Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Widespread Malware Campaign Targets Over 300,000 Users via Fake Downloads

Date of Publication

August 12, 2024

Admiralty Code

A1

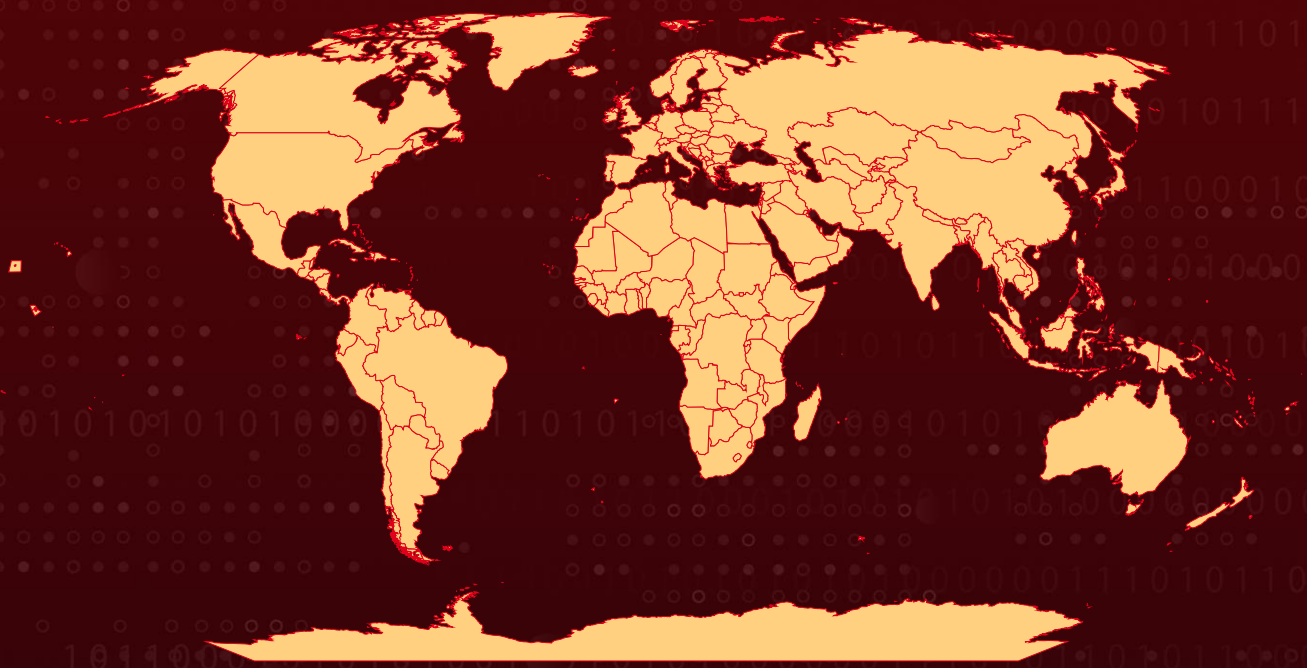
TA Number

TA2024308

Summary

First Appearance: 2021
Targeted Countries: Worldwide
Affected Platforms: Windows
Targeted Browsers: Chrome and Edge
Attack: A widespread malware campaign targets web browser extensions, affecting over 300,000 users of Google Chrome and Microsoft Edge. This polymorphic trojan installs malicious extensions through imitation download sites, hijacking search queries and redirecting users to harmful sites. It also prevents users from removing the extensions and disables browser updates, allowing it to persist undetected. The ongoing campaign underscores the urgent need for enhanced security measures and user awareness to combat the growing threat of malicious web extensions.

Attack Regions



Attack Details

#1

A widespread malware campaign has emerged, targeting web browser extensions and affecting users primarily of Google Chrome and Microsoft Edge. This campaign involves a polymorphic trojan that forcefully installs malicious extensions, potentially compromising the security and privacy of at least 300,000 users since its inception in 2021. The malware is particularly concerning due to its stealthy nature and ability to evade detection by many antivirus programs.

#2

The distribution of this trojan typically occurs through imitation download sites that masquerade as legitimate sources for popular applications and games. Users, seeking to download software, inadvertently download executables that do not fulfill their intended purpose. Instead of installing the desired applications, these executables install the malware on the user's system, setting the stage for further malicious activities.

#3

Once the trojan is installed, it registers a scheduled task that executes a PowerShell script. This script is responsible for downloading additional malicious payloads and modifying system settings to enforce the installation of harmful browser extensions. These extensions are designed to hijack search queries and redirect users to adversarial search engines, significantly degrading the browsing experience and potentially exposing users to further threats.

#4

One of the most alarming aspects of this malware is its ability to prevent users from disabling or removing the installed extensions. Additionally, it can disable browser updates, ensuring that the malware remains active and undetected. This creates a persistent threat, as users may be unaware that their browsing activities are being manipulated and monitored.

#5

Detection of this malware poses significant challenges, as many antivirus engines currently fail to recognize the installer or the malicious extensions. This lack of detection allows the malware to persist undetected on users' systems, making it crucial for users to be vigilant about the sources from which they download software and extensions.

#6

In response to this alarming situation, security researchers has informed both Google and Microsoft about the malware campaign, prompting the companies to take measures to mitigate the threat. This campaign highlights the growing risk associated with browser extensions and the need for enhanced security measures to protect users from similar malicious activities in the future.

Recommendations

Download from Official Sources: Always download applications and browser extensions directly from official websites or trusted sources, such as the Chrome Web Store or Microsoft Edge Add-ons store. Avoid third-party sites that may host malicious versions of popular software.

Review Permissions Carefully: Before installing any browser extension, carefully review the permissions it requests. Be cautious of extensions that ask for extensive permissions that seem unnecessary for their functionality.

Enable Browser Security Features: Utilize built-in security features in your browser, such as pop-up blockers, phishing protection, and safe browsing modes. Keeping these features enabled can help reduce the risk of encountering malicious downloads.

Regularly Update Your Browser and Extensions: Ensure that your web browser and all installed extensions are kept up to date. Regular updates often include security patches that protect against newly discovered vulnerabilities.

Use a Trusted Malware Removal Tool: To effectively remove malware from your system, download and run a reputable malware removal tool. Perform a full system scan, following the tool's instructions to detect and remove any malicious files or programs. Additionally, manually check for suspicious tasks in the Task Scheduler and registry entries, and remove any that are identified as part of the malware, ensuring that all persistence mechanisms are eliminated.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation	TA0011 Command and Control
TA0003 Persistence	TA0010 Exfiltration	TA0005 Defense Evasion	T1547.001 Registry Run Keys / Startup Folder
T1176 Browser Extensions	T1547 Boot or Logon Autostart Execution	T1070 Indicator Removal	T1547.009 Shortcut Modification

T1574.001 DLL Search Order Hijacking	T1574 Hijack Execution Flow	T1036 Masquerading	T1053.005 Scheduled Task
T1053 Scheduled Task/Job	T1059.001 PowerShell	T1059 Command and Scripting Interpreter	T1189 Drive-by Compromise
T1027 Obfuscated Files or Information	T1562 Impair Defenses	T1059.007 JavaScript	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	64e1473c7a5165484190bffd4a4a6cac, d1fc9e6d71a4867ab71af5566e525ba0
SHA1	02eb1f019d41924299d71007a4c7fd28d009563a, 06941262e1361c380acb6f04608ed5ae7d1c9d32, 06d06bb31b570b94d7b4325f511f853dbe771c21, 0885fd3ef0d221951e69f9424d4a4c3bda4c27f6, 0c89668954744ae7deb917312bdbea9da4cc5ec7, 0cdc202ba17c952076c37c85eece7b678ebaeef9, 0dfce59bee9ac5eb2b25508056df2225ef80552f, 24ad4e22bfd9a7b1238c04584d1c11ba747a59c7, 29c4cb1faa2e6f0a4352d01d8b8679cef13c5e63, 2a000fd4789def61f3c4eb19d237ca7c883515bf, 2c0dfb4016fb7ad302b56dc8d9b98d260b094210, 32d3d554b4c1ba5727fccc097b8f9973921e029a, 3406ab5de89be8784124e60ff69f57252caa695b, 3b9af4dffbd426873fff40a0bb774a722873b6c7, 3bd71a7db286e4d73dd6a3b8ce5245b982cad327, 3c3289569465f6888bb5f5d75995a12a9e8b9b8a, 3db731f11d9c85c9d2dcabee6ff8beeeee97fd7d, 485a7123de0eaef12e286b04a65cd79157d47fb4, 52f2f69805f9790502eb36d641575d521c4606a2, 58f231f5b70d92fca99e76c5636f25990a173d69, 593b10280a926134839feb8e2f9d0da9ee9c0593, 635cf72f978b29dc9c8aac09ea53bc68c2c8681b, 6bd339650f09170f3d6995ae210340aa2c86956e, 6ca66f2ecbfdca6de6bcf3ec8dc9680eb1eea28c, 71a0cce57881714af2558fcb3d86814e8e13e659, 7dc484d089584e93bb04652e1667854630b12d42, 7de95a8e148bfae7b671c086dd6dcffc9e796020,

TYPE	VALUE
SHA1	88baaa2eefe27ad5d2bc387a5ad96f507cbf00c1, 96c6cc391821604c787236061facc5c9a0106a74, a0576d244e8c15752113534c802e4cd9f68e8e49, a7ff4146d7ab62fc8922d77a57086d8ff6f257cf, a8f4eab0b73f5056489d36eb957bd0a70c6c9e6c, b295c9fd32eb12401263de5ec44c8f86b94938c3, b57022344af1b4cf15ead0bb15deacc6acb6ff18, b6ab97623171964f36ba41389d6bcd4ce2c3db8c, bbd51d7ac6e44d41c32a546b35c9d9cfc3abafee, bde186152457cacf9c35477b5bdda5bcb56b1f45, bf0eacb1afb00308f87159f67eb3f30d63e0cb62, c2cd89e1ce6c05188b425bba816ffd5f56f7e562, c2ea4ea024d5996acb23297c1bff7f131f29311a, c4f464637bfbfc31b7af53a43e6d3c74877796ac, d62c4654ba1ebb693922d2ecbb77d1e6d710bce7, da037a7d75e88e4731afe6f3f4e9c36f90bf1854, da884c769261c0b4dce41d4c9bcdb2672f223fd4, e1f8024441f84019b3124038b19e091b7214ca34, Ffdcd5acc8d5dc153ba2d7747de0c97603303e75
SHA256	21be0a068d7d1b57578bfb2ed850b3f3b1cfe4a4c47981ead95abdb8c20278fe, 22e7d2d85820b49f1278ce152c5ed39fd88087c7a998dcf348b6164d5b33bb8d, 5ce016d3133d960f68b0415d5bb825b143713ffaea751b098ffcf80353bc171b, d421d0cab4712291f54c15dd7d1a0dc02e498998f14b157bd11e1e6f43a54efe
URLs	hxxp[://]4kdownloads[.]com/app/4kvideodownloader_4[.]1_x64LTS[.]exe, hxxp[://]cdn[.]googlstaticontent[.]com/DesktopApp/YouTubeAppSetup[.]exe, hxxp[://]emu-dolphin[.]com/app/dolphin-x64-5[.]1[.]exe, hxxp[://]fpsunlockers[.]com/app/FPSUnlocker_4[.]1_x64LTS[.]exe, hxxp[://]insta[.]4kdownloads[.]com/app/Insta4kDownloader_ex64LTS[.]ex, hxxp[://]insta[.]4kdownloads[.]com/app/Insta4kDownloader_x64LTS[.]exe, hxxp[://]pcgameloop[.]com/app/GLP_installer_900221846[.]exe, hxxp[://]rummi[.]mrgameshub[.]com/app/RummikubSetup_ex64LTS[.]exe, hxxp[://]securedatacorner[.]com/exe/download/ChromeSetup[.]exe, hxxp[://]securedatacorner[.]com/exe/download/SteamSetup[.]exe, hxxp[://]tiktok[.]4kdownloads[.]com/app/TikTokDownloader_3[.]1_ex64LTS[.]exe, hxxp[://]winautoclicker[.]com/app/AutoClicker_x64LTS[.]exe, hxxp[://]wordle[.]mrgameshub[.]com/app/Wordle_x64LTS[.]exe, hxxp[://]yoursearchbar[.]me/search?q=
Domains	securedatacorner[.]com, Nvoptimie[.]com, nvoptimizer[.]com, Customsearchbar[.]me, yoursearchbar[.]me,

TYPE	VALUE
Domains	activesearchbar[.]me, msf-console[.]com, msf-edge[.]com, search-good[.]com, Microsearch[.]me, yglsearch[.]com, qcomsearch[.]comlaxsearch[.[comqtrsearch[.]comSafesearcheng[.]com, simplenewtab[.]com, Wonderstab[.]com, searchnukes[.]com, exyzsearch[.]com, kondoserp1[.]com

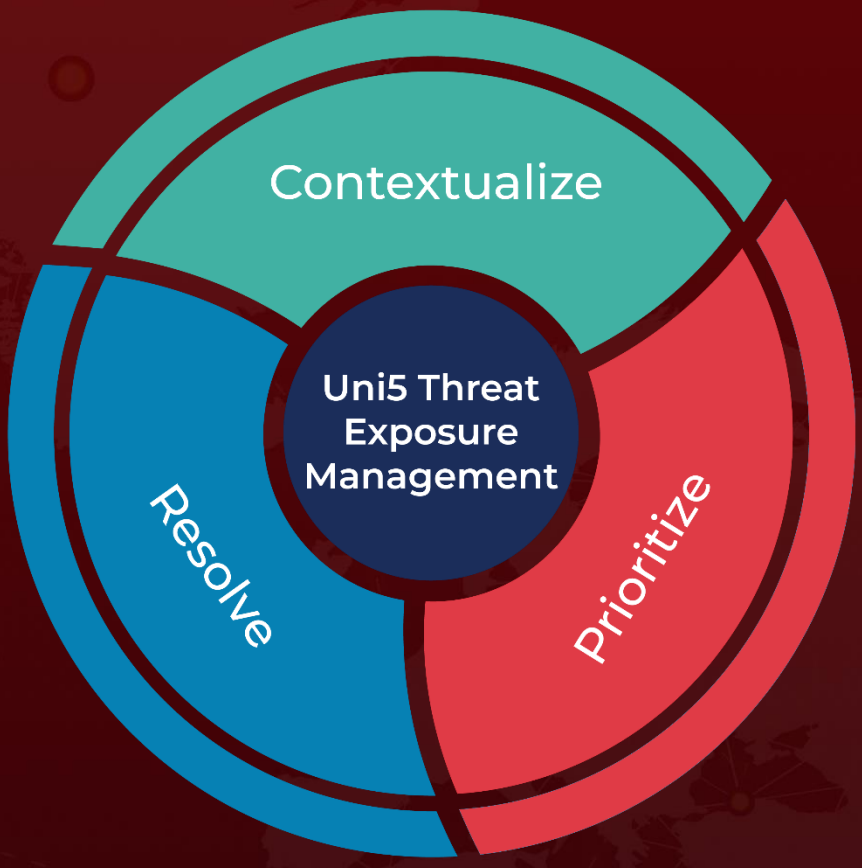
References

https://reasonlabs.com/research/new-widespread-extension-trojan-malware-campaign

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

August 12, 2024 • 6:30 AM

More at www.hivepro.com