Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

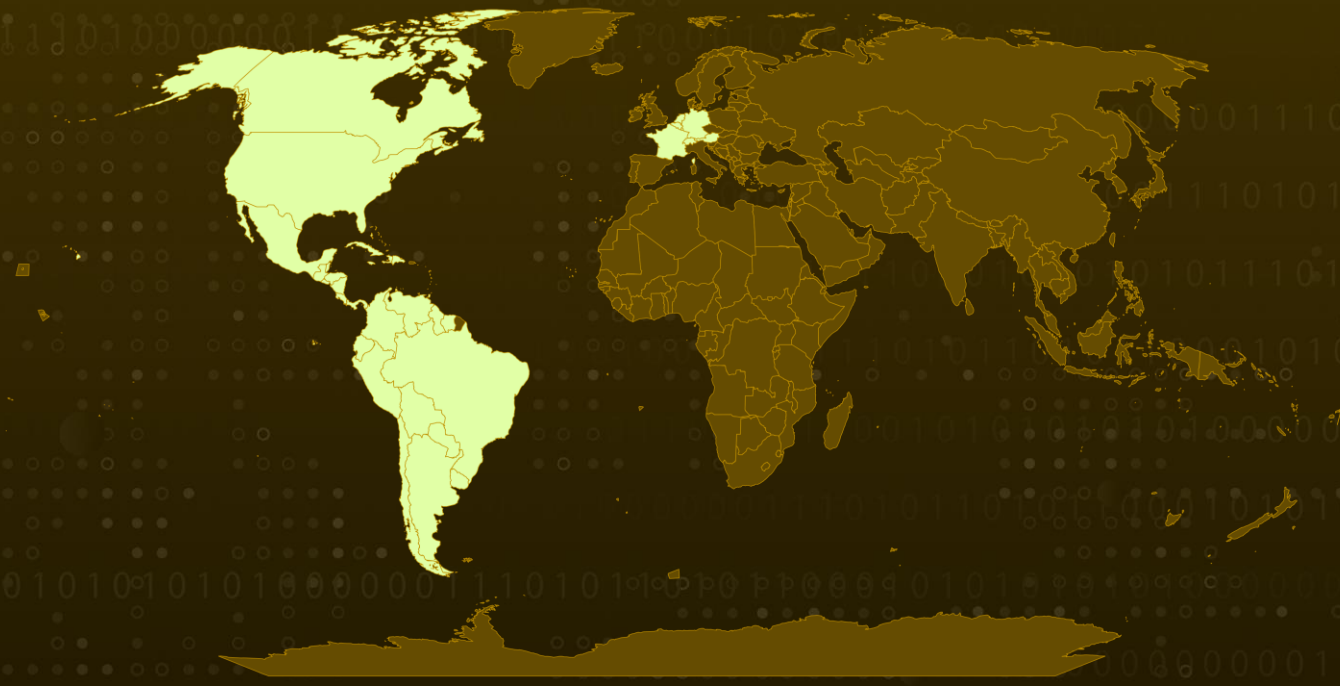
Mispadu Leverages CVE-2023-36025 Vulnerability in Latest Attack

Date of Publication	Admiralty Code	TA Number
February 7, 2024	A1	TA2024047

Summary

First appeared: November 2023
Attack Region: The Americas and parts of Western Europe
Targeted Industry: Finance, Banking, and Cryptocurrency
Malware: Mispadu infostealer
Affected Platform : Windows
Attack: A new variant of the Mispadu infostealer, a malware known for targeting Spanish and Portuguese speakers, specifically targets Mexican regions and leverages the CVE-2023-36025 vulnerability to gain access. It extends its data theft reach beyond previous versions, capturing browser history, cookies, and even cryptocurrency wallets.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-36025	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	Microsoft Windows	✓	✓	✓

Attack Details

#1 The Mispadu Stealer, an infostealer that emerged in 2019, was recently discovered during an investigation into the SmartScreen CVE-2023-36025 vulnerability. This investigation uncovered a fresh iteration of the Mispadu Stealer, which specifically targets certain regions, notably Mexico.

#2 The malware employs sophisticated techniques to evade detection, including bypassing SmartScreen warnings by utilizing crafted .url files pointing to malicious binaries on a threat actor's network share. This variant selectively targets victims in the Americas and parts of Western Europe, particularly focusing on Spanish and Portuguese-speaking users.

#3 The malware's primary objective is to extract data from web browsers, particularly targeting URLs associated with financial institutions and cryptocurrency organizations, especially in Mexico. The evolving nature of this new variant of Mispadu Stealer, despite similarities with previous campaigns, emphasizes the importance of maintaining a comprehensive cybersecurity strategy.

Recommendations

Patch Management: Ensure that all systems and software are regularly updated with the latest patches and security updates, including fixes for known vulnerabilities such as SmartScreen CVE-2023-36025. Regularly check for updates from trusted sources and apply them promptly.

Email Security: Deploy robust email filtering solutions to detect and block malicious attachments and phishing attempts. Implement email authentication mechanisms (SPF, DKIM, DMARC) to prevent email spoofing and phishing.

Endpoint Protection: Utilize reputable antivirus and anti-malware solutions for early detection and removal of Mispadu infostealer and similar threats. Keep endpoint protection software up-to-date to recognize and mitigate the latest malware variants.

User Privileges and Access Controls: Follow the principle of least privilege, granting users the minimum necessary access. Implement strong authentication mechanisms and enforce complex password policies.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0007** Discovery	**TA0005** Defense Evasion
TA0009 Collection	**TA0011** Command and Control	**T1102** Web Service	**T1140** Deobfuscate/Decode Files or Information
T1059 Command and Scripting Interpreter	**T1204** User Execution	**T1027** Obfuscated Files or Information	**T1204.002** Malicious File
T1204.001 Malicious Link	**T1189** Drive-by Compromise	**T1566.002** Spearphishing Link	**T1566** Phishing
T1190 Exploit Public-Facing Application	**T1082** System Information Discovery	**T1218.011** Rundll32	**T1218** System Binary Proxy Execution

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	2112360f64fc1673da60f8a75d4935b7, 6ce43b5b2fe55e4120f2a07a704ba244, 723df0296951abd2aeed01361cec6b0d, Eae83f4faad9356919741fac5a1153f1,
SHA1	319feee9bd7908c77a11672c1e06b83b7201cfd4, 47285d8372ca733ead51821a91c53b5e4c53c21b, a9f6520a8de82c3d6e06c41317e126947a0fb553, Ba6d10e36f41c4ebc85f6beb95afd2b7c92406ad, b276d76942d6cfb649120eddc57493f482c57f04,
SHA256	018beb515d323dee4f04ad9663863324859f4eb896576dbef1df950568084030, 0332d65ee6d896d1b326748e0108b1ac1ad97e94796dd17c7e15fa10317445a9,

TYPE	VALUE
SHA256	03bdae4d40d3eb2db3c12d27b76ee170c4813f616fec5257cf25a068c46ba15f, 135c9ef3baaef856dd9ca7801bfb690a3662646ab97568e916a1af06d382b81f, 1b7dc569508387401f1c5d40eb448dc20d6fb794e97ae3d1da43b571ed0486a0, 30b4ab9707347c6bdd9035d1562cab31c78a27f5ad410871cadffeb208cd85e8, 3e165f375f498d802ce7f47739ae9d93236f83811335da55aef1dc1c17694f53, 44c505974154050ec0c671eb2f1d27f72886243bfafff8c3523b0ce1d64f944a, 46d20fa82c936c5784f86106838697ab79a1f6dc243ae6721b42f0da467eaf52, 4a774438d15381d9ab308dd73c2917aee83897d654c39db24f4dd6f173564914, 4b276d43308450619fec6befdf92c5171298e3651ed6f06a5a637f8a5afc407f, 4c21caa1fc4c01fa51d918be8ab40077e79b5b8dbaea098328ff953fc7aca8c2, 4e209b1dd2d4eaa3b041dddbe7f1bd0c6b07145c0102999060d7ceeb64978e90, 748a57a4d4e806daa6c5e54af96f9e7839bc2260e5f0258e5edf617a92045085, 8e1d354dccc3c689899dc4e75fdbdd0ab076ac457de7fb83645fb735a46ad4ea, 974fe99972905800c1dd1a3527de58c291ed1f8f1c654f2f302d6b3b70af2b10, ac027e988dad213707537bdc0172509b9135115337c5744816b079390d5a3e82, b70ad99286733a4eb2ebc615fbfdbc9b278aaa15ad23d661696ae54eb186a5a4, bbaba0482f486b0d7b7738af8bc4731dbb80faef7f8b3888d9859726dbd53957, bc25f7836c273763827e1680856ec6d53bd73bbc4a03e9f743eddfc53cf68789, cf546a4c5c7fdd3935ed7d93f5482057e3c8ff8723c3a73caba1fc5e3a5c96b4, d4fed9ca90249707099926e336c0ec5abc0be8fbeb0e1889f7259e0e7312b9a0, d752b7472110cbf7f4513b64658c751148304f287b13df26890642d64b75c264,

TYPE	VALUE
SHA256	dd4018e2cff36fc896497d4539397e8334aa9a5910e73b45bde4f7206aa5ebe3, e136717630164116c2b68de31a439231dc468ddcbee9f74cca511df1036a22ea, e8deebe849f80654b53b73d41a379919a86c4c356715d34729335e79089127c7, fb3995289bac897e881141e281c18c606a772a53356cc81caf38e5c6296641d4,
URLs	hxxp://24[.]199[.]98[.]128/expediente38/8869881268/8594605066[.]exe, hxxp://24[.]199[.]98[.]128/impresion73/5464893028/8024251449[.]exe, hxxp://24[.]199[.]98[.]128/verificacion58/6504926283/3072491614[.]exe, hxxp://trilivok[.]com/4g3031ar0/cb6y1dh/it[.]php, hxxp://plinqok[.]com/3dzy14ebg/buhumo0/it[.]php, hxxp://trilivok[.]com/4g3031ar0/cb6y1dh/it[.]php, hxxp://malpedia[.]caad[.]fkie[.]fraunhofer[.]de/details/win[.]mispad
Hostname	malpedia[.]caad[.]fkie[.]fraunhofer[.]de, rfc[.]online[.]melendez[.]1981[.]d9f[.]zip, www1[.]secure[.]hsbcnet[.]com, bancadigital[.]monex[.]com[.]mx, empresas[.]bbvanet[.]com[.]mx, nixe[.]ixe[.]com[.]mx
Domains	hsbc[.]com[.]mx, joined[.]actor, moscovatech[.]com, plinqok[.]com, trilivok[.]com, xalticainvest[.]com
IPv4	24[.]199[.]98[.]128

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025

References

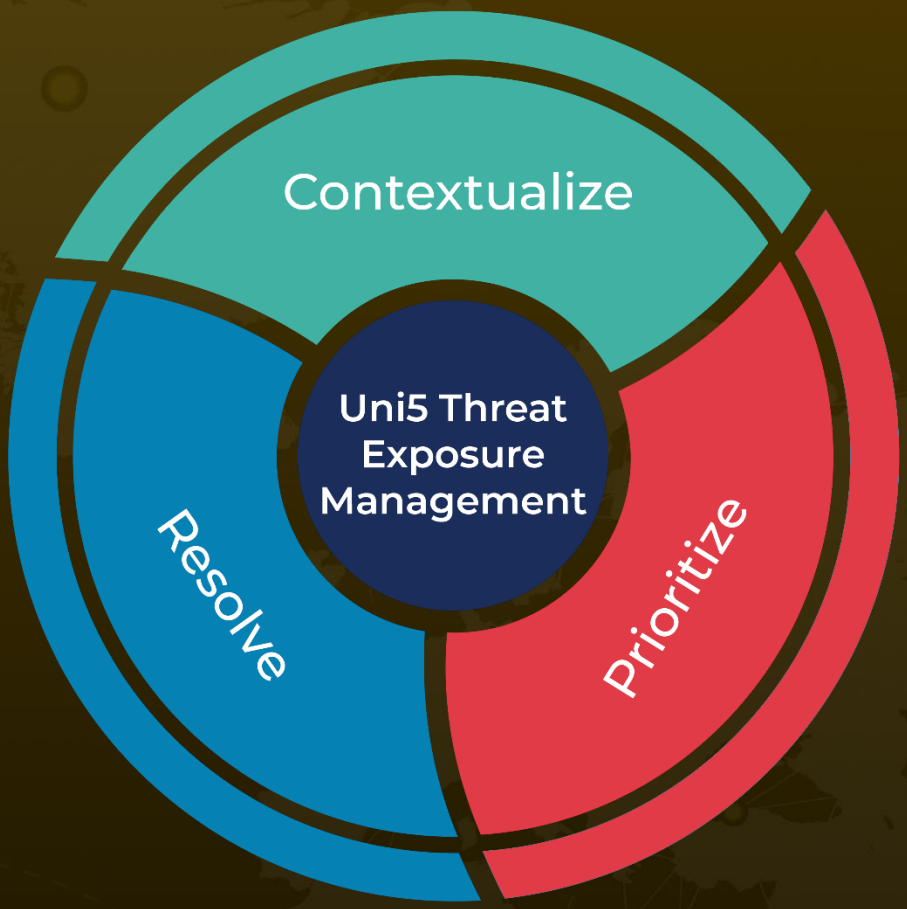
https://unit42.paloaltonetworks.com/mispadu-infostealer-variant/

https://www.hivepro.com/threat-advisory/mispadu-targets-latin-america-with-malspamming/

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

February 7, 2024 • 11:30 PM

More at www.hivepro.com