BLACKSWAN CYBERSECURITY

THREAT ADVISORY

August 13, 2024

Malware Campaign with Malicious Chrome and Edge Extensions

SUMMARY

A current malware campaign is using malicious Google Chrome and Microsoft Edge extensions to install a trojan via fake websites that appear legitimate. According to the ReasonLabs research team, "The trojan malware includes various payloads, from basic adware extensions that hijack search results to more advanced malicious scripts that install local extensions to steal sensitive data and execute a range of commands."

TECHNICAL DETAILS

The malware and its associated extensions have impacted over 300,000 users of Chrome and Edge. Malvertising is the primary tactic, where users are directed to lookalike websites mimicking Roblox FPS Unlocker, YouTube, VLC media player, Steam, or KeePass. These fake sites deceive users into downloading a trojan, which then acts as a delivery mechanism for installing malicious browser extensions.

Once installed, the trojan registers a scheduled task designed to run a PowerShell script that then downloads and executes additional payloads from a remote server. The script also modifies the Windows Registry to enforce the installation of extensions from the Chrome Web Store and Microsoft Edge Add-ons. These extensions hijack search queries on Google and Microsoft Bing, redirecting them through servers controlled by the attackers.

The installed extensions are highly persistent and cannot be disabled by the user, even when Developer Mode is enabled. According to ReasonLabs, newer versions of the script also prevent browser updates. The campaign includes launching a local extension, downloaded directly from a command-and-control (C2) server, which can intercept all web requests, sending them to the C2 server, receiving commands and encrypted scripts, and injecting and loading scripts into all web pages. The malware also hijacks search queries from search engines like Ask.com, Bing, and Google, rerouting them through its servers before directing users to other search engines.

Affected users are advised to take the following steps to mitigate the impact of this malware attack:

- Delete the scheduled task that reactivates the malware daily.
- Remove the associated Registry keys.
- Delete the following files and folders from the system:
  - C:Windowssystem32Privacyblockerwindows.ps1
  - C:Windowssystem32Windowsupdater1.ps1
  - C:WindowssystemWindowsUpdater1Script.ps1
  - C:Windowssystem32Optimizerwindows.ps1
  - C:Windowssystem32Printworkflowservice.ps1
  - C:Windowssystem32NvWinSearchOptimizer.ps1
  - C:Windowssystem32kondserp_optimizer.ps1
  - C:WindowsInternalKernelGrid
  - C:WindowsInternalKernelGrid3
  - C:WindowsInternalKernelGrid4
  - C:WindowsShellServiceLog
  - C:windowsprivacyprotectorlog
  - C:WindowsNvOptimizerLog

INDICATORS OF COMPROMISE (IoCs)

Domains:

- http[:]//wincloudservice[.]com/apps/$uid
- http[:]//sslwindows[.]com/apps/$uid
- securedatacorner[.]com
- Nvoptimie[.]com
- nvoptimizer[.]com
- Customsearchbar[.]me
- yoursearchbar[.]me
- 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

Extension IDs:

- "Google Updater" (local extension)

Chrome:

- nniikbbaboifhfjjkjekiamnfpkdieng - "Custom Search Bar" - 40K+ users
- nlmpchkfhgoclkajbifladignhbanjdk- "yglSearch" - 40K+ users
- bcmmbhidjmodkbeidljmhcijhkchokcj - "Qcom search bar" - 40+ users
- gdamghfpmkabflbpldhdpbbfofolgaji - "Qtr Search" - 6K+ users
- bbgbmlkfflffccognkcbbmkakbejnado - "Micro Search Chrome Extension" - 180K+ users (removed from Chrome store)
- pkofdnfadkamabkgjdjcddeopopbdjhg - "Active Search Bar" - 20K+ users (removed from Chrome store)
- dafkaabahcikblhbogbnbjodajmhbini- "Your Search Bar" - 40K+ users (removed from Chrome store)
- lfdkgganmodljeaemeadfhfhinpldmnf - "Safe Search Eng" - 35K+ users (removed from Chrome store)
- pjomkeecbjnbpmanlbeijbkahooibopk - "Lax Search" - 600+ users (removed from Chrome store)

Edge:

- fodkmcnpjapcffbmhelopfjhlmdmnbll - "Simple New Tab" - 100,000K+ users (removed from Edge store)
- Cmodflldkmidgkmpkllldpcmplemgoab - "Cleaner New Tab" - 2K+ users (removed from Edge store)
- Docmlpbiejclgidiacmjpkpoojgiacgn - "NewTab Wonders" - 7K+ users (removed from Edge store)
- dbncciiegloaglpkgjpjhfahaiopfppa - "SearchNukes" - 1K+ users (removed from Edge store
- ljgodogldijlkialfpccoekklegilffm - "EXYZ Search" - 1K+ users - this extension was registered with the same email of the creator of "Custom Search Bar", removed from Edge store)
- Odpgdmpimkafpjaihemmmmlalofkfpic - "Wonders Tab" - 6K+ users (removed from Edge store)

PowerShell scripts:

- C:\Windows\system32\Privacyblockerwindows.ps1
- C:\Windows\system32\Windowsupdater1.ps1
- C:\Windows\system32\WindowsUpdater1Script.ps1

- C:\Windows\system32\Optimizerwindows.ps1
- C:\Windows\system32\Printworkflowservice.ps1
- C:\Windows\system32\NvWinSearchOptimizer.ps1 - 2024 version
- C:\Windows\system32\kondserp_optimizer.ps1 - May 2024 version
- The contents of the invoked script: (new 2024 version - 9.8)
- https://www.virustotal.com/gui/file/5ce016d3133d960f68b0415d5bb825b143713ffaea751b098ffcf80353bc171b/content

Third-stage scripts (extension files fetched from C2):

- C:\Windows\InternalKernelGrid\analytics.js - 52f2f69805f9790502eb36d641575d521c4606a2
- C:\Windows\InternalKernelGrid\background.html - 3b9af4dffbd426873fff40a0bb774a722873b6c7
- C:\Windows\InternalKernelGrid\bg.js - da037a7d75e88e4731afe6f3f4e9c36f90bf1854
- C:\Windows\InternalKernelGrid\bg_fallback.js - d62c4654ba1ebb693922d2ecbb77d1e6d710bce7
- C:\Windows\InternalKernelGrid\config.js - b6ab97623171964f36ba41389d6bcd4ce2c3db8c - endless multiple hashes, this script contains the UID of the infected user, thus different hash for each user
- C:\Windows\InternalKernelGrid\content.js - 58f231f5b70d92fca99e76c5636f25990a173d69
- C:\Windows\InternalKernelGrid\crypto-js.min.js - bde186152457cacf9c35477b5bdda5bcb56b1f45
- C:\Windows\InternalKernelGrid\crypto.js - 635cf72f978b29dc9c8aac09ea53bc68c2c8681b
- C:\Windows\InternalKernelGrid\devtools.html - 0885fd3ef0d221951e69f9424d4a4c3bda4c27f6
- C:\Windows\InternalKernelGrid\devtools.js - da884c769261c0b4dce41d4c9bcdb2672f223fd4
- C:\Windows\InternalKernelGrid\extensions_page.css - da884c769261c0b4dce41d4c9bcdb2672f223fd4
- C:\Windows\InternalKernelGrid\extensions_page.js - 96c6cc391821604c787236061facc5c9a0106a74
- C:\Windows\InternalKernelGrid\icon.png - c2cd89e1ce6c05188b425bba816ffd5f56f7e562
- C:\Windows\InternalKernelGrid\manifest.json - 2a000fd4789def61f3c4eb19d237ca7c883515bf
- C:\Windows\InternalKernelGrid\version.txt - 06d06bb31b570b94d7b4325f511f853dbe771c21
- rc.js - 0dfce59bee9ac5eb2b25508056df2225ef80552f
- C:\Windows\InternalKernelGrid3\bg.js - 29c4cb1faa2e6f0a4352d01d8b8679cef13c5e63
- C:\Windows\InternalKernelGrid4\bg.js - bbd51d7ac6e44d41c32a546b35c9d9cfc3abafee
- C:\windows\internalkernelgrid3\extensions_page.js - 3db731f11d9c85c9d2dcabee6ff8beeeee97fd7d
- C:\windows\internalkernelgrid4\extensions_page.js - 88baaa2eefe27ad5d2bc387a5ad96f507cbf00c1
- C:\Windows\InternalKernelGrid4\config.js - 3406ab5de89be8784124e60ff69f57252caa695b- endless multiple hashes, this script
- contains the UID of the infected user, thus different hash for each user. In kerndelGrid4 the apiDomain is “nvoptimize[.]com”

Existence of These Folders:

- C:\Windows\InternalKernelGrid
- C:\Windows\InternalKernelGrid3
- C:\Windows\ShellServiceLog
- C:\windows\privacyprotectorlog
- C:\Windows\InternalKernelGrid4
- C:\Windows\NvOptimizerLog

Existence of These Scheduled Tasks:

- \NvOptimizerTaskUpdater_V2

Registry Activity:

- MACHINE\SOFTWARE\NVOPTIMIZER, InstallLocation, C:\Windows\NvOptimizerLog
- USER\S-1-...\SOFTWARE\NVOPTIMIZER, InstallLocation, C:\Windows\NvOptimizerLog

- MACHINE\SOFTWARE\WOW6432NODE\NVOPTIMIZER, InstallLocation, C:\Windows\NvOptimizerLog
- MACHINE\SOFTWARE\NVOPTIMIZER, ExecFileName, Download_Checkpoint-Setup-v-aj8e3aA.exe
- SOFTWARE\\Policies\\Google\\Chrome\\ExtensionInstallForcelist
- SOFTWARE\\Policies\\Microsoft\\Edge\\ExtensionInstallForcelist

Installer URL Examples (NOT All are Included):

- https[://]dn[.]keepass[.]tech[/]api[/]download[?]app
- https[://]winautoclicker[.]com/app/AutoClicker_x64LTS.exe
- https[://]downloadbucket1x.s3.eu-west-1.amazonaws[.]com/FPSUnlocker_x64.exe
- https[://]4kdownloads[.]com/app/4kvideodownloader_4.1_x64LTS.exe
- https[://]fpsunlockers[.]com/app/FPSUnlocker_4.1_x64LTS.exe
- https[://]emu-dolphin[.]com/app/dolphin-x64-5.1.exe
- https[://]pcgameloop[.]com/app/GLP_installer_900221846.exe
- https[://]tiktok.4kdownloads[.]com/app/TikTokDownloader_3.1_ex64LTS.exe
- https[://]insta.4kdownloads[.]com/app/Insta4kDownloader_ex64LTS.exe
- https[://]cdn.googlstaticontent[.]com/DesktopApp/YouTubeAppSetup.exe
- https[://]insta.4kdownloads[.]com/app/Insta4kDownloader_x64LTS.exe
- https[://]rummi.mrgameshub[.]com/app/RummikubSetup_ex64LTS.exe
- https[://]wordle.mrgameshub[.]com/app/Wordle_x64LTS.exe
- https[://]securedatacorner[.]com/exe/download/SteamSetup.exe
- https[://]securedatacorner[.]com/exe/download/ChromeSetup.exe

More Hashes:

- 3c3289569465f6888bb5f5d75995a12a9e8b9b8a
- 0cdc202ba17c952076c37c85eece7b678ebaeef9
- Bf0eacb1afb00308f87159f67eb3f30d63e0cb62
- 485a7123de0eaef12e286b04a65cd79157d47fb4
- B57022344af1b4cf15ead0bb15deacc6acb6ff18
- 3bd71a7db286e4d73dd6a3b8ce5245b982cad327
- C2ea4ea024d5996acb23297c1bff7f131f29311a
- 6ca66f2ecbfdca6de6bcf3ec8dc9680eb1eea28c
- 02eb1f019d41924299d71007a4c7fd28d009563a
- 0c89668954744ae7deb917312bdbea9da4cc5ec7
- 6ca66f2ecbfdca6de6bcf3ec8dc9680eb1eea28c
- B295c9fd32eb12401263de5ec44c8f86b94938c3
- 06941262e1361c380acb6f04608ed5ae7d1c9d32
- 24ad4e22bfd9a7b1238c04584d1c11ba747a59c7
- 2c0dfb4016fb7ad302b56dc8d9b98d260b094210
- A8f4eab0b73f5056489d36eb957bd0a70c6c9e6c
- 6bd339650f09170f3d6995ae210340aa2c86956e
- 593b10280a926134839feb8e2f9d0da9ee9c0593
- 6bd339650f09170f3d6995ae210340aa2c86956e
- 7de95a8e148bfae7b671c086dd6dcffc9e796020
- 71a0cce57881714af2558fcb3d86814e8e13e659
- 485a7123de0eaef12e286b04a65cd79157d47fb4
- ffdcd5acc8d5dc153ba2d7747de0c97603303e75
- 32d3d554b4c1ba5727fccc097b8f9973921e029a
- 7dc484d089584e93bb04652e1667854630b12d42
- a0576d244e8c15752113534c802e4cd9f68e8e49
- e1f8024441f84019b3124038b19e091b7214ca34
- 06941262e1361c380acb6f04608ed5ae7d1c9d32
- A7ff4146d7ab62fc8922d77a57086d8ff6f257cf
- C4f464637bfbfc31b7af53a43e6d3c74877796ac
- 2a000fd4789def61f3c4eb19d237ca7c883515bf

RECOMMENDATIONS

- Identify and delete the scheduled task that reactivates the malware daily.
- Remove any malicious Registry keys associated with the malware.
- Manually locate and delete the specific malicious scripts and folders from your system as listed in the detailed technical analysis.
- Consider reinstalling or resetting your browsers (Google Chrome and Microsoft Edge) to remove any lingering malicious extensions or configurations.
- Use reputable antivirus and anti-malware software to scan and clean your system thoroughly.
- Regularly monitor your system for unusual activity and ensure all software, including your browsers, is up to date.

REFERENCES

- https://reasonlabs.com/research/new-widespread-extension-trojan-malware-campaign
- https://thehackernews.com/2024/08/new-malware-hits-300000-users-with.html