Research on Discord Malware

Researched by at0m from Cosmodium Cybersecurity

How is this malware delivered?

It all starts from a DM from user *Damianeq93#3538*

Discord ID Lookup Results

Message Screenshot

Once you join in the server you will see advertisements for free cheat ware these ads come link 2 websites where these cheats are hosted: **The links are provided below (please be careful)**

> https://infinitycheatsv2.web.app/

- Screenshot of this website ^ > https://infinitycheats.lol/
- Screenshot of this website ^

Now lets take a look at downloading one of these files . All files are hosted on discord which is a weird spot to host files. Taking a look at one of these cheats we get a lot of hits on Virus Total Take a look at this graph to see how many detection are linked with this zip Screenshot of VT Total Graph

From the File hosted on discord labeled as "Infinity Cheats Loader.zip" we have 2 main files "InfinityCheatsLoader.exe" and "LithiumCore.dll"

Infinity Cheats Loader has contacted 2 domains

1. cdn.discordapp.com (where the file was hosted)
2. t4ck0wsvvpbmktxzluyee11uce27kbct.nl (Some files hosted + additional malware)

Infinity Cheats Loader also drops a malicious file

1. "node.exe" (c7763a056e28d06eeca1405377a3f2c1b291b02c38725aa3d411b814100330d2)

After some additional research this is either BBY stealer or something similar. BBY stealer is a piece of malware that steals things such as chrome login data. We see this behavior when it tries to grab: "%USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Login Data.bby"

It also creates and runs some powershell scripts: "C:\Users\user\Desktop\temp.ps1"

The rest of this behavior can be looked at with the hashes a have provided. Here is a list of some IOCs (Indicator of Compromise) : ZIP = 08a6cfa040119ffb455c061284fb392d50fdc644b37b7ca4e4a8badf2d7a7c70 DLL = 5bf9ce4949e8ab02250c78367c5abb8c0eb22b9beb8362d8ef0b4e710a9192bd EXE = ab740bd78e7fe3bd2f3e4bf22d632fcf576751de53d369acfffafe3f1ec9c516 Domain = t4ck0wsvvpbmktxzluyee11uce27kbct.nl