Chrome Extensions Steal Roblox Currency, Uses Discord

blog.trendmicro.com/trendlabs-security-intelligence/malicous-chrome-extensions-stealing-roblox-game-currency-sending-cookies-via-discord/

August 24, 2017

Cyber Threats

We discussed how threat actors use the voice/chat client Discord to steal cookies from the running Roblox process on a Windows PC. Since then, we've noticed another attack going after the same information, only this time it is via Chrome extensions.

By: Stephen Hilt, Lord Alfred Remorin August 24, 2017 Read time: (words)

We recently discussed how cyber criminals are using the popular voice/chat client Discord to steal cookies from the running Roblox process on a Windows PC. Since then, we've noticed another attack going after the same information, only this time it is via Chrome extensions (CRX files).

While it currently only targets Roblox users, the same technique can be used to steal cookies from any website. The stolen information is sent via Discord, but this could also be configured to use other chat platforms. We learned this particular Chrome extension was, in fact, for sale on the Dream Market underground marketplace for only 99 cents:

Figure 1. Roblox Trade Bot being sold on the "Dream Market" underground marketplace (Click to enlarge)

We obtained samples of this bot using the following file names: *ROBLOX BOT.zip*, *Crm5extension.crx*, *Roblox Enhancer.crx*, and *DankTrades.zip*. The first .ZIP file contains a file named *bgWork.js.*

Figure 2. ZIP file contents

Searching for the terms *CRM5* or *bgWork.js* lead right back to the forum *v3rmillion.net*. This underground marketplace forum is a hotspot for Roblox hacks, where users even trade ROBUX (the in-game currency of Roblox) for other work or products.

Looking into *bgWork.js,* there is a configured Discord webhook that sends out the stolen Roblox cookie via the Discord API when installed. In this case, the example shows that the extension is called a Trade Bot and claims to be a RAP (Recent Average Price) Value assistant that can help you trade your ROBUX for something else. This extension doesn't do that; it will only send a stolen cookie to a Discord channel, leaving the user with nothing in return.

Figure 3. Title and message of the malicious extension (Click to enlarge)

bgWork.js will send the message via Discord using a predefined webhook, which could also be changed to use any of the other chat platforms discussed in our paper titled *How New Chat Platforms Can Be Abused by Cybercriminals*.

Figure 4. Code sending stolen cookie via Discord (Click to enlarge)

The extension also sets up an alarm that will trigger an event every 15 minutes. This event will send the stolen cookie (again) through the Discord API. These alarms ensure that the updated cookie is constantly uploaded to the attacker.

Figure 5. Alarm set for every 15 minutes

At the beginning of the *bgWork.js* file (where the variables are configured), the attacker can change their webhook URL, or the cookie they want to steal. This means that this could be used to steal *any* cookie that is in the web browser; this capability is new to this version.

Figure 6. Code for configuring cookie to steal and Discord API (Click to enlarge)

Because CRX files are just ZIP files with a different extension, the malware can be easily reconfigured to steal the cookies from any website besides Roblox. Changing the extension's *manifest.json* file will allow for its properties to be changed (such as its name and description), making it more likely for an unsuspecting user to fall victim to this attack.

Figure 7. manifest.json file of Chrome extension (Click to enlarge)

Unless a user looks into the extension's code, it looks benign. It may run for a long period of time, allowing an attacker to steal ROBUX repeatedly if the victim keeps purchasing or acquiring new ROBUX. All it takes is one time running the extension for the ROBUX cookie to be stolen and sent to the actor.

Figure 8. Roblox Trade Assist extension installed in Google Chrome (Click to enlarge)

The extension sends the Roblox cookie to a Discord channel like the previous malware, as seen below. We modified the code to send it to a Discord channel of our choice:

Figure 9. Cookies sent to Discord (Click to enlarge)

Unlike previous versions of Roblox cookie stealers like TSPY_RAPID.A and TSPY_RAPID.D that were compiled using C#, this particular malware will also work on Macintosh computers.

Figure 10. Roblox Trade Assist extension installed in Google Chrome on an OS X system (Click to enlarge)

The version we found required the user to manually install the extension into his Chrome browser, which required Developer Mode to be turned on. We wondered if any of these trade bots made it into the official Chrome web store, and found that they did:

Figure 11. Roblox Trade Bot extensions in the Chrome web store (Click to enlarge)

Checking the reviews for these add-ons, we saw that some users complained that these were stealing ROBUX. One reviewer even stated it steals the whole Roblox account.

Figure 12. Reviews of Roblox Trade Bot (Click to enlarge)

We looked at all the Roblox trade bots that were listed in the web store, and found that all of these were malicious; they would send your cookies to a remote Discord webhook. One of them, once installed, even shares the same icon as the malicious extension that was discussed earlier.

Figure 13. Malicious Chrome extension with TRADE icon (Click to enlarge)

This shows that even extensions inside the Chrome web store can be malicious and steal ROBUX from user accounts.

Figure 14. Contents of ROBLAX Trade/Snipe BOT extension's bgwork.js file (Click to enlarge)

This is a good time to remember to always verify the permissions required before installing any Chrome extension. If you are unsure about these permissions, it's better to not install the extension in the first place. This particular malicious extension requires the "Read and change all your data on the websites you visit" permission, which should be a hint of its malicious behavior.

Figure 15. ROBLOX Trade/Snipe BOT Permissions

Anyone who has downloaded one of these extensions should delete this extension from their browser. This can be done via the Extension Manager within Chrome; Google provides step-by-step directions on how to do so here.

Trend Micro detects these malicious extensions as BREX_CUKIEGRAB.SM. We have already reported these extensions to Google; as of this time they have not yet removed them.

The following SHA-256 hashes are associated with this threat:

- 0061a5f52c5b577f679e81da3ab3ad3803c20e345c16ffc4dbc8b76386d42a00
- 4c4af30a94cd25b23579e12b64191a056bda3c51b6e531a2202d3863b19432b3
- d9f21e401ef0197a2af66133e3f7fc3a4ea3efb4437884a4383076bad4060b02