Discord C2   
(Red Path)

Graphical user interface, text, application

Description automatically generated

Summary

Attack Explains:

Third-Party software as Command and Control (C2) is using some legitimate third-party services such as Gmail, twitter, in this case, Discord to normal, expected traffic to avoid detection. It can communicate with systems under their control within a victim network.

We are going to create a go program ‘DiscordGo’ using discord bot, and upload and execute in the target windows system, in order remotely send commands and control by using discord.

Target Address: 172.26.15.94 Remote Control Software: Discord.

Target System: Windows 10 Malicious file created: windows-agent.exe

Account Compromised: brailee.ogden (windows account). Password: ‘Winter2022’

Tools: OpenVpn, Evil-winrm, Invoke-Snow.ps1, Go language, DiscordGo

Create Proper Discord Bot and Discord Server

Create discord account and go to this link <https://discord.com/developers/applications> to create discord bot. Select OAuth2 to have proper authorization and configuration like below to connect to discord bot.

Graphical user interface, text, application

Description automatically generated

Click bot to in the left column and set up the Bot and copy the bot token.

Graphical user interface, text, application, Teams

Description automatically generated

Go to the Discord and create a Discord Server, and select discord server setting

Graphical user interface, application, Teams

Description automatically generated

Go to the Server Widget and copy the server ID

A screenshot of a computer

Description automatically generated with medium confidence

In the Bot page, select URL Generator and click the administrator privilate.

After that, copy the link on the botton and paste it in the browser.

Text

Description automatically generated

Then you will see this and allow you to add the bot to the server you want.

Graphical user interface, application, Teams

Description automatically generated

Set up DiscordGO and create C2 files.

Download DiscordGo on Github

https://github.com/emmaunel/DiscordGo   
https://github.com/thepcn3rd/DiscordGo

After downloading DiscordGo, configure variables.go file in the Discord/pkg/util

And put the server ID, and Bot Token’s credentials.

Text

Description automatically generated

Go back to DiscordGo main directory and use “make” to compile the files and created C2 files.

Graphical user interface, text

Description automatically generated

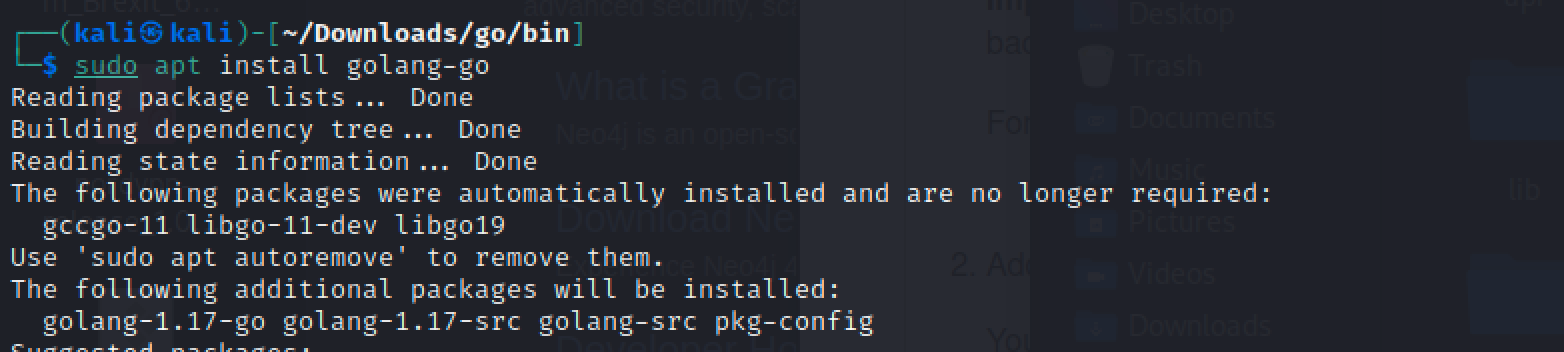
You need to download go program tools by executing the two commands below in order to compile DiscordGo files.

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated



After downloading and installing “go” program tools, then you can execute “make” command to compile the files in DiscordGo

As the result shows below, it compiles successfully. It creates a bin directory and inside of the bin directory has 5 programs, and windows-agent.exe is the file we are going to execute in the windows system.

Text

Description automatically generated

Uploading and Execution of C2 file.

Connect to VPN to hide your identiy and pivot to windows 10 system. Using brailee.ogden’s credentials to gain access.

Execute invoke-snows.ps1 to enable to upload the windows-agent.exe

And rename it to system32.exe. verify after uploading using “dir” command

Text

Description automatically generated

Run the C2 program “system32.exe” using .\

And run “get-process” to see if it is running and connect to discord server successfully.

As it shows it Process ID 206*8 means C2 is working*

Text

Description automatically generated

Check your discord, it shows that windows 10 connect to discord and you can start sending commands and controlling the compromise windows 10 system remotely via the discord bot.

Graphical user interface, text, application

Description automatically generated