Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

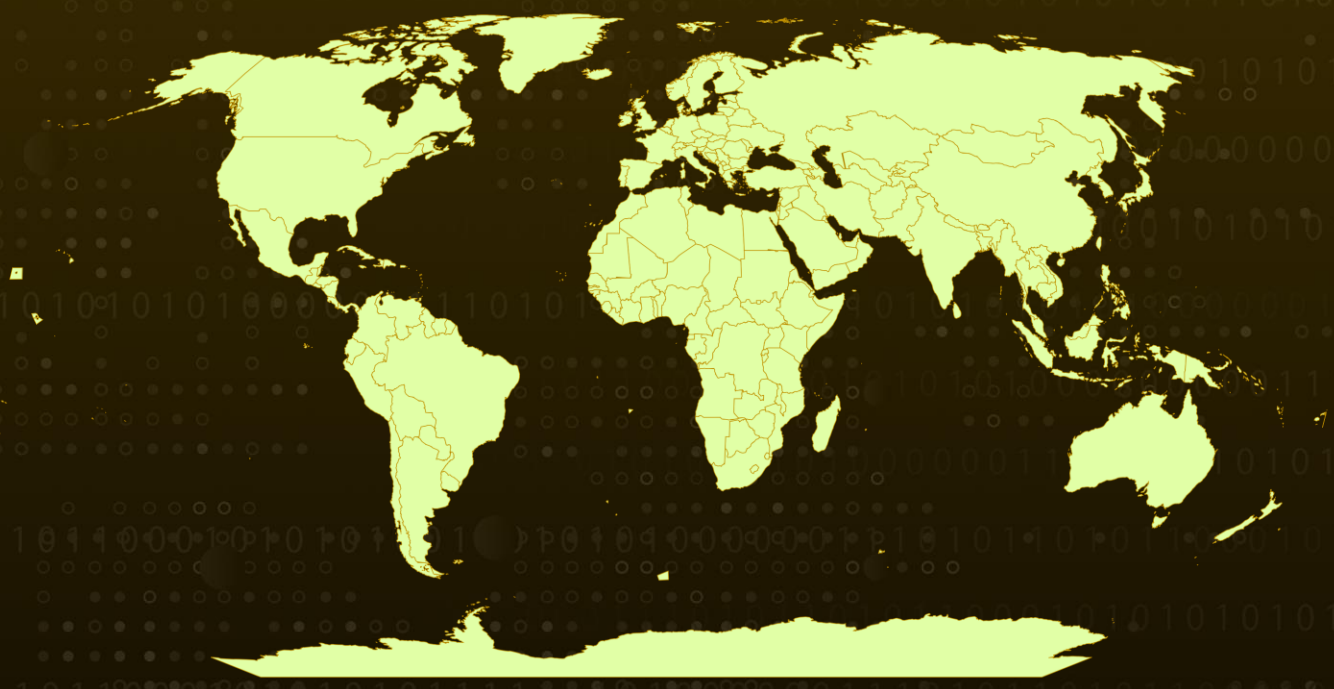
Surging JavaScript Threats Steal Your Secrets

Date of Publication	Admiralty Code	TA Number
January 04, 2024	A1	TA2024005

Summary

Attack Discovered: December 2023
Attack Region: Worldwide
Attack: The threat actors utilize malicious JavaScript samples, taking advantage of popular survey sites, low-quality hosting, and web chat APIs to steal sensitive information. They create chatbots registered under notable figures, like an Australian footballer, in specific campaigns. Additionally, these actors employ various tactics, including injecting web skimmers into compromised sites and setting up traditional phishing sites, to execute their malware campaigns.

Attack Regions



Attack Details

#1 Threat actors are employing malicious JavaScript to steal sensitive information, employing various tactics such as exploiting popular survey sites, leveraging low-quality hosting, and utilizing web chat APIs. Certain campaigns involve the creation of chatbots linked to well-known personalities, deployment of web skimmers and utilizing traditional approach of phishing sites. To avoid detection, they incorporate multi-level obfuscation, abuse cloud APIs, unusual DOM interactions, and selective payload detonation.

#2 Attackers were found to be leveraging legitimate cloud APIs to extract sensitive data, including PINs and customer numbers. They exploit Chatbot APIs, survey form APIs, rentable domains, and dynamic DNS domains. The usage of cloud APIs enable them to blend exfiltrated data with legitimate one, effectively eluding detection.

#3 These JavaScript based malwares employs unusual DOM objects for data exfiltration; for instance a hidden image object loads remote image, providing exfiltrated data as part of request parameter. Notably, they are shifting away from dynamic code generation as many detectors have specialized monitoring mechanisms for dynamically generated codes. They also employ a selective conditional detonation which increases their effectiveness and further helps them in evading during dynamic analysis.

#4 The surge in JavaScript-based malwares underscores a growing trend where these malicious entities are actively evolving and adapting, this adaptability serves as a significant challenge. Security practitioners are advised to monitor exfiltration endpoints, while service providers should proactively remove malicious entities to enhance overall cybersecurity.

Recommendations

Remain vigilant: 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.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place.

Monitor Network Traffic: Utilize network monitoring tools to scrutinize incoming and outgoing traffic, identifying irregular communication patterns. This can help detect and thwart attackers attempting to establish connections with their command-and-control servers.

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.

Configure privacy settings: Adjust your browser's privacy settings to control the amount of information it collects and shares. This includes blocking third-party cookies, enabling "Do Not Track," and using the browser's private or incognito mode when needed.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0010 Exfiltration
T1583 Acquire Infrastructure	T1566 Phishing	T1027 Obfuscated Files or Information	T1589 Gather Victim Identity Information
T1059 Command and Scripting Interpreter	T1059.007 JavaScript	T1217 Browser Information Discovery	T1204 User Execution
T1480 Execution Guardrails	T1036 Masquerading	T1189 Drive-by Compromise	T1537 Transfer Data to Cloud Account
T1567 Exfiltration Over Web Service	T1539 Steal Web Session Cookie		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	bf3ab10a5d37fee855a9336669839ce6ad3862ad32f97207d4e959faaba0a3ed, 13429eebb74575523b242e16b51eacf287a351c6de04557ec3cc343812aae0cb, db346adb1417340e159c45c5e4fdaea039c0edbca6e62ad46aa9aec1cf1273a1, da416dd6d35e2b779d164f06d4798ca2d9a3d3867e7708b11bf6a863a5e7ffc2, f82ef9a948b4eaf9b7d8cda13c5fa8170c20b72fde564f7d3a0f271644c73b92, acf325dad908534bd97f6df0926f30fc7938a1ac6af1cec00aa45bcf63699e24

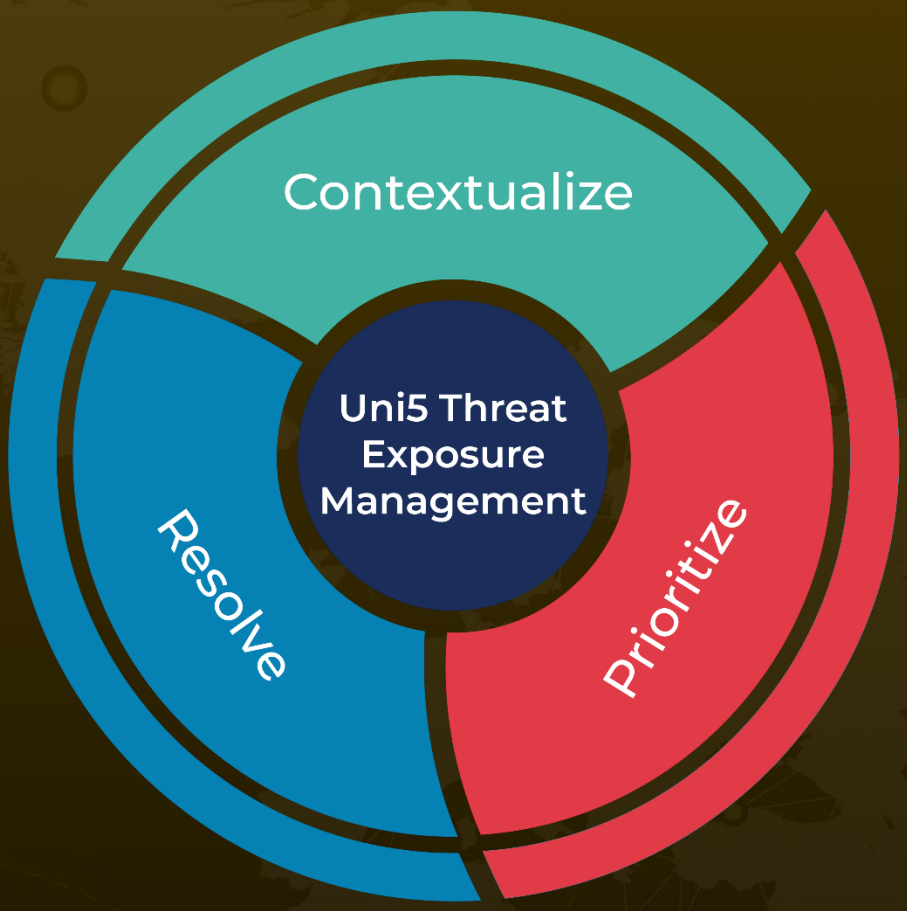
References

https://unit42.paloaltonetworks.com/malicious-javascript-steals-sensitive-data/

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 04, 2023 . 6:10 AM

More at www.hivepro.com