available AMSI bypass tools, the script decodes a base64-encoded executable and loads it via reflection to deploy Lumma Stealer. Some samples also use obfuscation tools like Babel to further hinder analysis. The Lumma Stealer campaign highlights the evolving tactics of cybercriminals, particularly in leveraging user interactions to facilitate malware execution.

Recommendations

- **Enhanced Email Security:** Enhance email security by Implementing advanced spam filters, anti-phishing solutions, and email authentication protocols. Educate employees about identifying and reporting suspicious emails to prevent successful phishing attempts.
- **Restrict Execution of Untrusted Scripts:** Set up your systems to block any unsigned or untrusted scripts from running. Enforce policies that only allow signed scripts to execute, reducing the chances of malicious PowerShell commands or JavaScript snippets being used to compromise your network.
- **Monitor Network Activity:** Regularly track network traffic for unusual patterns or connections to known malicious domains or IP addresses.
- **Strengthen Awareness Against Social Engineering**: Provide ongoing training to help users recognize fake CAPTCHA pages and other phishing techniques. Educating employees on these tactics empowers them to avoid unknowingly executing malicious commands and reduces the risk of successful attacks.
- **Regularly Update and Patch:** Ensure operating systems, browsers, and software are kept up to date to address known vulnerabilities and reduce the risk of malware exploitation.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0011 Command and Control	T1583 Acquire Infrastructure	T1583.008 Malvertising	T1566 Phishing
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.003 Windows Command Shell	T1059.007 JavaScript
T1204 User Execution	T1218 System Binary Proxy Execution	T1218.005 Mshta	T1027 Obfuscated Files or Information
T1140 Deobfuscate/Decode Files or Information	T1132 Data Encoding	T1132.001 Standard Encoding	T1070 Indicator Removal

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	gustavu[.]shop/path0forwarding-stepv2[.]html, sos-de-muc-1[.]exo[.]io/after/clear/then/continue-ri-1[.]html, retrosome[.]shop/proceed-to-next-page-riii2[.]html, jazmina[.]shop/pass-this-step-to-go-next-riii2[.]html, norpor[.]shop/surfing-toward-next-pagev2[.]html, bestinthemarket[.]com/courses[.]html, edidos[.]shop/pass-this-step-to-go-further-riii1[.]html, joopshoop[.]shop/speedy-check-waitv111[.]html, sos-at-vie-2[.]exo[.]io/simulation/continue/ruweb/keep-browsing-to-continue-web-55[.]html, towercrash[.]com/play[.]html, sos-at-vie-1[.]exo[.]io/sotbuck/next/step/to/have-to-pass-this-step-web5[.]html, celebrationshub[.]shop/continue-to-browse[.]html, royaltyfree[.]pics/have-to-pass-this-step[.]html, cubesmatch[.]com/play[.]html, sos-ch-dk-2[.]exo[.]io/onr/play[.]html, sos-bg-sof-1[.]exo[.]io/kierendisk/strangled/path/final/keep-browsing-to-continue-web-s5[.]html, sos-ch-gva-2[.]exo[.]io/instance-of/verification/pass-to-continue-s7[.]html, kizmond[.]shop/myforwarding-path-gotov01[.]html, speedmastere[.]com/play[.]html, rezomof[.]shop/pass-this-step-to-continue-s7[.]html, luxeorbit[.]shop/you-have-to-pass-this-step-2[.]html, bazaar[.]abuse[.]ch/download/34f8309b94241f6e5b24/, dokedok[.]shop/pass-this-step-to-go-next-riii1n[.]html, sharethewebs[.]cfd/must-clear-this-check[.]html, diamondrushed[.]com/play[.]html, googlsearchings[.]cfd/you-have-to-pass-this-step-2[.]html, sharethewebs[.]click/you-have-to-pass-this-step-2[.]html, sos-ch-dk-2[.]exo[.]io/last-instance/to-verify/pass-this-step-to-continue-s6[.]html, milta[.]shop/next-page-proceeding-waitv1[.]html, iconcart[.]shop/must-clear-this-check-rii[.]html, googlsearchings[.]online/you-have-to-pass-this-step-2[.]html, crystaltreasures[.]shop/get-going-forward[.]html, sharethewebs[.]click/must-clear-this-check[.]html, sos-ch-dk-2[.]exo[.]io/last/page/complete-and/must-complete-to-continue-re6[.]html,

TYPE	VALUE
URLs	sos-de-muc-1[.]exo[.]io/asist/last/check/keep-browsing-to-continue-web-55[.]html, ghazaano[.]shop/Need-to-Pass-this-Stepv2[.]html, oliveroh[.]shop/pass-this-step-to-continue-s7[.]html, espiano[.]shop/proceed-to-next-page-riii1[.]html, sos-ch-gva-2[.]exo[.]io/instance-of/verification/path-to-next-7[.]html
MD5	907992bfa7e5bfd56e59e86e83677e70, dbb81b8d6585511af65cc84fb4536d3c, faaada2346f084e12353da454a3a33c2, 69c5123c9240df4a25141bb828405883, 0ea0350dfb3d146e5939271268e4e52a, f7aee95cda3475aef88f06193c7622a5, a5d2c4a9bca49328d64d48ee3b331811, e9b876903c100f8789071de91d405da9, d5a675995c0e20c53991595252306b18, 30f43a6fdb205be22445308a6f89096a, db4c6ccf5015db1ba253692016904835, 3686cad7078128482ac6bd5c46a953ac, dd74b4fb6bc7807df71fd589fb25a2cc, 7e929ee11f9d2dabd90ea6c21568d689, bf407bfaa4f8fbf7d6cc655939cceee0, 2fd36c3bf514f10855b76785af31d4ef, ea27fc140d8b655d900bd8ee1fb5fdd5, 67cadbdd12fa42dccf7bd3b0a2700c75, b7204abea15496e68f490eb9da3cca54, b377795978c82087db0a0bcd69cdbfff, d5d0aa662174e3b148642574f99eb357, 83c30841c22491cc465206e3e26a5571, a45f93ced67a7a21ca6ea08e4078e874, 4755a5cff067cb450b2b871bcd2e3ece, e57f7e8ce851cfd206ca999d8525d6e4, ca6775302bf389a78b3a732e58629cd5, 3272a4855cb310b676bdb0c4ff221417, 5b567f16133db6d4b1e58aacc5d58800, 2ae547b5b79c6c3cc7463b946aa38ee9, 9e55e377eb6707746cde46344e8f4a46, 08da9a5f3cf4f3e448fb45d5cd74297d, 380565ca4713bf766a6b7136f9d46382, 3734e365ab10e73a85320916ba49c3ee, 1f07e1668f18440abc05d9b2a58a7640, e53474ed38d9da707eb7783b5478a2ec, c2430d166b53fb388cfc92785eeb18d7, a94ecef988b7c3a69b91c24cd9632156, 1d7d6cf1329fcc28d82778f4406d9245, edc1a96e3ac9d13654e1dcb4d7f6a37c, 29178a065d290c55fdc12cfe90b0fae6,

TYPE	VALUE
MD5	802ceab005721dffaaae01c846766e0e, b06f858cbfe8ef08c58353a4433adf54, ff8db603e6d75b0e9d9c0eec0b1c7280, b30d6b4cbf6f5c137f8b9800a02584cb, 393c64810ddb7437fa040194ecb972ca, 93b8729bbb1d413bfd44436d0c544116, a181e4f186f156cbb238984f8a5bf4e6, a151c8fd5326c1670c0ea3245d01f9a8, 00317b9ff31f7aa93f7c7891e0202331, 82e5e8ec8e4e04f4d5808077f38752ba, 14d8486f3f63875ef93cfd240c5dc10b, 0ba2afe43cc4deed266354b1c2cfb5a7
SHA256	179e242265226557187b41ff81b7d4eebbe0d5fe5ff4d6a9cfffe32c83934a46, 007969cf64583d251ed63eda2c365f6cbfd768f37d05e699415d166021b3e294, d8ef30084c328836d45892cd65a7a0fc91f8deed5ac859b6492fd6297b1e5d34, 676550965b9ca97782aab492e2ab86d85c7350aaeeacae99493b14bbc81bd146, b94ddefd39d32a753564e6871d11750fa56b993cad3ea40955139e584ad3bef8, 86d50a7fc8d245876b791efe85eb7f64cd48b9e9648b4bf8bee22dbae66fe3aa, 02a0bba5b3cc6a650d611c2f6d6a8ce6a696c230521f0de43824a19ced716acd

References

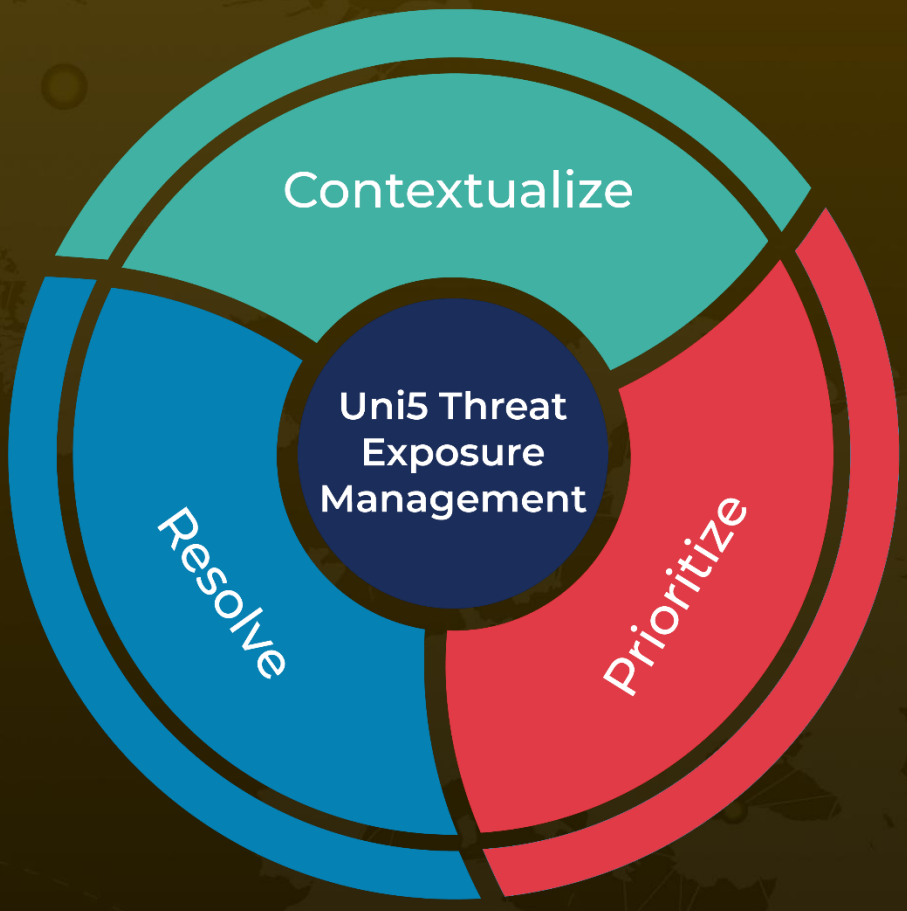
https://www.netskope.com/blog/lumma-stealer-fake-captchas-new-techniques-to-evade-detection

https://hivepro.com/threat-advisory/microsoft-smartscreen-flaw-used-for-covert-stealer-deliveries/

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

January 27, 2025 • 6:30 AM

More at www.hivepro.com