Jun 10 2023

NETMANAGEIT

Intelligence Report

Analysis of new active malware: MediaArena - PUA

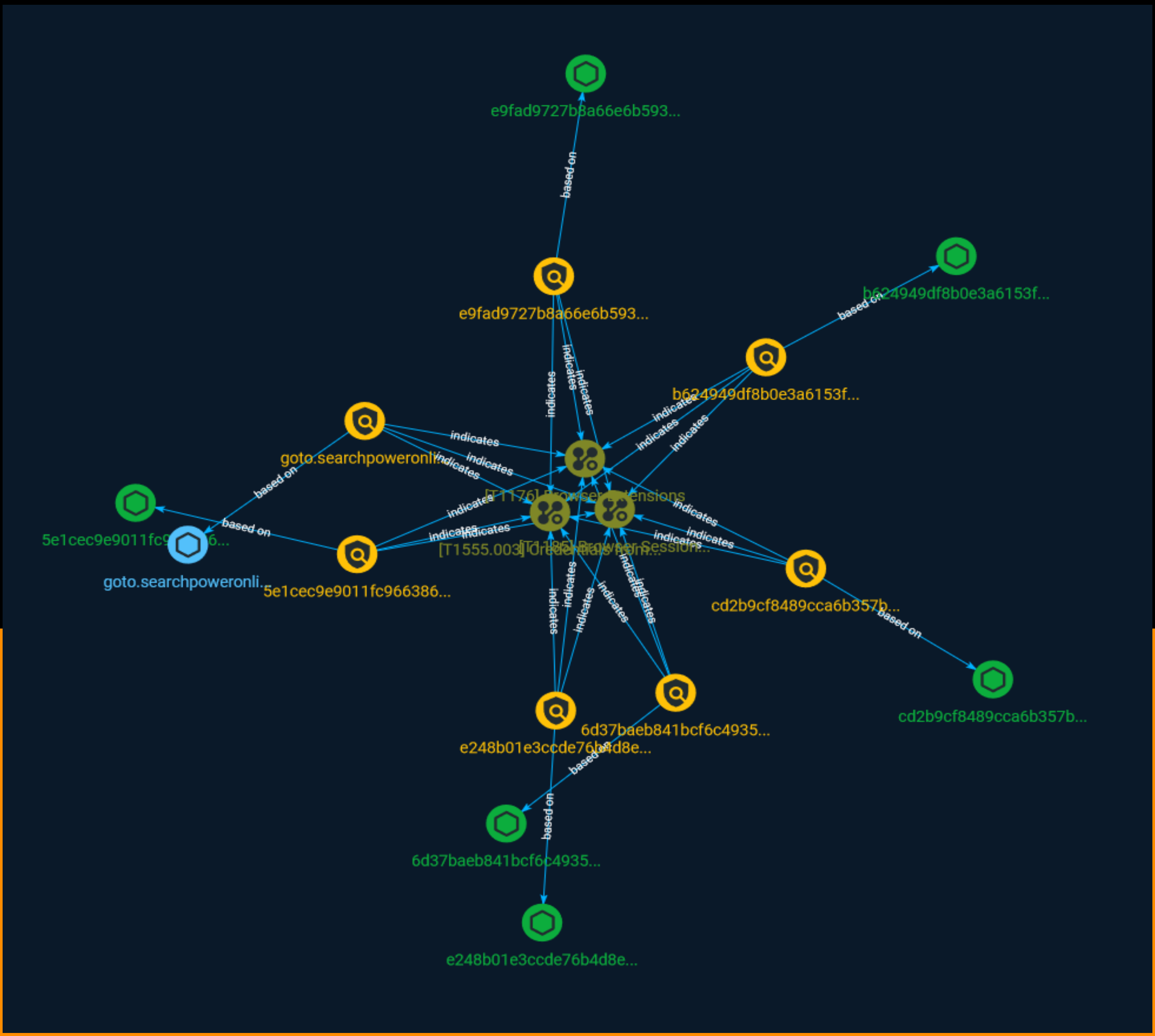

Table of contents

Overview

Entities

Observables

External References

Overview

Description

MediaArena is a piece of software that masks itself as a useful tool but secretly reconfigures some browser settings to steal your search queries. It masks for instance a docx-to-pdf converter, a tool to convert video to animated GIF and so on. Distribution appears to occur via advertisements shown on webpages in an ongoing malvertising campaign. The victim is tricked to click the advert and may install this tool on their workstation. All search queries the victim enters are redirected to a third party where search results are served with ads, and the search queries are collected and sold. This allows bad actors to manipulate search, gather data on your company, inject drive-by downloads in a targeted way and do many other things.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Attack-Pattern

Name

Browser Session Hijacking

ID

T1185

Description

Adversaries may take advantage of security vulnerabilities and inherent functionality in browser software to change content, modify user-behaviors, and intercept information as part of various browser session hijacking techniques.(Citation: Wikipedia Man in the Browser) A specific example is when an adversary injects software into a browser that allows them to inherit cookies, HTTP sessions, and SSL client certificates of a user then use the browser as a way to pivot into an authenticated intranet.(Citation: Cobalt Strike Browser Pivot)(Citation: ICEBRG Chrome Extensions) Executing browser-based behaviors such as pivoting may require specific process permissions, such as `SeDebugPrivilege` and/or high-integrity/administrator rights. Another example involves pivoting browser traffic from the adversary's browser through the user's browser by setting up a proxy which will redirect web traffic. This does not alter the user's traffic in any way, and the proxy connection can be severed as soon as the browser is closed. The adversary assumes the security context of whichever browser process the proxy is injected into. Browsers typically create a new process for each tab that is opened and permissions and certificates are separated accordingly. With these permissions, an adversary could potentially browse to any resource on an intranet, such as [Sharepoint](https://attack.mitre.org/techniques/T1213/002) or webmail, that is accessible through the browser and which the browser has sufficient permissions. Browser pivoting may also bypass security provided by 2-factor authentication.(Citation: cobaltstrike manual)

Name
Credentials from Web Browsers
ID
T1555.003
Description
Adversaries may acquire credentials from web browsers by reading files specific to the target browser.(Citation: Talos Olympic Destroyer 2018) Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from web browsers. For example, on Windows systems, encrypted credentials may be obtained from Google Chrome by reading a database file, \`AppData\Local\Google\Chrome\User Data\Default\Login Data\` and executing a SQL query: \`SELECT action_url, username_value, password_value FROM logins;\`. The plaintext password can then be obtained by passing the encrypted credentials to the Windows API function \`CryptUnprotectData\`, which uses the victim's cached logon credentials as the decryption key.(Citation: Microsoft CryptUnprotectData April 2018) Adversaries have executed similar procedures for common web browsers such as FireFox, Safari, Edge, etc.(Citation: Proofpoint Vega Credential Stealer May 2018)(Citation: FireEye HawkEye Malware July 2017) Windows stores Internet Explorer and Microsoft Edge credentials in Credential Lockers managed by the [Windows Credential Manager](https://attack.mitre.org/techniques/T1555/004). Adversaries may also acquire credentials by searching web browser process memory for patterns that commonly match credentials.(Citation: GitHub Mimikittenz July 2016) After acquiring credentials from web browsers, adversaries may attempt to recycle the credentials across different systems and/or accounts in order to expand access. This can result in significantly furthering an adversary's objective in cases where credentials gained from web browsers overlap with privileged accounts (e.g. domain administrator).
Name
Browser Extensions
ID

T1176

Description

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions.(Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control.(Citation: Chrome Extension C2 Malware)

Indicator

Name

5e1cec9e9011fc96638620a2ca8e08eeaeaea8a28c47fe619082abcc6794aebc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'5e1cec9e9011fc96638620a2ca8e08eeaeaea8a28c47fe619082abcc6794aebc']

Name

b624949df8b0e3a6153fdfb730a7c6f4990b6592ee0d922e1788433d276610f3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'b624949df8b0e3a6153fdfb730a7c6f4990b6592ee0d922e1788433d276610f3']

Name

6d37baeb841bcf6c4935a54f29df049d405df48345014cc12852b814d279d86e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6d37baeb841bcf6c4935a54f29df049d405df48345014cc12852b814d279d86e']

Name

goto.searchpoweronline.com

Pattern Type

stix

Pattern

[hostname:value = 'goto.searchpoweronline.com']

Name

cd2b9cf8489cca6b357bc2706a68f5a12aeb696380ce7371803d68f08e337630

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cd2b9cf8489cca6b357bc2706a68f5a12aeb696380ce7371803d68f08e337630']

Name

e248b01e3ccde76b4d8e8077d4fcb4d0b70e5200bf4e738b45a0bd28fbc2cae6

Description

ConventionEngine_Term_Users

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e248b01e3ccde76b4d8e8077d4fcb4d0b70e5200bf4e738b45a0bd28fbc2cae6']

Name

e9fad9727b8a66e6b593d8b416f1c60b692ffc91b72e14bb30c40a1ce9b6a260

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e9fad9727b8a66e6b593d8b416f1c60b692ffc91b72e14bb30c40a1ce9b6a260']

StixFile

Value
e248b01e3ccde76b4d8e8077d4fcb4d0b70e5200bf4e738b45a0bd28fbc2cae6
5e1cec9e9011fc96638620a2ca8e08eeaeaea8a28c47fe619082abcc6794aebc
e9fad9727b8a66e6b593d8b416f1c60b692ffc91b72e14bb30c40a1ce9b6a260
cd2b9cf8489cca6b357bc2706a68f5a12aeb696380ce7371803d68f08e337630
6d37baeb841bcf6c4935a54f29df049d405df48345014cc12852b814d279d86e
b624949df8b0e3a6153fdfb730a7c6f4990b6592ee0d922e1788433d276610f3

Hostname

Value
goto.searchpoweronline.com

External References

- https://otx.alienvault.com/pulse/6478b506a9bcf5c50e555e3f
- https://northwave-cybersecurity.com/threat-intel-research/analysis-of-new-active-malware-mediaarena-pua