Home › News › Security › Discord Abused to Spread Malware and Harvest Stolen Data

Discord Abused to Spread Malware and Harvest Stolen Data

By **Lawrence Abrams** October 31, 2019 03:17 PM **0**

Malware developers and attackers are abusing the Discord chat service by using it to host their malware, act as command and control servers, or by modifying the chat client to perform malicious behavior.

As security companies shore up defenses against malware distribution and communication methods, malware developers and cyber threat actors have to evolve their tactics by abusing other services.

Such is the case with the Discord chat service, which has been abused by malware developers for years.

Below we take a look at three ways that Discord is being used; as a malware hosting and distribution service, a malware communications server, and through client modifications.

Discord as a malware hosting and distribution service

While Discord is designed as a chat service, it allows members to upload files to a chat channel so that others can download them.

Users can then right-click on an uploaded file and select the "Copy link" option to get a URL that can be shared with others, even non-Discord users, in order to download the file.

Copy link of uploaded file

For example, in the image above I uploaded the Windows Calculator (calc.exe) and copied its public link of https://cdn.discordapp.com/attachments/636608706401927172/639502346656677914/calc.exe. As you can see this file is hosted on Discord's CDN, but can be shared with anyone.

What's even more interesting is that the uploader can delete that file within the Discord, but the URL can still be used to download the file. This means that even though the file is deleted in the chat, it is not actually deleted from the Discord CDN.

This feature is being used by malware developers as an easy and anonymous way to distribute infections. In just a brief glance on VirusTotal, malware such as the NanoCore RAT, screenlockers, keyloggers, and Roblox cookie stealers, to just name a few, are being distributed in this way.

While Discord sometimes displays warnings at download pages when malicious files are reported, in our tests most malicious downloads are not flagged.

The good news is that Discord does perform some sort of file scanning or blocking of malicious files, as when I tried to upload a sample of the DarkComet RAT found by JayTHL with 65 detections on VirusTotal, Discord would not allow the file to be uploaded.

Discord blocking an upload

With that said, that file is already present on Discord to this day. This means that they do not scan previously uploaded files on their CDN to take advantage of updated virus definitions or known malware.

Discord webhooks being used as stolen data drops

Discord contains a feature called webhooks that allows websites or external applications to send messages to a Discord channel.

When creating webhooks, the server owner will be given a special URL that is used with the Discord API to send messages to the specified channel.

Creating a webhook

Like all useful features, developers of malware such as ransomware, information-stealing Trojans, RATs, and more can abuse webhooks to send information to the attacker when a user is infected.

For example, this information stealer will attempt to steal a victim's saved login credentials from Chrome, Firefox, and Opera and the victim's Discord user token.

Stealing saved logins and Discord tokens

It then sends this compiled information to the attacker using these Discord webhooks.

Command & Control Webhooks

This feature is also commonly used by malware that steals victim's Discord tokens, which can then be used by the attacker to login as that particular Discord user.

MalwareHunterTeam also found an example of an NPM package that was using webhooks to steal Discord user tokens.

Discord client files can easily be modified

If you are a reader of BleepingComputer then you may have read our story about a recent malware discovered by MalwareHunterTeam that modifies the JavaScript files of the Discord client to perform malicious behavior.

As the Discord client makes its JavaScript files modifiable by the user, any malware that runs as the user can also modify these files.

File permissions for Discord JavaScript files

When modifying the files, the attacker will add their own JavaScript code to the Discord client files so that it is executed when the client is launched or when particular URLs are opened by the client.

Modified Discord files

This is exactly what happened in a recent malware that modified the Discord JS files in order to steal Discord tokens and other information about the victim and send it to the attacker via a webhook.

What's so devious about this tactic is that even if the malware is removed, the malicious JavaScript will remain in the Discord client and will most likely not be detected by antivirus software. The only way to clean the client, would be to uninstall and reinstall the software.

BleepingComputer has suggested that Discord institute file integrity checks on startup and warn a user if the client files have been modified.

Discord alert mockup

While Discord has stated they will be increasing security in the future, it has not provided a plan on how they are going to do so.

BleepingComputer has reached out to Discord with questions regarding these issues, but has not heard back at this time.

Related Articles:

Office 365 Adds Malware ZAP Toggle to Security & Compliance Center

QSnatch Malware Infects Thousands of NAS Devices, Steals Credentials

xHelper Trojan Variant Reinstalls Itself After Removal, Infects 45K

Android Trojan Infects Tens of Thousands of Devices in 4 Months

Discord Turned Into an Info-Stealing Backdoor by New Malware

CDN DISCORD MALWARE

LAWRENCE ABRAMS

Lawrence Abrams is the creator and owner of BleepingComputer.com. Lawrence's area of expertise includes malware removal and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

PREVIOUS ARTICLE NEXT ARTICLE

Post a Comment

Community Rules

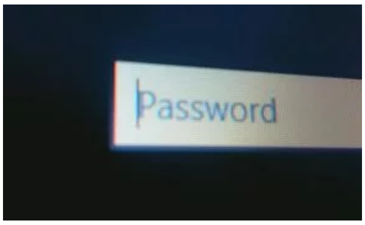
You need to login in order to post a comment

Login

Not a member yet? Register Now

You may also like:

POPULAR STORIES



21 Million Logins for Top 500 Firms Offered on the Dark Web

World's First Domain Registrar Network Solutions Discloses Breach

NEWSLETTER SIGN UP

Email Address...

SUBMIT

Follow us:

MAIN SECTIONS

News

Downloads

Virus Removal Guides

Tutorials

Startup Database

Uninstall Database

File Database

Glossary

COMMUNITY

Forums

Forum Rules

Chat

USEFUL RESOURCES

Welcome Guide

Sitemap

COMPANY

About BleepingComputer

Contact Us

Send us a Tip!

Advertising

Write for BleepingComputer

Social & Feeds

Changelog

Terms of Use - Privacy Policy