Contents

1 Introduction

If you know the enemy and know yourself, you need not fear the result of a hundred battles.

Sun Tzu

To be a good blue team, we should practice red teaming.
WinPeas, Bloodhound

2 Covenant Malware

video
Instructions on their GitHub
Blog Tutorial That blog stinks at telling you how to make a listener Listener
You need GIT and .NET for this to work. You can go to their websites here for windows: https://git-scm.com/download/win https://dotnet.microsoft.com/en-us/download

```
git clone --recurse-submodules https://github.com/cobbr/Covenant
cd Covenant/Covenant
dotnet build
dotnet run
```

"After running these commands, the Covenant service should be up and running. You can then browse to the Covenant application interface on its default web port of 7443 to set up a user account and begin using the framework." -Bing
You should install covenant on your computer, or whatever computer you plan to use as the C2 server. This will let you control the windows machines.
to install .NET on linux: directions
"It looks like Covenant is running, but you may not have permission to start listeners on low-numbered ports because you are running Covenant non-elevated" -Bing

Make sure to go to https://127.0.0.1:7443 and not localhost:7443, the https is important

For the Grunt to work, .NET has to be installed on the victim. It can be installed from the server manager, in the "Features" menu

Anti Grunt countermeasures: "Yes, if you uninstall the .NET Framework 3.5 from the victim machine, it is likely that the Grunt will stop working. Grunts are small programs that are executed on the target machine and communicate with the Covenant server to receive commands and send back results. If the Grunt requires the .NET Framework 3.5 to run, then uninstalling it will prevent the Grunt from functioning properly." -Bing

I think it is very funny that malware has dependencies.

to get your IP address over the VPN

```
ip addr show tun0 | grep inet | awk '{ print $2 }'
```

Yes, if you are using RDP to connect to a virtual machine, the virtual machine should be able to see the IP address of the machine you are connecting from. You can check the IP address of the RDP client by following these steps on the virtual machine:

Open the Command Prompt by pressing the Windows key + R and typing cmd. Type netstat -n — find ":3389" and press Enter. This will display a list of active connections to the RDP port (3389). Look for the connection that corresponds to your RDP session. The IP address of the RDP client will be listed next to the ESTABLISHED entry.

Get a kali box on the range. If you get errors when creating VMs in proxmox, you can view the file /var/log/pve/tasks/index for information

3 Cloudflare Tunnels

Justin mentioned how he was going to connect to the machines using cloudflare tunnels. So I will practice that and document it.

You can use your own domain, or you can have cloudflare provide one for you.

You need to install cloudflared on the machines you are connecting to

So to install on proxmox: wget -q https://github.com/cloudflare/cloudflared/releases/latest/download/cloud linux-amd64.deb && sudo dpkg -i cloudflared-linux-amd64.deb

To do it without a domain: cloudflared tunnel –url http://localhost:80

Take note of the random url generated.

cloudflared access tcp –hostname randomsubdomain.trycloudflare.com –url tcp://localhost:5900

4 Malware to look into

Here is some random stuff so I don't forget to look into it: https://github.com/0x44F/WinKit, https://github.com/D4stiny/spectre, this guy's stuff: https://github.com/DarkCoderSc?tab=repositories,

https://en.wikipedia.org/wiki/DarkComet, (infected file, do not run on main OS): https://github.com/zxo2004/DarkComet-RAT-5.3.1, https://github.com/quasar/Quasar, https://github.com/screetsec/TheFatRat

5 Legitimate Administration Software

https://www.islonline.com/us/en/ https://devolutions.net/remote-desktop-manager/