Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

New Chromeloader Shampoo Campaign Infecting Chrome and Stealing Data

Date of Publication	Admiralty Code	TA Number
June 21, 2023	A1	TA2023272

Summary

First appeared: March, 2023
Attack Region: Worldwide
Affected Platform: Google Chrome browser users on Windows and MacOS
Malware: Shampoo
Attack: The current ChromeLoader Shampoo campaign, where users unknowingly download and execute VBScript files from malicious websites. These files trigger a series of PowerShell scripts, leading to the installation of a malicious Chrome extension that redirects searches, injects ads, and collects sensitive information.

Attack Regions

Attack Details

#1

A recent ChromeLoader Campaign, known as Shampoo, is utilizing a malicious Chrome browser extension. The campaign has been active since March 2023. ChromeLoader is a browser hijacker that installs browser extensions to redirect search results and promote unwanted software. In the past, ChromeLoader campaigns targeted Windows and macOS systems, and some even dropped additional malware like ransomware.

#2

In the current campaign, ChromeLoader is distributed through malicious websites offering free downloads of copyrighted media and games. The infection chain of Shampoo starts with victims downloading and executing the VBScript files, which then trigger a series of PowerShell scripts.

#3

These scripts set up a scheduled task to ensure persistence of the malware on the victim's system. Every 50 minutes, the scheduled task runs a looping script that downloads and executes another PowerShell script. This script is responsible for installing the malicious Chrome extension.

#4

Once installed, the ChromeLoader Shampoo extension gathers sensitive information, redirects search queries, and injects advertisements into the victim's browsing session. It disables search suggestions in the address bar, sends data back to a command-and-control server, and logs the last search query.

#5

It also prevents victims from accessing the Chrome extensions screen, redirecting them to the Chrome settings screen instead. Removing the Shampoo malware is challenging due to its multiple persistence mechanisms. The malware reinstalls itself even if the victim attempts to remove it or reboot the system.

Recommendations

To remove ChromeLoader Shampoo, users should delete scheduled tasks and associated registry key, and then reboot the computer to ensure complete removal of the malware.

Deploy and maintain reliable antivirus and anti-malware software across all devices to detect and block malicious scripts, files, and extensions associated with ChromeLoader Shampoo. Regularly scan systems for potential threats.

Keep systems and browsers up to date with the latest security patches and educate users about the risks of downloading content from untrusted sources to minimize the chances of ChromeLoader Shampoo infections.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0011 Command and Control	TA0005 Defense Evasion	TA0002 Execution
TA0007 Discovery	TA0001 Initial Access	TA0009 Collection	T1070 Indicator Removal
T1189 Drive-by Compromise	T1027 Obfuscated Files or Information	T1204 User Execution	T1204.001 Malicious Link
T1059 Command and Scripting Interpreter	T1027.009 Embedded Payloads	T1059.005 Visual Basic	T1204.002 Malicious File
T1059.001 PowerShell	T1053.005 Scheduled Task	T1053 Scheduled Task/Job	T1176 Browser Extensions
T1622 Debugger Evasion	T1071 Application Layer Protocol	T1059.007 JavaScript	T1132.002 Non-Standard Encoding
T1132.001 Standard Encoding	T1132 Data Encoding	T1012 Query Registry	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	eaf8a42542aa5b50c557010b00e00533561bac8a8520f94e718d9c20db7d52ef cdb89fa263f512d396020efee1396dc1ac2eda17f4d5a2f7c0177d4a1d8b9744
Domains	mysitesext[.]com worldtimesext[.]com cesprincipledecli[.]com dogsfanext[.]com raconianstarvard[.]com ghtsustachedstimaar[.]com entxviewsinterf[.]com disguishedbriting[.]com gingleagainedame[.]com ebruisiaculturerp[.]com dprivatedqualizebr[.]com alfelixstownrus[.]com ticalsdebaticalfelixs[.]com edeisasbeautif[.]com dmiredindee[.]com sverymuchad[.]com swordhiltewa[.]com wedonhissw[.]com ndalargere[.]com wobrightsa[.]com yeshehadtwo[.]com sapphiresan[.]com oldforeyes[.]com vesoffinegold[.]com rwiththinlea[.]com ildedalloverw[.]com rincelewasgi[.]com oftheappyri[.]com dthestatueof[.]com ighabovethe[.]com cityonatall[.]com olumnstoo[.]com tropicalhorizonext[.]com edrubyglowe[.]com herofherlittl[.]com andhthrewdo[.]xyz

References

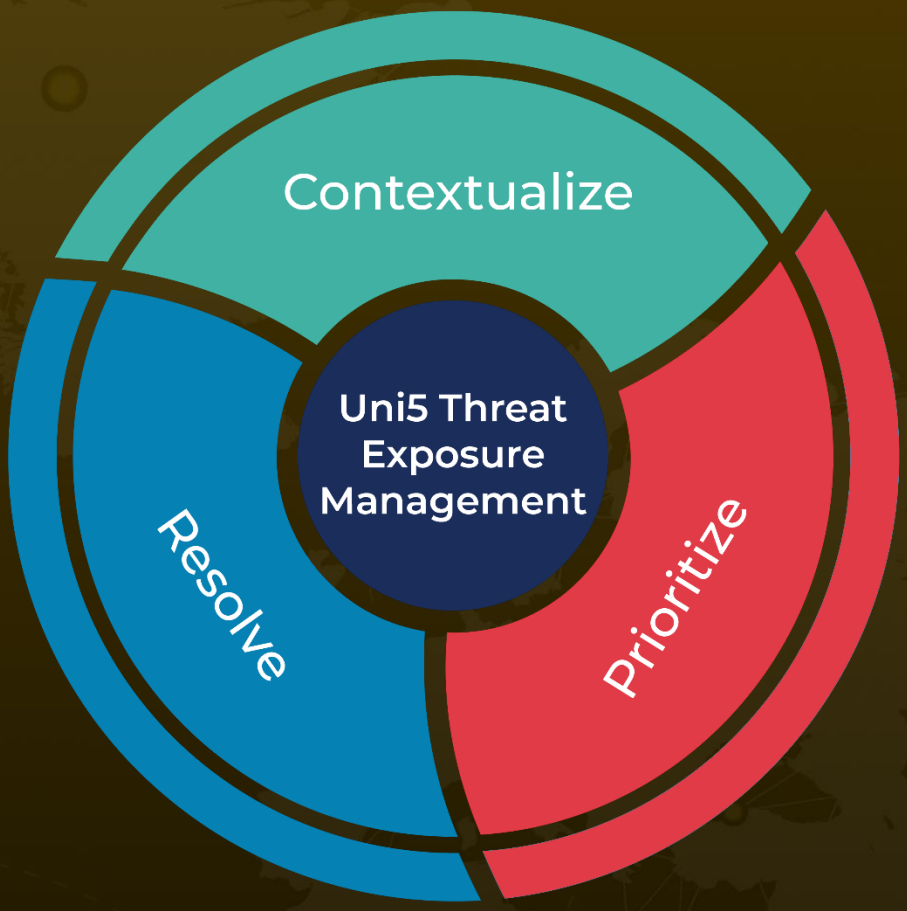
https://threatresearch.ext.hp.com/shampoo-a-new-chromeloader-campaign/

https://www.bleepingcomputer.com/news/security/new-shampoo-chromeloader-malware-pushed-via-fake-warez-sites/

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 21, 2023 • 5:00 AM

More at www.hivepro.com