Jun 19 2023

NETMANAGEIT

Intelligence Report

Shampoo: A New ChromeLoader Campaign

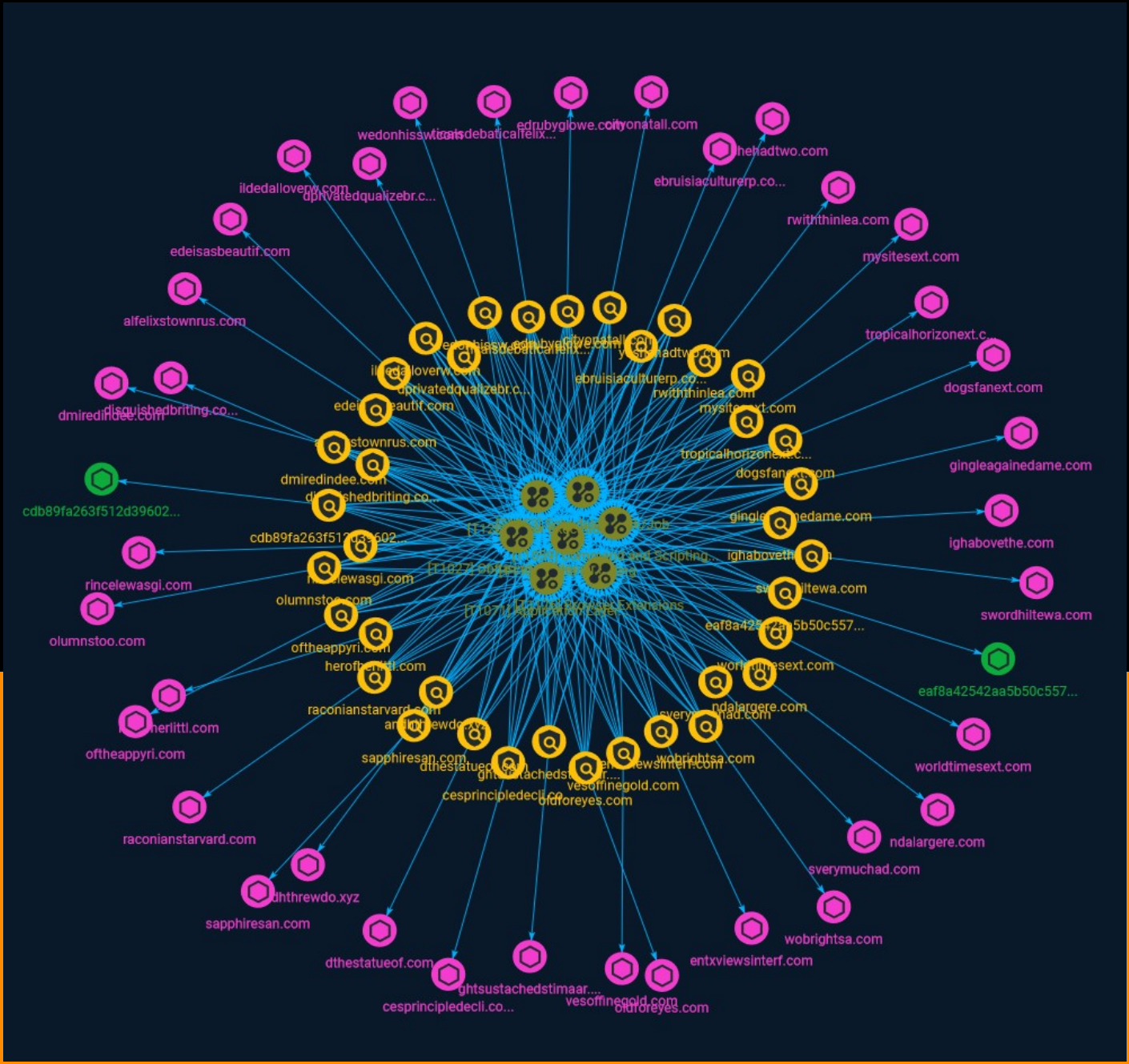

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A new malware campaign built around a new Google Chrome extension has been detected by HP Wolf Security and is able to gather sensitive personal information and inject advertisements into a victim' browsing session, but is difficult to get rid of.

Confidence

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

15 / 100

Attack-Pattern

Name

Scheduled Task/Job

ID

T1053

Description

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security) Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process. (Citation: ProofPoint Serpent)

Name

Data Encoding

ID

T1132

Description

Adversaries may encode data to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system. Use of data encoding may adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, or other binary-to-text and character encoding systems.(Citation: Wikipedia Binary-to-text Encoding) (Citation: Wikipedia Character Encoding) Some data encoding systems may also result in data compression, such as gzip.

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to

deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

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)

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Indicator

Name
rincelewasgi.com
Pattern Type
stix
Pattern
[domain-name:value = 'rincelewasgi.com']
Name
rwiththinlea.com
Pattern Type
stix
Pattern
[domain-name:value = 'rwiththinlea.com']
Name
entxviewsinterf.com

Pattern Type
stix
Pattern
[domain-name:value = 'entxviewsinterf.com']
Name
dprivatedqualizebr.com
Pattern Type
stix
Pattern
[domain-name:value = 'dprivatedqualizebr.com']
Name
gingleagainedame.com
Pattern Type
stix
Pattern
[domain-name:value = 'gingleagainedame.com']
Name
cesprincipledecli.com

Pattern Type
stix
Pattern
[domain-name:value = 'cesprincipledecli.com']
Name
ticalsdebaticalfelixs.com
Pattern Type
stix
Pattern
[domain-name:value = 'ticalsdebaticalfelixs.com']
Name
ndalargere.com
Pattern Type
stix
Pattern
[domain-name:value = 'ndalargere.com']
Name
disguishedbriting.com

Pattern Type
stix
Pattern
[domain-name:value = 'disguishedbriting.com']
Name
mysitesext.com
Pattern Type
stix
Pattern
[domain-name:value = 'mysitesext.com']
Name
dthestatueof.com
Pattern Type
stix
Pattern
[domain-name:value = 'dthestatueof.com']
Name
edeisasbeautif.com

Pattern Type
stix
Pattern
[domain-name:value = 'edeisasbeautif.com']
Name
ighabovethe.com
Pattern Type
stix
Pattern
[domain-name:value = 'ighabovethe.com']
Name
raconianstarvard.com
Pattern Type
stix
Pattern
[domain-name:value = 'raconianstarvard.com']
Name
ebruisiaculturerp.com

Pattern Type

stix

Pattern

[domain-name:value = 'ebruisiaculturerp.com']

Name

sverymuchad.com

Pattern Type

stix

Pattern

[domain-name:value = 'sverymuchad.com']

Name

cdb89fa263f512d396020efee1396dc1ac2eda17f4d5a2f7c0177d4a1d8b9744

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cdb89fa263f512d396020efee1396dc1ac2eda17f4d5a2f7c0177d4a1d8b9744']

Name

dogsfanext.com

Pattern Type

stix

Pattern

[domain-name:value = 'dogsfanext.com']

Name

sapphiresan.com

Pattern Type

stix

Pattern

[domain-name:value = 'sapphiresan.com']

Name

wedonhissw.com

Pattern Type

stix

Pattern

[domain-name:value = 'wedonhissw.com']

Name

worldtimesext.com

Pattern Type

stix

Pattern

[domain-name:value = 'worldtimesext.com']

Name

oftheappyri.com

Pattern Type

stix

Pattern

[domain-name:value = 'oftheappyri.com']

Name

yeshehadtwo.com

Pattern Type

stix

Pattern

[domain-name:value = 'yeshehadtwo.com']

Name

ghtsustachedstimaar.com

Pattern Type

stix

Pattern

[domain-name:value = 'ghtsustachedstimaar.com']

Name

alfelixstownrus.com

Pattern Type

stix

Pattern

[domain-name:value = 'alfelixstownrus.com']

Name

swordhiltewa.com

Pattern Type

stix

Pattern

[domain-name:value = 'swordhiltewa.com']

Name

andhthrewdo.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'andhthrewdo.xyz']

Name

edrubyglowe.com

Pattern Type

stix

Pattern

[domain-name:value = 'edrubyglowe.com']

Name

wobrightsa.com

Pattern Type

stix

Pattern

[domain-name:value = 'wobrightsa.com']

Name

olumnstoo.com

Pattern Type

stix

Pattern

[domain-name:value = 'olumnstoo.com']

Name

tropicalhorizonext.com

Pattern Type

stix

Pattern

[domain-name:value = 'tropicalhorizonext.com']

Name

oldforeyes.com

Pattern Type

stix

Pattern

[domain-name:value = 'oldforeyes.com']

Name

ildedalloverw.com

Pattern Type

stix

Pattern

[domain-name:value = 'ildedalloverw.com']

Name

eaf8a42542aa5b50c557010b00e00533561bac8a8520f94e718d9c20db7d52ef

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'eaf8a42542aa5b50c557010b00e00533561bac8a8520f94e718d9c20db7d52ef']

Name

herofherlittl.com

Pattern Type

stix

Pattern

[domain-name:value = 'herofherlittl.com']

Name
cityonatall.com
Pattern Type
stix
Pattern
[domain-name:value = 'cityonatall.com']
Name
vesoffinegold.com
Pattern Type
stix
Pattern
[domain-name:value = 'vesoffinegold.com']
Name
dmiredindee.com
Pattern Type
stix
Pattern
[domain-name:value = 'dmiredindee.com']

Domain-Name

Value
mysitesext.com
ticalsdebaticalfelixs.com
rincelewasgi.com
edrubyglowe.com
edeisasbeautif.com
sverymuchad.com
ndalargere.com
wobrightsa.com
disguishedbriting.com
yeshehadtwo.com
ighabovethe.com
herofherlittl.com
ghtsustachedstimaar.com

ebruisiaculturerp.com

cesprincipledecli.com

dthestatueof.com

gingleagainedame.com

vesoffinegold.com

worldtimesext.com

andhthrewdo.xyz

ildedalloverw.com

dogsfanext.com

raconianstarvard.com

entxviewsinterf.com

rwiththinlea.com

sapphiresan.com

dprivatedqualizebr.com

olumnstoo.com

dmiredindee.com

tropicalhorizonext.com

swordhiltewa.com

cityonatall.com
oldforeyes.com
alfelixstownrus.com
oftheappyri.com
wedonhissw.com

StixFile

Value
eaf8a42542aa5b50c557010b00e00533561bac8a8520f94e718d9c20db7d52ef
cdb89fa263f512d396020efee1396dc1ac2eda17f4d5a2f7c0177d4a1d8b9744

External References

- https://threatresearch.ext.hp.com/shampoo-a-new-chromeloader-campaign/
- https://otx.alienvault.com/pulse/649081740301076f96dfbce0