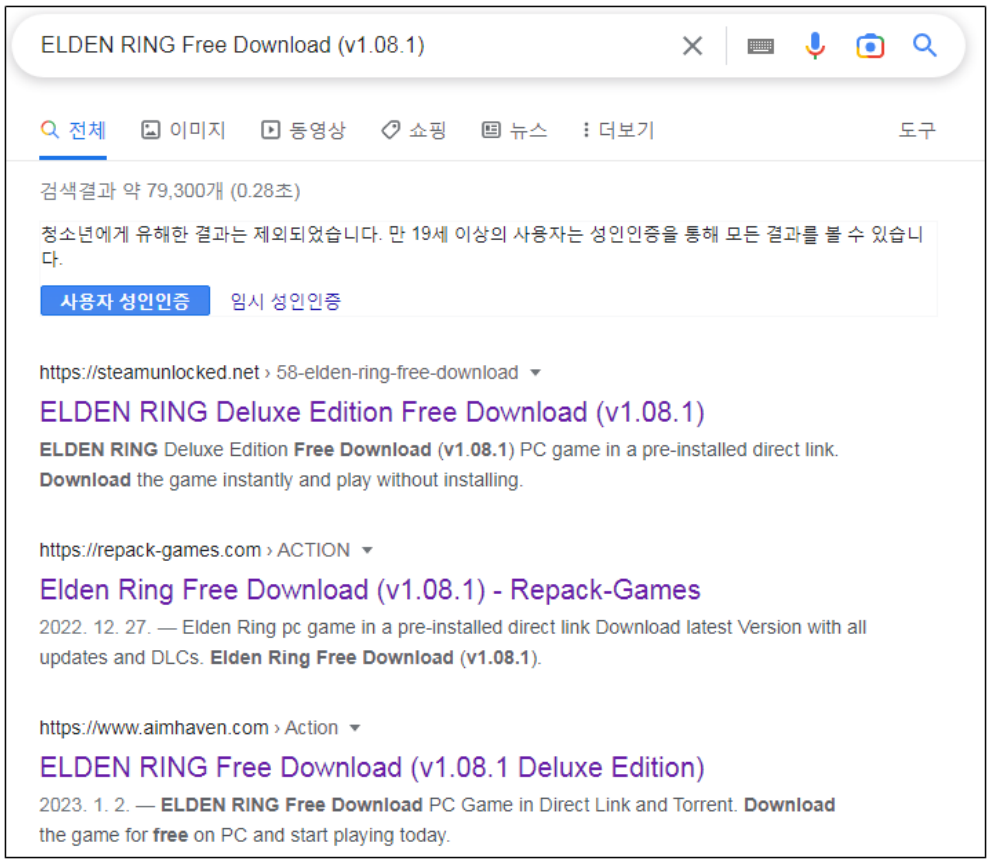
ChromeLoader campaign lures with malicious VHDs for popular games

By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

February 26, 2023 11:10 AM **0**

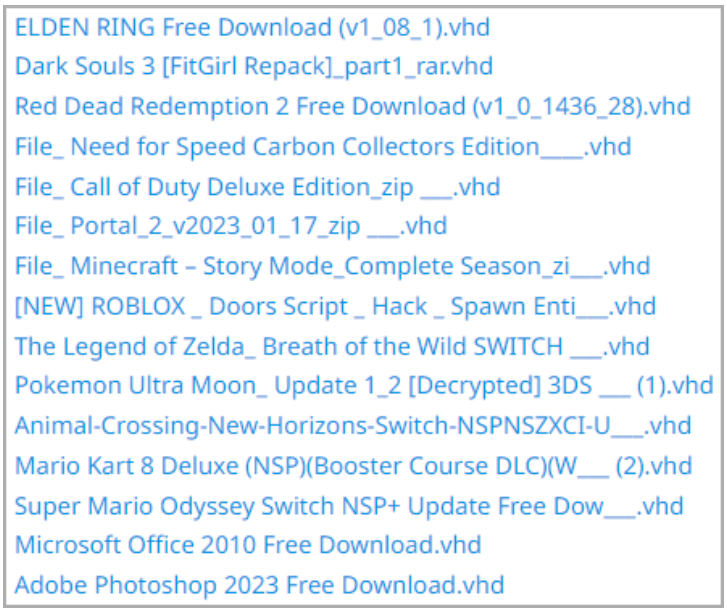
Security researchers have noticed that the operators of the ChromeLoader browser hijacking and adware campaign are now using VHD files named after popular games. Previously, such campaigns relied on ISO-based distribution.

The malicious files were discovered by member of the Ahnlab Security Emergency Response Center (ASEC (https://asec.ahnlab.com/en/48211/)) through Google search results to queries for popular games



Google Search results linking to adware sites *(ASEC)*

Among the game titles abused for adware distribution purposes are Elden Ring, ROBLOX, Dark Souls 3, Red Dead Redemption 2, Need for Speed, Call of Duty, Portal 2, Minecraft, Legend of Zelda, Pokemon, Mario Kart, Animal Crossing, and more.



VHD files used in latest ChromeLoader campaign *(ASEC)*

A network of malvertising sites distributes the malicious files, which appear as legitimate game-related packages, that install the ChromeLoader extension.

ChromeLoader hijacks the browser searches to show advertisements. Itt also modifies the browser settings, and collects credentials and browser data.

According to Red Canary (https://www.bleepingcomputer.com/news/security/new-chromeloader-malware-surge-threatens-browsers-worldwide/) data, the malware bacame more prevalent in May 2022. In September 2022, VMware reported (https://www.bleepingcomputer.com/news/security/vmware-microsoft-warn-of-widespread-chromeloader-malware-attacks/) new variants carying out more sophisticated network activities. In some cases the actor even delivered the Enigma ransomware.

In all cases seen throughout 2022, ChromeLoader arrived on the target system as an ISO file. Lately, the operators appear to prefer the VHD packaging.

VHD files can be easily mounted on on a Windows system and are supported by multiple virtualization software.

The images include several files but only one of them, a shortcut called "Install.lnk," is visible. Deploying the shortcut triggers the execution of a batch script that decompresses the content of a ZIP archive.

Contents of VHD files *(ASEC)*

In the next step, the batch file executes "data.ini," a VBScript, and a JavaScript that fetches the final payload from a remote resource.

According to ASEC, ChromeLoader will start redirecting to advertisement sites, thus generating revenue for its operators.

The researchers say that the addresses hosting the payload are not longe accessible. They note that the malicious Chrome extension that ChromeLoader creates and executes can also collect credential data stored in the browser.

ASEC's report provides a short set of indicators of compromise that can help detect the ChromeLoader threat.

Users are advised to avoid downloading games from unofficial sources, and keep away from cracks for popular products as they typically have a high security risk.

Related Articles:

VMware, Microsoft warn of widespread Chromeloader malware attacks (https://www.bleepingcomputer.com/news/security/vmware-microsoft-warn-of-widespread-chromeloader-malware-attacks/)

Activision confirms data breach exposing employee and game info (https://www.bleepingcomputer.com/news/security/activision-confirms-data-breach-exposing-employee-and-game-info/)

GTA Online bug exploited to ban, corrupt players' accounts (https://www.bleepingcomputer.com/news/security/gta-online-bug-exploited-to-ban-corrupt-players-accounts/)

Shady reward apps on Google Play amass 20 million downloads (https://www.bleepingcomputer.com/news/security/shady-reward-apps-on-google-play-amass-20-million-downloads/)

ADWARE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/ADWARE/)

CHROMELOADER (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CHROMELOADER/)

GAMES (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/GAMES/)