Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

MediaArena: A Deceptive Browser Hijacker Exploiting User Data and Security Threats

Date of Publication	Admiralty Code	TA Number
June 06, 2023	A1	TA2023253

Summary

First appeared: June, 2023
Attack Region: Worldwide
Affected Platform: Microsoft Edge, Google Chrome, and other browsers
Malware: MediaArena
Attack: MediaArena is a deceptive software that hijacks browsers, redirects searches, and collects user data for malicious activities, emphasizing the importance of removal and caution.

Attack Regions

Attack Details

#1 A new type of unwanted software called "MediaArena" has been detected, posing a security threat to users. It disguises itself as a useful tool but actually modifies browser settings to steal search queries. The software is distributed through malvertising campaigns, where users are tricked into clicking on ads and installing the tool.

#2 Once installed, all search queries are redirected to a third-party website, allowing the collection and sale of user data. This enables bad actors to manipulate search results, gather information, and potentially deliver targeted drive-by downloads. The malware primarily affects users of Microsoft Edge as their main browser. The prevalence of this software is widespread, affecting over 600 hosts across various environments.

#3 The widespread infection of the software is attributed to an ongoing malvertising campaign, where users are lured into downloading the malware through advertisements related to their current website content. The removal process involves uninstalling the program and removing the custom search engine from the browser settings, with specific steps depending on the browser used.

Recommendations

- **Keep software updated:** Regularly update your operating system, web browsers, and other software to ensure you have the latest security patches. This helps protect against known vulnerabilities that malware like MediaArena may exploit.
- **Use reliable security software:** Install reputable antivirus and anti-malware software on your devices. Keep it updated and perform regular scans to detect and remove potential threats, including MediaArena.
- **Exercise caution when downloading and installing software:** Be cautious of downloading software from untrusted sources. Stick to official app stores and verified websites. Read user reviews, check app permissions, and ensure the software comes from reputable developers before installation.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0006 Credential Access	TA0001 Initial Access
TA0005 Defense Evasion	TA0009 Collection	TA0011 Command and Control	T1007 System Service Discovery
T1036 Masquerading	T1204 User Execution	T1555.003 Credentials from Web Browsers	T1555 Credentials from Password Stores
T1176 Browser Extensions	T1189 Drive-by Compromise	T1115 Clipboard Data	T1055 Process Injection
T1059 Command and Scripting Interpreter			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	33c02d70abb2f1f12a79cfd780d875a94e7fe877 4041a7410598c46d7657ceb94b0af4ebbc7a9c0a
SHA256	5e1cec9e9011fc96638620a2ca8e08eeaeaea8a28c47fe619082abcc6794aebc e248b01e3ccde76b4d8e8077d4fcb4d0b70e5200bf4e738b45a0bd28fbc2cae6 cd2b9cf8489cca6b357bc2706a68f5a12aeb696380ce7371803d68f08e337630 e9fad9727b8a66e6b593d8b416f1c60b692ffc91b72e14bb30c40a1ce9b6a260 6d37baeb841bcf6c4935a54f29df049d405df48345014cc12852b814d279d86e
Hostname	Goto[.]searchpoweronline[.]com

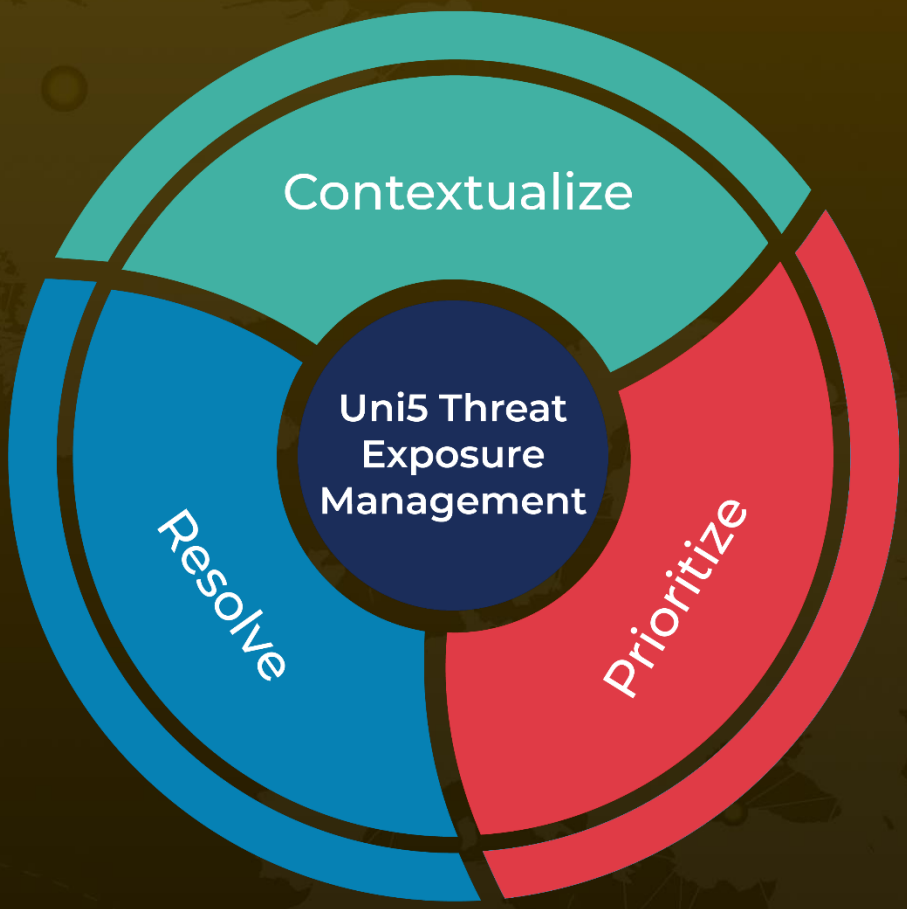
References

https://northwave-cybersecurity.com/threat-intel-research/analysis-of-new-active-malware-mediaarena-pua

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

June 06, 2023 • 7:30 AM

© 2023 All Rights are Reserved by HivePro

More at www.hivepro.com