Gamers, get ready: scammers disguise cryptocurrency and password-stealing Scavenger trojans as cheats and mods

Published: 2025-07-24 · Archived: 2026-04-05 13:34:45 UTC

July 24, 2025

Doctor Web's virus laboratory has detected Trojan.Scavenger—a family of malicious apps that threat actors use to steal confidential data from crypto wallets and password managers from Windows users. Threat actors chain together several trojans from this family, exploiting DLL Search Order Hijacking vulnerabilities to execute their payloads and exfiltrate data.

Introduction

In 2024, the company Doctor Web investigated an information security incident, involving an attempt to carry out a targeted attack on a Russian enterprise. The attack's scheme included using malware that exploited the DLL Search Order Hijacking vulnerability in a popular web browser. When Windows applications launch, they search —in different locations and in a certain sequence—for all the libraries they need to operate properly. To "trick" the apps, attackers place malicious DLL files where they will be searched for first, such as in the installation directory of the target software. At the same time, the threat actors give their trojan files the names of legitimate libraries located in directories that have a lesser search priority. As a result, when launched, vulnerable apps will load malicious DLL files first. These trojan libraries operate as part of the apps and get the same permissions.

Following the incident in question, our specialists implemented functionality in Dr.Web anti-virus products that make it possible to track and prevent attempts to exploit DLL Search Order Hijacking vulnerabilities. While analyzing the telemetry data of this feature, Doctor Web's virus analysts detected attempts to download previously unknown malware into several browsers of our clients. Our investigation into these cases allowed us to uncover a new hacker campaign, which is the subject of this article.

Trojan.Scavenger malicious programs infect computers in several stages and an infection starts with downloader trojans getting into the target systems in various ways. Our specialists detected two chains of this campaign with a different number of trojan components involved.

Chain of three loaders

In this chain, the starting component is **Trojan.Scavenger.1**, malware representing a dynamic library (a DLL file). It can be distributed via torrents and game-related sites either as part of pirated games or under the guise of different patches, cheats, and mods. Next, we will look at an example where scammers passed off the trojan as a patch.

Trojan.Scavenger.1 is distributed in a ZIP archive along with installation instructions in which fraudsters encourage their potential victim to place the "patch" into the Oblivion Remastered game directory—allegedly to improve its performance:

```
 Drag umpdc.dll and engine.ini to the game folder:
\steamapps\common\Oblivion Remastered\OblivionRemastered\Binaries\Win64

Engine.ini will automatically be loaded by the module.
The module will also apply some native patches to improve performance
```

The name of the malicious file was chosen by the attackers deliberately, as a legitimate file with the name umpdc.dll is located in the Windows system directory %WINDIR%\System32. It is part of a graphic API used by various programs, including games. If the victim's version of the game has an unpatched vulnerability, the copied trojan file will automatically be launched along with it. It is worth noting that the version of the Oblivion Remastered game, relevant at the time of the study, was correctly handling the library search order for the file umpdc.dll; for this reason, in the example in question, **Trojan.Scavenger.1** could not automatically start with the game and continue the infection chain.

When successfully launched, the trojan downloads from a remote server and launches the next stage, which is the malicious downloader **Trojan.Scavenger.2** (tmp6FC15.dll). In turn, this trojan downloads and installs other modules from this family into the system—**Trojan.Scavenger.3** and **Trojan.Scavenger.4**.

Trojan.Scavenger.3 represents a dynamic library version.dll that is copied into the directory of one of the target browsers based on the Chromium engine. This file has the same name as one of the system libraries from the directory %WINDIR%\System32. Browsers vulnerable to DLL Search Order Hijacking do not check where the library with such a name is loaded from. And since the trojan file is located in their catalog, it has priority over the legitimate system library and is loaded first. Our virus analysts detected attempts to exploit this vulnerability in the browsers Google Chrome, Microsoft Edge, Yandex Browser, and Opera.

When launched, **Trojan.Scavenger.3** disables the target browser's protective mechanisms, such as the mechanism that launches its sandbox, causing the JavaScript code to be executed in the primary memory space. Moreover, the trojan disables the verification of browser extensions. To do so, it determines where the corresponding Chromium library is by the presence of the export function CrashForExceptionInNonABICompliantCodeRange in it. Next, it searches for the extension verification procedure in this library and patches it.

After that, the trojan modifies the target extensions installed in the browser, receiving necessary modifications in the form of JavaScript code from the C2 server. The following extensions are being modified:

- crypto wallets
  - Phantom
  - Slush
  - MetaMask
- password managers
  - Bitwarden
  - LastPass

In this case, it is not the originals that are modified, but the copies that the trojan placed in the directory %TEMP%/ServiceWorkerCache in advance. And to make the browser "pick up" the modified extensions,

Trojan.Scavenger.3 hooks the functions CreateFileW and GetFileAttributesExW by substituting the local paths to the original files with paths to the modifications (Dr.Web detects the latter as **Trojan.Scavenger.5**).

The modifications themselves are presented in two variants:

- a time stamp is added to the Cookie;
- a routine for sending user data to the C2 server is added.

The attackers obtain mnemonic phrases from Phantom, Slush, and MetaMask crypto wallets. They also receive the authorization Cookie and user-added passwords from the password managers Bitwarden and LastPass, respectively.

In turn, **Trojan.Scavenger.4** (profapi.dll) is copied to the directory containing the installed Exodus crypto wallet. The trojan is launched automatically with this app, also by exploiting the DLL Search Order Hijacking vulnerability in it (the legitimate system library profapi.dll is located in the directory %WINDIR%\System32, but due to the vulnerability, the loading priority is given to the trojan file when the wallet is launched).

After it starts up, **Trojan.Scavenger.4** hooks the function v8::String::NewFromUtf8 from the V8 engine responsible for working with JavaScript and WebAssembly. With its help, the malicious app can obtain various user data. In the case of the Exodus program, the trojan searches for the JSON that has the key passphrase and reads its value. As a result, it gets the user's mnemonic phrase that can be used to decrypt or generate a new private key for the victim's crypto wallet. Next, the trojan locates the private key seed.seco from the crypto wallet, reads its, and sends it to the C2 server together with the mnemonic phrase it obtained earlier.

Chain of two loaders

In general, this chain is identical to the first one. However, instead of **Trojan.Scavenger.1**, the distributed archives with the "patches" and "cheats" for games contain a modified version of **Trojan.Scavenger.2**. It is presented not as a DLL file but as a file with the extension .ASI (this is actually a dynamic library with a changed extension).

The archive also comes with installation instructions:

```
Copy BOTH the Enhanced Nave Trainer folder and "Enhanced Native Trainer.asi" to the same folder as the scriptho
```

After the user copies the file to the specified directory, it will automatically run when the target game is launched, as it will accept it as its own plugin. From this point on, the infection chain repeats the steps from the first variant.

The family's common features

Most of this family's trojans have a number of common features. One of them is the standard procedure for verifying the running environment to detect a virtual machine or debug mode. If trojans detect signs that they are being launched in a virtual environment, they stop working.

Another common attribute of the family is the general algorithm for communicating with the C2 server. To connect to it, trojans go through the procedure of creating an encryption key and verifying the encryption. This involves sending two requests. The first one is needed to receive part of the key that is used for encrypting some parameters and data in certain requests. The second request is executed to check the key and contains some parameters, including a randomly generated string, the current time, and the encrypted time value. The C2 server responds to this request with the string it received earlier. All consecutive requests have time parameters, and if they are missing, the server will refuse to establish the connection.

For detailed technical descriptions of the malicious programs detected, please refer to the PDF version of the study or visit the Doctor Web virus library.

More about **Trojan.Scavenger.1**

More about **Trojan.Scavenger.2**

More about **Trojan.Scavenger.3**

More about **Trojan.Scavenger.4**

More about **Trojan.Scavenger.5**

Conclusion

We notified the developers whose software was exploited via the security flaws we detected, but they deemed the DLL Search Order Hijacking vulnerabilities as not requiring a fix. However, the protection against this type of attacks that we added to our Dr.Web anti-virus products successfully counteracted the exploitation of vulnerabilities in the affected browsers even before we learned about the **Trojan.Scavenger** malware family. Because of that, these trojans did not pose a threat to our users. And as part of this study, we also added the corresponding protection for the Exodus crypto wallet app.

Indicators of compromise
