> Discord Attacks

> A brief discussion about social engineering attacks in Discord Social Media

---

Published: 04/11/2022
Last Updated: 04/11/2022 - 11:39 am (BRT)
Author: Vinícius Lôbo

Discord is a VOIP/Server Chat Social Media released in may 13, 2015 as an adversary to Teamspeak and Skype. Focused in Gaming Communities and appealing to a great internet public, Discord gained a lot of recognition pretty fast, acquiring a $5M Revenue in 2016 and having 10M Active Users in 2017 [1].

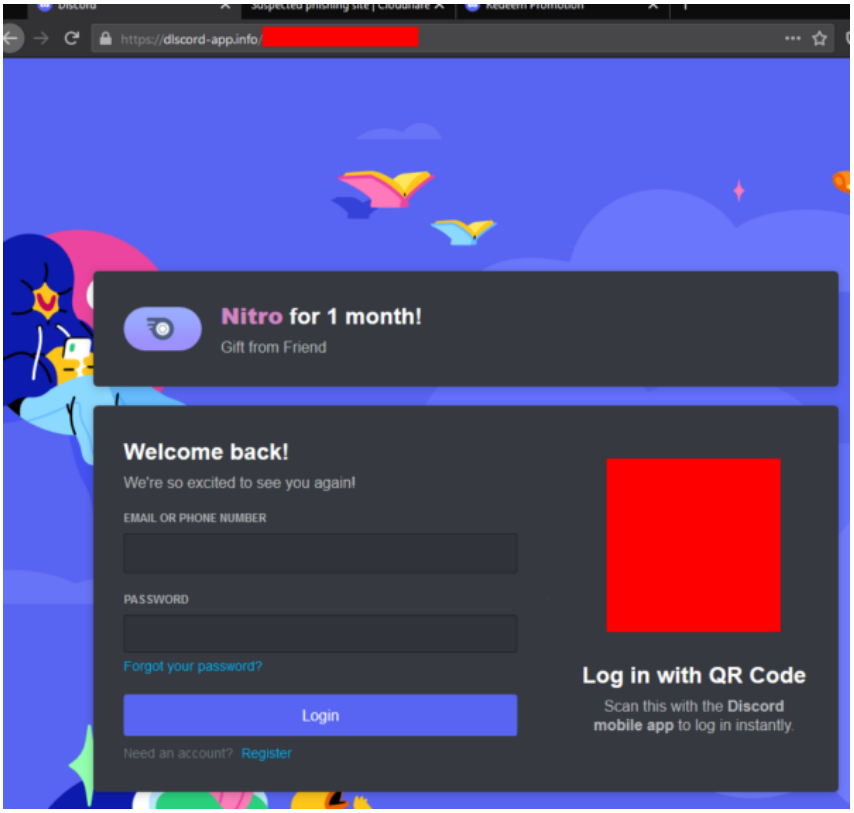
With such popularity gained in these last years, Discord counts with more than 140M Monthly Active Users and has about 13M Weekly Active Servers [2]. And with the COV-19 Pandemic that forced lockdowns all over the world, it impulsonated even more Discord usage, not only by Gaming Communities, but by Students/Schools and Companies as well that started using the App as a Communication Tool (such as Slack).

Although it looks all fun and games, we know that, when an App like this one, that focuses on creating Community Servers, can attract every kind of person, to the CEO's of big companies, to Scammers and Criminals. And considering that as said before, with more people joining, more data available is to be stolen by these Scammers, to leaked addresses that can lead to Doxxing [3], to bank and credit card information, and considering that in 2017 Discord started a Paid Subscription plan (Discord Nitro), scams that look for money just got even more common.

Social Engineering is the greatest weapon used by those criminals that target your data, we are going to go through some of the most common attacks that Scammers utilize to get your account credentials/general Info.

1. Discord Nitro Phishing

The most common attack type, it focuses on tricking the victim into thinking they gained a free subscription of Discord Nitro (a paid subscription that gives your account some features, such as using gif pfp, better screen sharing quality, better audio quality,...) by clicking a link they send them. When the victim clicks the link, they're redirected to a page that looks official and asks you to enter your account credentials. By doing that, you're actually sending your login/password to the scammer, using that to lock you out of your account, and send the same phishing [4] link to your friends/servers.

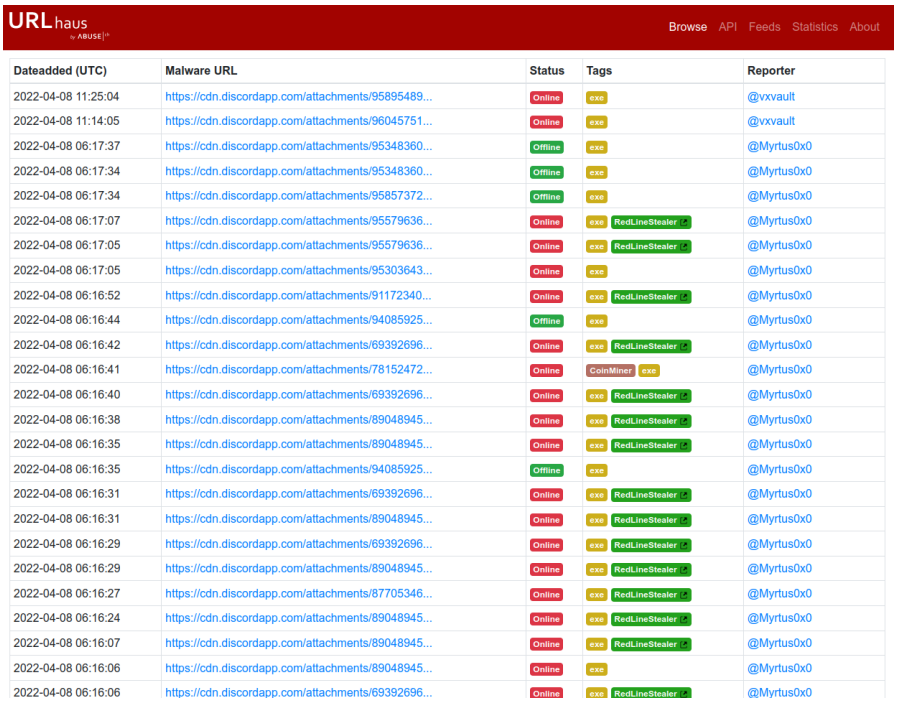


"Example of phishing site used by scammers to trick victims into giving their personal info. If you look closely, you'll see that the "i" in "discord" is actually an "l".

https://blog.malwarebytes.com/scams/2021/10/discord-scammers-lure-victims-with-promise-of-free-nitro-subscriptions/

2. Media Infected Links

A recent and dangerous attack that has taken over Discord, is the Infected Links are masked as media, such as images and videos. In discord, every media sent is archived with a link in their cdn server, and is shown as “cdn.discordapp.com/…”. In recent analysis, it was shown that some links that redirect to images and videos, are actually infected with extremely dangerous malwares, such as Backdoors [5] and RAT’s [6], that when downloaded, execute these malwares stealthily, and some even with Persistence (if you restart your pc, the malware will restart as well as soon as the OS boot up as well).



URLhaus — Browse API Feeds Statistics About

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2022-04-08 11:25:04	https://cdn.discordapp.com/attachments/95895489...	Online	exe	@vxvault
2022-04-08 11:14:05	https://cdn.discordapp.com/attachments/96045751...	Online	exe	@vxvault
2022-04-08 06:17:37	https://cdn.discordapp.com/attachments/95348360...	Offline	exe	@Myrtus0x0
2022-04-08 06:17:34	https://cdn.discordapp.com/attachments/95348360...	Offline	exe	@Myrtus0x0
2022-04-08 06:17:34	https://cdn.discordapp.com/attachments/95857372...	Offline	exe	@Myrtus0x0
2022-04-08 06:17:07	https://cdn.discordapp.com/attachments/95579636...	Online	exe RedLineStealer	@Myrtus0x0
2022-04-08 06:17:05	https://cdn.discordapp.com/attachments/95579636...	Online	exe RedLineStealer	@Myrtus0x0
2022-04-08 06:17:05	https://cdn.discordapp.com/attachments/95303643...	Online	exe	@Myrtus0x0
2022-04-08 06:16:52	https://cdn.discordapp.com/attachments/91172340...	Online	exe RedLineStealer	@Myrtus0x0
2022-04-08 06:16:44	https://cdn.discordapp.com/attachments/94085925...	Offline	exe	@Myrtus0x0
2022-04-08 06:16:42	https://cdn.discordapp.com/attachments/69392696...	Online	exe RedLineStealer	@Myrtus0x0
2022-04-08 06:16:41	https://cdn.discordapp.com/attachments/78152472...	Online	CoinMiner exe	@Myrtus0x0
2022-04-08 06:16:40	https://cdn.discordapp.com/attachments/69392696...	Online	exe RedLineStealer	@Myrtus0x0
2022-04-08 06:16:38	https://cdn.discordapp.com/attachments/89048945...	Online	exe RedLineStealer	@Myrtus0x0
2022-04-08 06:16:35	https://cdn.discordapp.com/attachments/89048945...	Online	exe RedLineStealer	@Myrtus0x0
2022-04-08 06:16:35	https://cdn.discordapp.com/attachments/94085925...	Offline	exe	@Myrtus0x0
2022-04-08 06:16:31	https://cdn.discordapp.com/attachments/69392696...	Online	exe RedLineStealer	@Myrtus0x0
2022-04-08 06:16:31	https://cdn.discordapp.com/attachments/89048945...	Online	exe RedLineStealer	@Myrtus0x0
2022-04-08 06:16:29	https://cdn.discordapp.com/attachments/69392696...	Online	exe RedLineStealer	@Myrtus0x0
2022-04-08 06:16:29	https://cdn.discordapp.com/attachments/89048945...	Online	exe RedLineStealer	@Myrtus0x0
2022-04-08 06:16:27	https://cdn.discordapp.com/attachments/87705346...	Online	exe RedLineStealer	@Myrtus0x0
2022-04-08 06:16:24	https://cdn.discordapp.com/attachments/89048945...	Online	exe RedLineStealer	@Myrtus0x0
2022-04-08 06:16:07	https://cdn.discordapp.com/attachments/89048945...	Online	exe RedLineStealer	@Myrtus0x0
2022-04-08 06:16:06	https://cdn.discordapp.com/attachments/89048945...	Online	exe	@Myrtus0x0
2022-04-08 06:16:06	https://cdn.discordapp.com/attachments/69392696...	Online	exe RedLineStealer	@Myrtus0x0

“Some infected discord links, differently from the phishing scams, the link is actually official, but the media related to that link is infected.

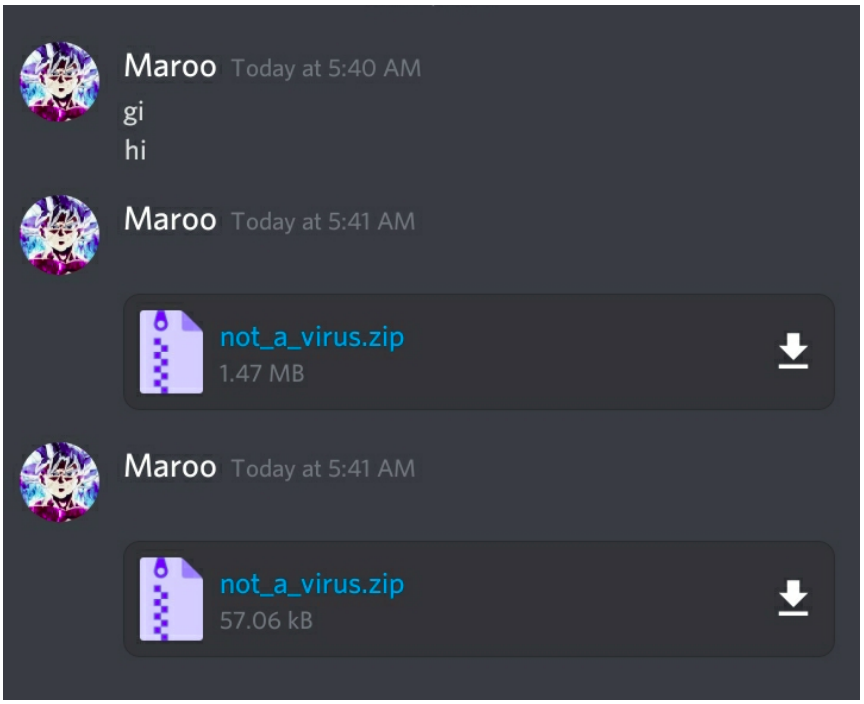
https://urlhaus.abuse.ch/browse.php?search=https%3A%2F%2Fcdn.discordapp.com

3. Fake Giveaways

Closely related to the Nitro phishing scam, this consists of the same technique of tricking the victim into giving personal information believing they've won a giveaway (game key, money, crypto, streaming subscription, …). What makes this attack a bit different from the Nitro ones, is not only the fact that some of these may include more evident (and discord-unrelated) phishing sites, but it can also involve collection of not only Account Information (Login and Password), but Personal Information as well (Full Name, ZIP, Address, Phone, Birth-Date, …), which can lead to Doxxing, and in some more aggressive cases, home invasion and kidnapping.

4. Suspicious Files

Similar to infected links, these attacks involve use of infected files, masked as games or executables in general, that may be used to steal information (Backdoors, Trojans, Spywares) or lock your computer in exchange for money, the feared Ransomware. [7]



"As stupid this looks, it's still a valid danger, as some users fall for it"

https://discord.com/blog/common-scams-what-to-look-out-for

As seen in all of the examples, these attacks share a lot of common similarities, the biggest one being the use of Social Engineering Tactics to spread these attacks. The usage of Phishing, Spoofing, Blackmailing are just a few examples of tactics used by criminals to steal your information.

The best way of protecting yourself is to always make sure you follow this simple security rule: “don’t click links from people you don’t know”. It’s a simple concept but people forget about it, principally when there’s a promise of “gifts” and “rewards”. Although, this concept has flaws, because as we’ve seen, some scammers take control of friends' accounts and act like someone you know. A good way to counter that, is to enter in contact with your friend through other social media and ask if they had an account breach.

Social Engineering is a very powerful weapon, and responsible for the great majority of cyberattacks in the world. But in the same way it’s a very strong attack, it can also be detected and countered easily if you’re paranoid enough. Basically saying, **suspect everything and be suspicious of everyone, even if it’s your friend.** That’s the best way to avoid Social Engineering attacks.

~So long, and thanks for all the fish

[1]https://www.businessofapps.com/data/discord-statistics/
[2]https://backlinko.com/discord-users
[3]https://www.malwarebytes.com/doxxing
[4]https://www.malwarebytes.com/phishing
[5]https://www.malwarebytes.com/backdoor
[6]https://blog.malwarebytes.com/threats/remote-access-trojan-rat/
[7]https://www.malwarebytes.com/ransomware