Detection of malicious code infecting the web browsers of 300,000 PCs, silently stealing user data

A worldwide malware campaign has installed malicious extensions into the web browsers of more than 300,000 computers globally.

Malicious code, when successfully infected on the target system, can silently modify browser executable files to hijack the home page and steal browsing history.

Installers and extensions, typically, are not scanned by antivirus tools, so they can stealthily steal data and execute commands on infected devices without fear of detection.

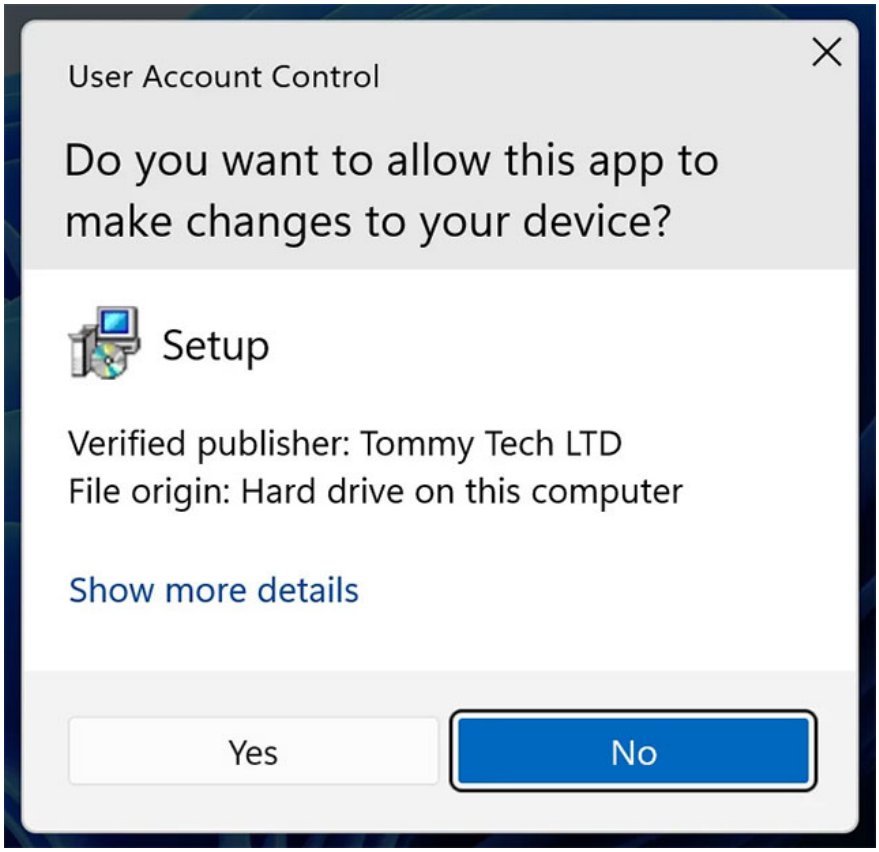
This campaign was first noted by security researchers at ReasonLabs. The expert group warns that the threat actors behind this campaign are using various malvertising themes to achieve the initial infection.

Infection through web browser

ReasonLabs said the infection begins with victims downloading software installers from fake websites, often advertised in Google search results.

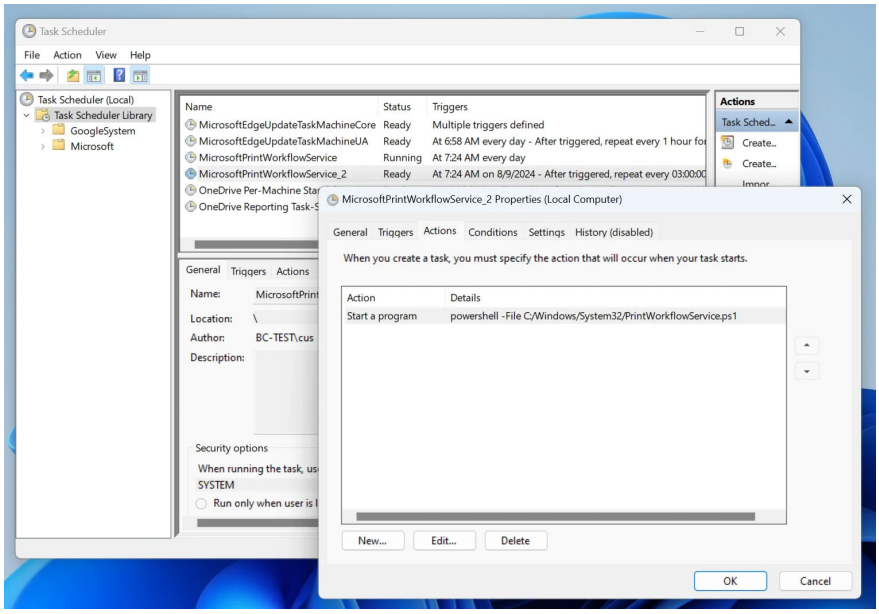
This malware campaign uses lures such as Roblox FPS Unlocker, TikTok Video Downloader, YouTube downloader, VLC video player, Dolphin Emulator and KeePass password manager.

The downloaded installers were digitally signed by 'Tommy Tech LTD' and had successfully avoided detection by all AV tools on VirusTotal at the time of analysis by ReasonLabs.



However, they do not contain anything resembling commonly found software tools, but instead run a PowerShell script C:WindowsSystem32PrintWorkflowService.ps1 to download another hidden malware from a remote server, and execute it on the victim's computer. The script will also modify the Windows registry to force installation of extensions from Chrome Web Store and Microsoft Edge Add-ons.

A scheduled task is also silently created to load the PowerShell script at varying intervals, allowing the threat actor to push additional malware or install other payloads.



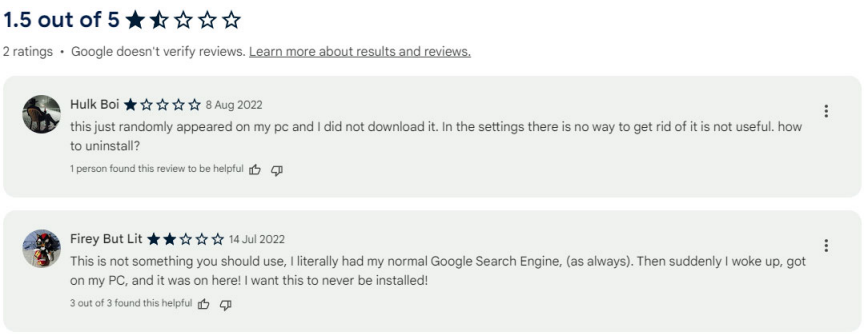
Analysis results showed that the malware installed a large number of different Google Chrome and Microsoft Edge extensions aimed at hijacking victims' search queries, changing homepages, and redirecting searches. search through the threat actor's servers so they can steal their browsing history.

ReasonLabs found the following Google Chrome extensions related to this campaign:

1. Custom Search Bar – 40K+ downloads
2. yglSearch – 40K+ downloads
3. Qcom search bar – 40+ downloads
4. Qtr Search – 6K+ downloads
5. Micro Search Chrome Extension – 180K+ downloads (removed from Chrome store)
6. Active Search Bar – 20K+ downloads (removed from Chrome store)
7. Your Search Bar – 40K+ downloads (removed from Chrome store)
8. Safe Search Eng – 35K+ downloads (removed from Chrome store)
9. Lax Search – 600+ downloads (removed from Chrome store)

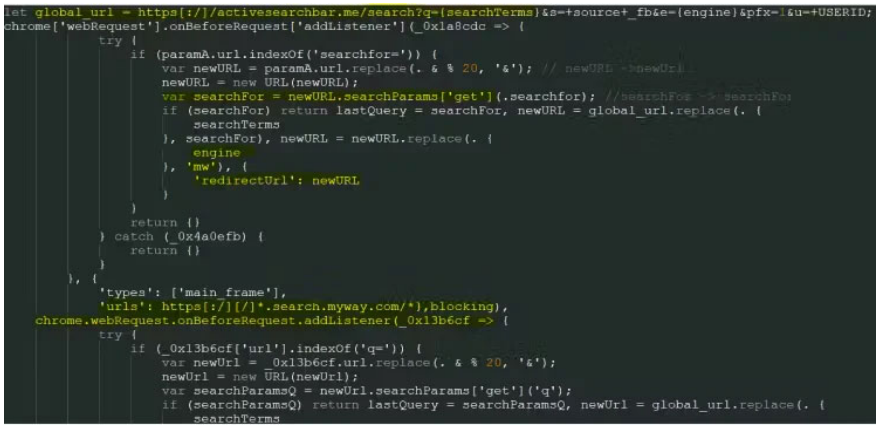
For Edge

1. Simple New Tab – 100,000K+ downloads (removed from Edge store)
2. Cleaner New Tab – 2K+ downloads (removed from Edge store)
3. NewTab Wonders – 7K+ downloads (removed from Edge store)
4. SearchNukes – 1K+ downloads (removed from Edge store)
5. EXYZ Search – 1K+ downloads (removed from Edge store)
6. Wonders Tab – 6K+ downloads (removed from Edge store)



Through these extensions, malicious attackers hijack users' search queries and instead redirect them to malicious results or advertising pages that generate revenue for the attacker. labour.

Additionally, they can collect login credentials, browsing history, and other sensitive information, monitor victims' online activities, and execute commands received from command and control servers (C2).



Malware uses many different methods to maintain persistence on the system, making it very difficult to remove. It may be necessary to uninstall and reinstall the browser.

PowerShell payloads will search and modify all web browser shortcut links to force loading of malicious extensions and disable the automatic update mechanism when the browser is started. This is to prevent Chrome's built-in protections from updating and detecting malware.

At the same time, it also prevents the installation of future security updates, leaving Chrome and Edge vulnerable to new vulnerabilities.

Even more cunning, the malware modifies DLLs used by Google Chrome and Microsoft Edge to hijack the browser's home page to a website under the threat actor's control, such as https ://microsearch[.]me/.

" *The purpose of this script is to locate browser DLLs (msedge.dll if Edge is the default browser) and change specific bytes at specific locations within it* ," ReasonLabs explains.

" *Doing so allows the script to hijack the default search from Bing or Google to the hacker's search portal. The script can check which browser version is installed and look for the corresponding bytes* ."

The only way to remove this modification is to upgrade to a new browser version or reinstall the browser.

Manual cleanup

To remove malicious code from the system, victims must go through a multi-step process to delete malicious files.

First, remove the scheduled task from Windows Task Scheduler, looking for suspicious entries pointing to scripts like 'NvWinSearchOptimizer.ps1', usually located in 'C:Windowssystem32.'

Second, delete malicious registry entries by opening Registry Editor ('Win+R' > regedit) and navigating to:

HKEY_LOCAL_MACHINESOFTWAREPoliciesGoogleChromeExtensionInstallForcelist
HKEY_LOCAL_MACHINESOFTWAREPoliciesMicrosoftEdgeExtensionInstallForcelist
HKEY_LOCAL_MACHINESOFTWAREWOW6432NodePoliciesGoogleChromeExtensionInstallForcelist
HKEY_LOCAL_MACHINESOFTWAREWOW6432NodePoliciesMicrosoftEdgeExtensionInstallForce list. list

Right-click on each key with the malicious extension name and select "Delete" to delete them.

Finally, use an AV tool to remove malware files from the system, or navigate to 'C:WindowsSystem32' and delete 'NvWinSearchOptimizer.ps1' (or similar).

Reinstalling the browser after the cleanup process may not be required, but is highly recommended to clean up highly invasive modifications made by malware.