The Evolution of the Chromeloader Malware

By Abe Schneider, Bethany Hardin, Lavine Oluoch

Published: 2022-09-19 · Archived: 2026-04-05 15:03:57 UTC

Executive Summary

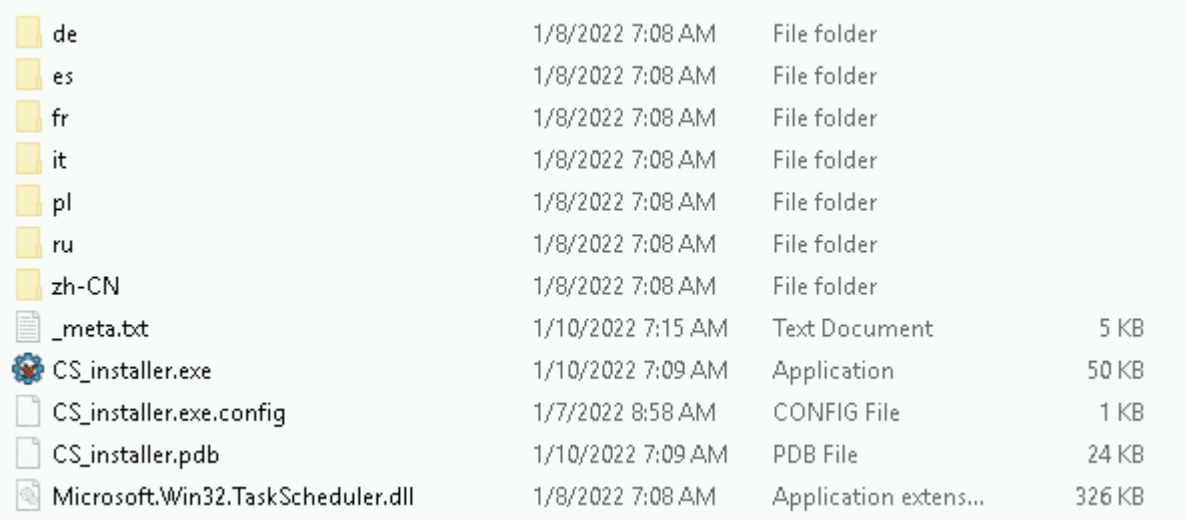
ChromeLoader proves to be an extremely prevalent and persistent malware. It initially drops as an .iso and can be used to leak users' browser credentials, harvest recent online activity and hijack the browser searches to display ads. The VMware Carbon Black Managed Detection and Response (MDR) team observed the first Windows variants of ChromeLoader in the wild in January 2022 and the macOS version in March 2022.

There are some variants known to ChromeLoader, including ChromeBack and Choziosi Loader. Unit 42 researchers have found evidence of The Real First Windows Variant using the AHK(AutoHotKey) tool to compile a malicious executable and drop version 1.0 of the malware.

Although this sort of malware is created with an intent to feed adware to the user, ChromeLoader also increases the attack surface of an infected system. This can eventually lead to much more devastating attacks such as ransomware. In this article, the VMware Carbon Black MDR team will show evidence of such attacks happening.

History

At the beginning of January 2022, the malware CS_installer was seen in the wild targeting Chrome browsers. CS_installer used ISO image file downloads and relied on user execution to initiate infection. The malware ultimately aimed to install a Chrome extension that acted as a browser hijacker, gathering personal information and tracking the user's browsing activity. CS_installer was also known as ChromeLoader as that was one of the names of the scheduled task the malware created. CS_Installer used a .NET executable by the same name to kick off the infection chain and install the malicious chrome extension.



CS_Installer activity died down for a bit and soon after a similar malware emerged. While this was also delivered via ISO files, there were differences in execution. This recent malware relies on a batch script in the mounted drive to install the second stage payload also delivered within the same ISO and start infection. This payload which would be the main malware file moving forward has varying names, some of the most common ones are mentioned below.

While the initial infection techniques and the contents of these two malware types are different, the objective is the same: to gather user data and track browsing activity while feeding adware. The naming convention of the scheduled tasks used by both samples to gain persistence was also very similar to **Chromeloader**. In addition, the coincidental timing of this second malware emerging right after CS_Installer/ChromeLoader died down would lead us to hypothesize that they are the same malware, the second variant being an evolution of the first.

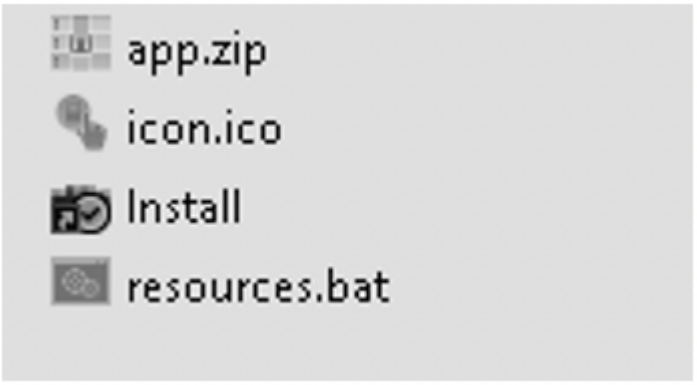
Other security professionals at Palo Alto Networks and Red Canary have alluded to the similarity and possible connection between these two malware. We will therefore also reference the second variant as ChromeLoader as we analyze the incidents MDR has responded to in this article.

ChromeLoader Delivery

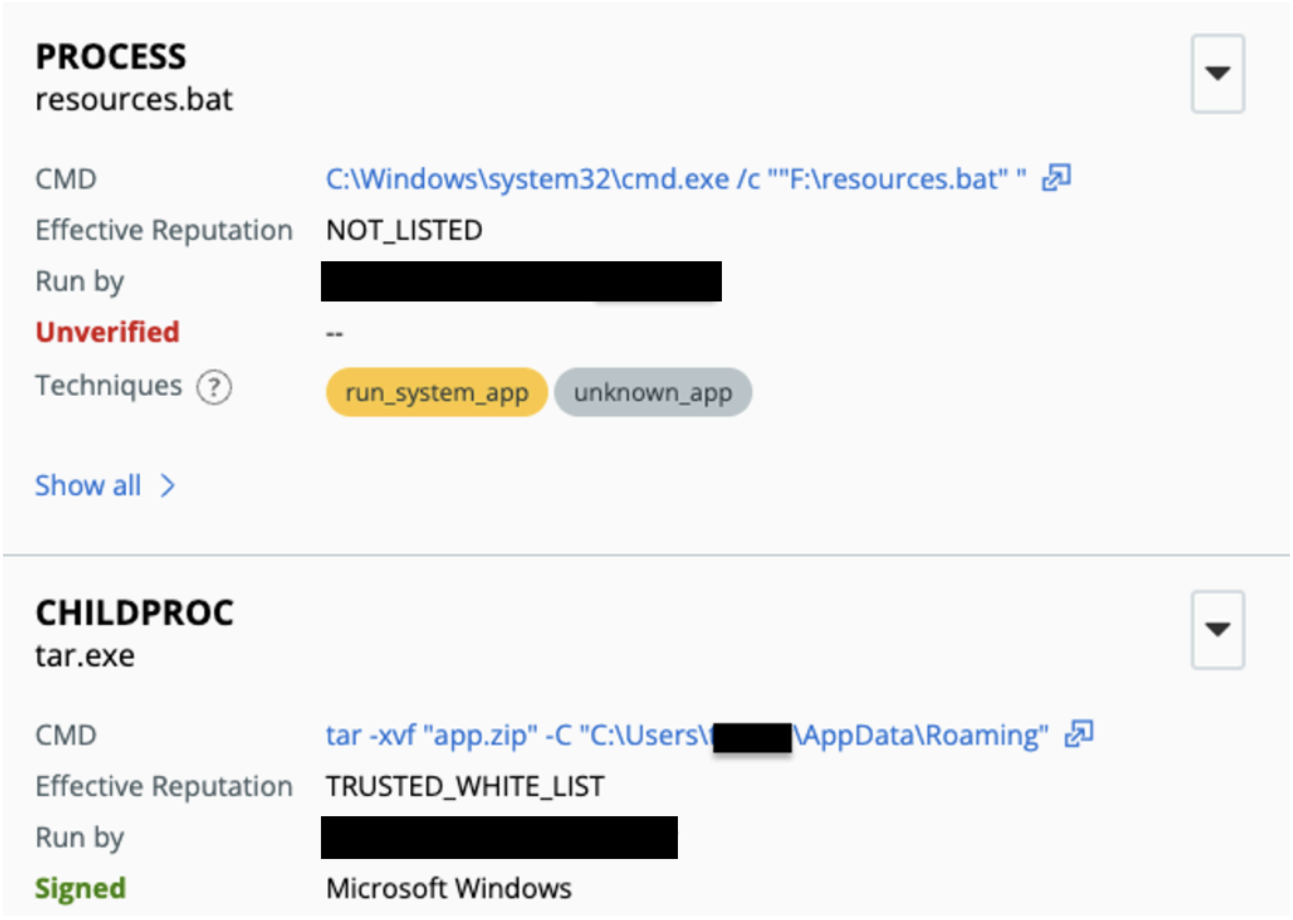
In a ChromeLoader infection, malware authors offer pirated or cracked versions of games or software. They typically distribute this software on social media platforms, through torrents, on pirating sites, or bundled with legitimate games and software. When the victim installs this malicious file, they unknowingly download an ISO file that contains Chromeloader and oftentimes other malware. This Optimal Disk Image file is unable to do any harm to the machine until the victim double-clicks on the ISO and runs the Install shortcut. The user is likely to open this file, thinking it's a legitimate game download.

Attack Chain

The disk image is mounted as a virtual CD-ROM disk, with contents similar to the graphic below:



Once the Install shortcut is double-clicked, resources.bat executes the command: tar -xvf "app.zip" -C, extracting the contents of app.zip into "C:\Users\UserName\AppData\Roaming".



An executable is then dropped onto the user's device. In this case **bloom.exe** is the executable.

Other variants are listed below:

- **Cash.exe**
- **Flbmusic.exe**
- **Opensubtitles-uploader.exe**
- **Diet.exe**
- **Healthy.exe**
- **Strength.exe**
- **Shape.exe**
- **Energy.exe**
- **Bloom.exe**
- **Tone.exe**

```
tar -xvf "files.zip" -C "%APPDATA%"
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v flbmusic /f
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v flbmusic /t REG_SZ /d "%APPDATA%\flbmusic\flbmusic.exe "nHYhjs"" /f
start /d "%APPDATA%\flbmusic" flbmusic.exe "rlVcuMh"
```

Embedded within the **bloom.exe** binary is **nw.exe** – a software component of **nw.js**. The script **nw.js** allows developers to write native applications in HTML and JavaScript, and further allows Node.js modules to be called directly from the Document Object Model (DOM). Its name stands for Node-Webkit and was built upon

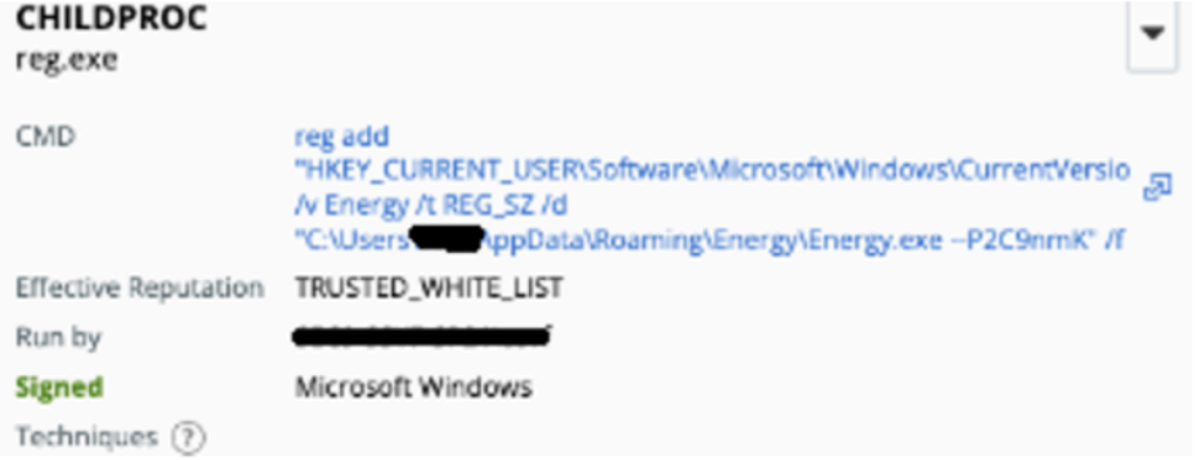
Chromium/node.js which provides application runtime to allow the executable to make successful external network connections to malicious websites.

Instances of this malware also use scheduled tasks for persistence. A list of task names used include:

$tsn = @(“chrome window”,”chrome panel”, “chrome tab”, “chrome view”, “chrome cast”, “chrome history”, “chrome flags”, “chrome bookmarks”, “chrome conf”, “chrome storage”, “chrome tools”, “chrome settings”, “chrome support”, “chrome tele”)

The dropped archive bat files (**resources.bat, configuration.bat, properties.bat**) creates a RUN key to persist the malware. It does this by unzipping various .DLL’s that are then extracted into the \AppData\Roaming folder and adding registry keys as seen below:

- reg add “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run” /v Bloom /t REG_SZ /d “C:\Users*\AppData\Roaming\Bloom\Bloom.exe –qyS7” /f



These dropped executable files were also seen attempting to harvest browser credentials.

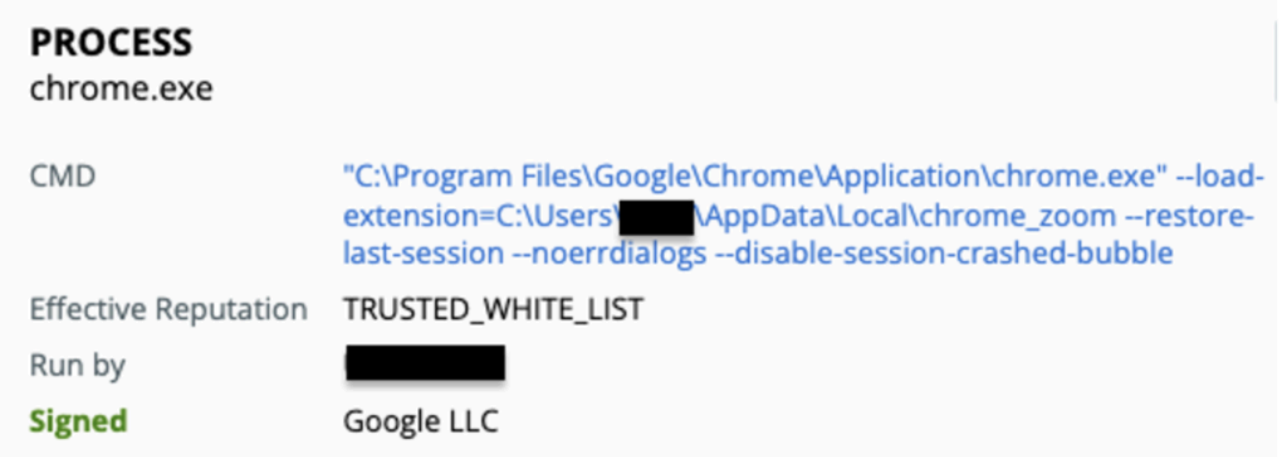
The adware eventually executes a base64 encoded powershell script that creates and writes encoded text in the registry. Some examples of the registry keys we’ve seen being created are:

- HKCU:\Software\LogiShdr\
- HKCU:\Software\Martin Prikyrl\
- HKCU:\Software\SiberSystems\
- HKCU:\Software\aignes\
- HKCU:\Software\BinaryFortressSoftware\
- HKCU:\Software\AeroTechnologies\
- HKCU:\Software\LightScribe\
- HKCU:\Software\ZabaraKatranemiaPlc\

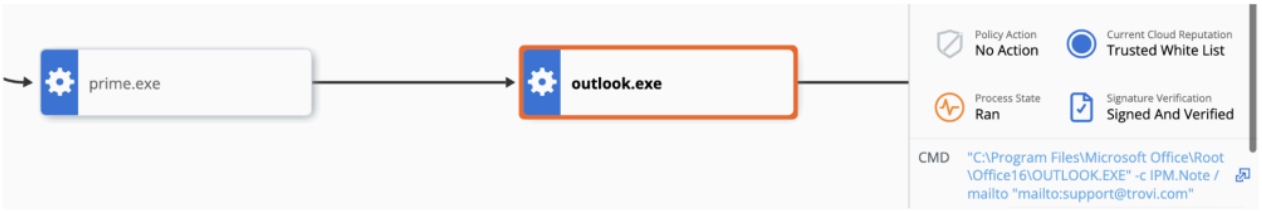
The encoded script written to this location is executed at set intervals, making network connection to suspect domains such as:

- oughsheukwa[.]autos
- ukizeiasnin[.]com
- lyrecomemu[.]xyz
- tooblycars[.]com
- texceededon[.]autos
- ymenthejuiasq[.]xyz
- koooblycar[.]com
- rooblimyooki[.]com
- Yooblygoobnku[.]com
- ringhereny.autos

Soon after this powershell command is ran, the malware attempts to load the chrome extension chrome_zoom as seen in the screenshot below:



We have also seen evidence of the executables (**prime.exe, bloom.exe**, etc) then spawn **outlook.exe** to be used for data exfiltration as seen in the example below.

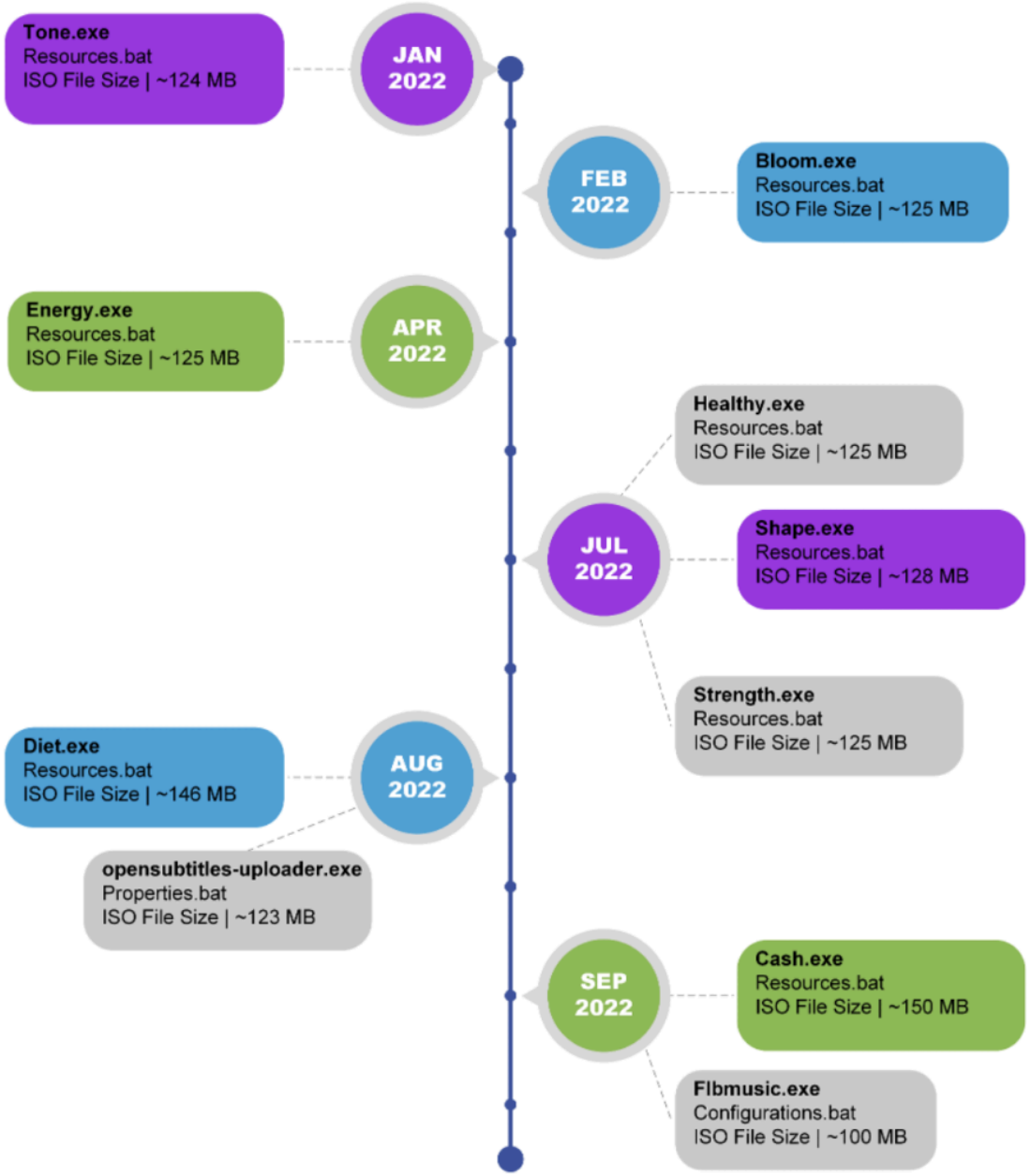


Evolution Timeline

Tone.exe was first seen in the wild at the end of January 2022. This was one of the first evolutions of ChromeLoader and is mentioned in an article from Palo Alto Networks Unit 42 as Variant 2.

Following the spread of **Tone.exe** the VMware Carbon Black MDR team saw **bloom.exe** make an appearance in customer environments, beginning March 2022. The .iso file the user downloads contains the batch script, **resources.bat**, which unzips the file **bloom.exe**. This executable is seen making external network connections and exfiltrating sensitive data.

Since the release of the Bloom variant there have been numerous new Chromeloader renditions that follow the same attack chain and use different process names and hashes to avoid detection. Below is a chart showing the date each variant was first detected in our customers' environments and some of the naming conventions that were used with each variant.



Notable Variants

Opensubtitles-uploader.exe

This variant drops **properties.bat** instead of the previously seen **resources.bat**. In the ISO archive, there is an executable named **opensubtitles-uploader.exe**. OpenSubtitles is a legitimate program that helps users find subtitles for popular movies and TV shows, however, in this case, the malware author is impersonating the software by using the same name. This executable is used in conjunction with this adware program and redirects web traffic, steals credentials, and recommends other malicious downloads posed as legitimate updates.

Similar to previous variants, tar is used to unzip the archive **files.zip** to the AppData\Roaming directory, followed by **properties.bat** adding run keys to the registry for persistence. OpenSubtitles is also masquerading as the file **nw.exe** which is used in order to run JavaScript and HTML programs.

The most recent Chromeloader variants are commonly unknown and don't appear to be malicious at a glance. The VMware CarbonBlack MDR team has become accustomed to identifying the new chromeloader IOC's and can stop the attack quickly.

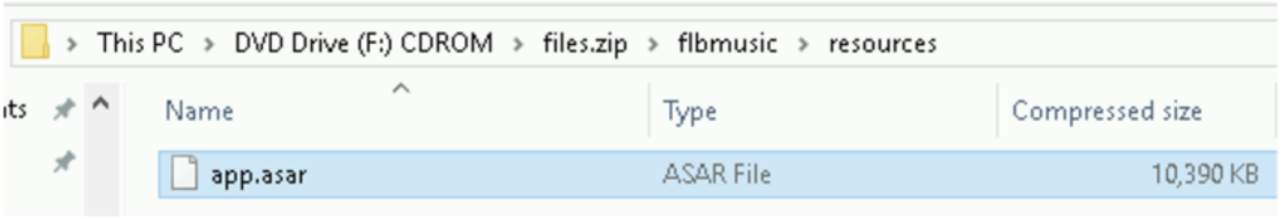
Flbmusic.exe

This variant is typically dropped on Windows systems. This **configurations.bat** file unzips the folder named **files.zip** which contains the executable **flbmusic.exe** and other various libraries and files. Soon after, **flbmusic.exe** is then added to the \CurrentVersion\Run for persistence, followed by the executable being started.

FLB Music

Flbmusic.exe is a legitimate program for cross platform music playing. However, the malware author is impersonating this software. This program contains **electron.exe.pdb** which is a portable database used in debugging configurations for Electron.

Very similar to Chromeloaders previous versions using NW.js, Electron is a runtime that allows you to create desktop applications with HTML5, CSS, and JavaScript. By embedding Chromium and Node.js into its binary, Electron allows attackers to load in modules that allow these applications to listen on specified ports and communicate over the network.



Electron requires you to package your app before distributing, which contains the applications' unprotected source code. This makes it possible for application X to extract application Y and inject vulnerable scripts, without the victim knowing it.

Evidence of Attack Escalation and Module Loading

While thought to be just a credential stealing browser hijacker, ChromeLoader has been seen in its newest variants to be delivering more malicious malware and used for other nefarious purposes.

As recent as late August, ZipBombs have been seen being dropped onto infected systems. The ZipBomb is dropped with the initial infection in the archive the user downloads. The user must double-click for the ZipBomb to run. Once run, the malware destroys the user's system by overloading it with data. The ZipBomb, seen in ChromeLoader archives, is the classic and sophisticated – **42.zip**, which is 42 kilobytes in size when compressed but over 40 petabytes when decompressed. This file has been seen under the names **vir.exe, very_fun_game.zip, passwords.zip, AzizGame (1).zip, nudes.zip, unreleased_songs.zip, FreeNitro.zip, jaws2018crack.zip**.

Another malware included in the archive the user downloads is Enigma Ransomware. This attack has also been seen as recent as late August 2022. It is distributed in HTML attachments found in the archive. When the attachment is opened, it will launch the default browser, execute its embedded javascript, and then follow its standard chain. Names that have been seen in this attack include **REG-archive.zip** and **KeyFILE-Generator_protected.exe**. The malware will typically drop its ransom note as r**eadme.txt**.

Another part of the infection seen is that in some cases, the attacker uses their installation servers to download and install unsecured versions of Windows. The URLs seen include:

- hXXp://ctldl[.]windowsupdate[.]com/msdownload/update/v3/static/trustedr/en/disallowedcertstl[.]cab
- hXXp://ctldl[.]windowsupdate[.]com/msdownload/update/v3/static/trustedr/en/authrootstl[.]cab

More information on this can be found at Microsoft's website.

Another software seen in the .bat downloaded by the user is Utorrent. It is often named after cracks, movies, video games, or wallpapers.

Some names seen include:

- **wild.eight.v0.6.19.multi.8.cracked3dm.torrent**
- **need for speed rivals crack v3 updated december zip**
- **mechanic.simulator.2018.update.v1.0.4bat.torrent**
- **Vector magic desktop edition 1.15 product key**
- **Need for speed most wanted (2005 video game) download**
- **evangile.w.happiness.steam.edition.rar**
- **creed.originsfull.unlocked.part03.rar**

While Utorrent itself is just a BitTorrent client for Windows, it often comes bundled with other malware that the user chooses to accept to install when asked if they accept the EULA. Utorrent will also install the unsecured versions of Windows that have been mentioned previously.

Carbon Black Detection

Our skilled MDR analysts continuously hunt for prevalent and active threats in our customers' environments. Thus far we have found 50+ infected organizations that use our services. VMware Carbon Black products prove to be very reliable when detecting and alerting on malicious behavior generated by chromeloader, our sensors pick up behaviors that many other other security vendors can't.

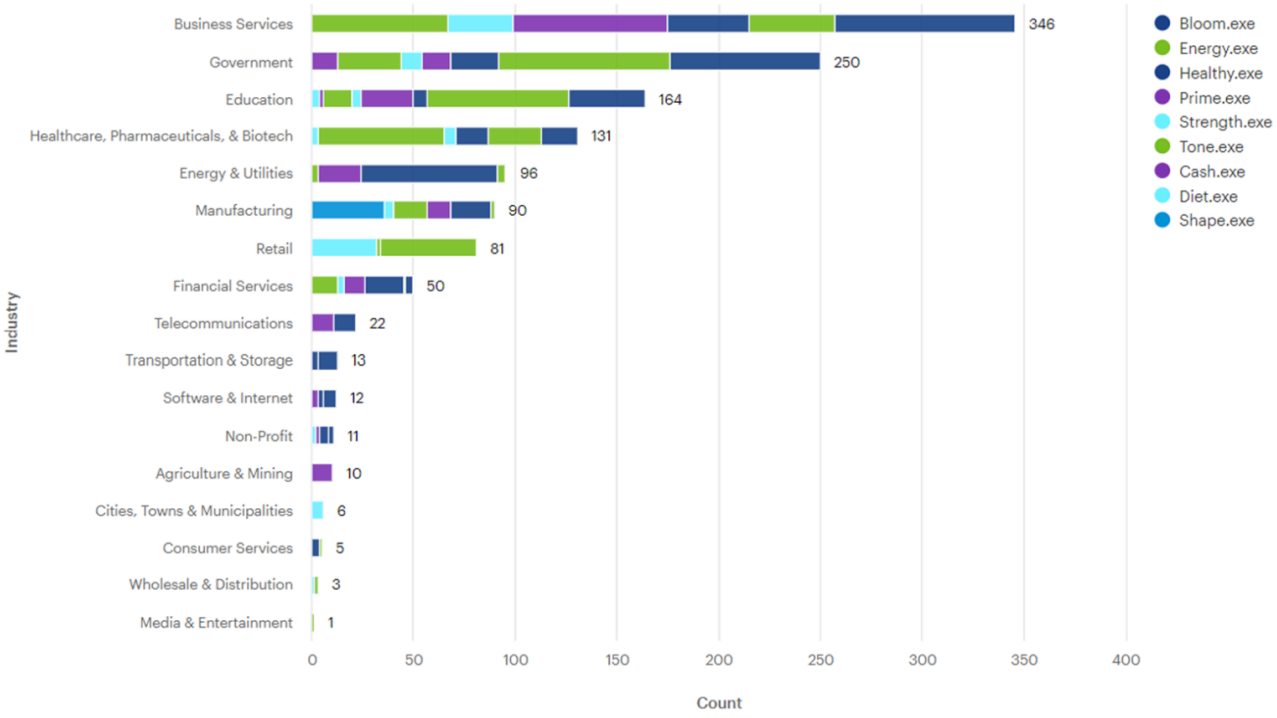
Since the behaviors and tactics of this malware have changed so frequently, the majority of current IOC's such as file hashes and C2 IPs become unreliable indicators of infection. Our MDR analysts are highly trained to pick out malicious behavior. Using data generated from recent attacks seen in other organizations the team is able to quickly confirm malicious behaviors and contain the threat. MDR continues to prove that human expertise is extremely valuable to contain threats and respond in a timely manner.

9:52:52 am Aug 30, 2022 [redacted] User [redacted] added Reputation Override for Organization ID 4620 of type SHA256 to BLACK_LIST with content: 864e41e08c741f440d9335cb08da8e810daf7a96856ccef7de385c2557b84ca9 | tone.exe

Summary

It's no surprise that this pesky adware has been one of our most frequent attacks. This campaign has gone through many changes over the past few months, and we don't expect it to stop.

The VMware Carbon Black MDR team is highly efficient at detecting this threat and has found that of over 50+ customers, the majority of the infected are with the business services industry, seconded by government.



In the picture above we have broken down the attack prevalence across industries and how each industry is impacted by the different executables of ChromeLoader. The majority of cases we are seeing are linked to Bloom.exe, followed by Energy.exe. It is imperative that these industries take note of the prevalence of this attack and prepare to respond to it, because as seen above ChromeLoader can lead to nastier infections.

As we've seen in previous Chromeloader infections, this campaign widely leverages **powershell.exe** and is likely to lead to more sophisticated attacks. The Carbon Black MDR team believes this is an emerging threat that needs to be tracked and taken seriously due to its potential for delivering more nefarious malware. It has been seen before that adware is waved off as just being a nuisance malware, however because of this, malware authors are able to take advantage and use it for wider attacks like Enigma ransomware.

It's important to track all threats in an environment. VMware's Carbon Black MDR team makes this possible by tracking and responding to the threats for you and your environment.
