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.

2 Covenant Malware

Covenant is a .NET command and control framework. It works by installing Grunts on the target machine. Grunts work like reverse shells, they connect to a listener on the C2 server.

You should install covenant on whatever computer you plan to use as the C2 server. This will let you control the windows machines. Covenant requires GIT and .NET to work. You will also need to install .NET on the victim machine.

- Instructions on their GitHub
- Blog Tutorial
- More information on listeners

To install GIT on windows, go here: https://git-scm.com/download/win

To install .NET, you can download it from the website or you can install it in server manager (in the "Features" menu).

To install .NET on linux, follow these directions

After installing the dependencies, we can install and run covenant with:

```
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

If you would like to have listeners on ports 1-1023, you should run Covenant as root.

The web console can be accessed at https://127.0.0.1:7443 and not localhost:7443, as the https is important

For the Grunt to work, .NET has to be installed on the victim.

Anti Grunt countermeasures: "If you uninstall the .NET Framework 3.5 from the victim machine, it is likely that the Grunt will stop working." -Bing. I think it is very funny that malware has dependencies.

2.1 Troubleshooting the VPN

I tried a lot of ways to get the Grunt to recognize my machine. The only solutions that worked are a Kali VM or Cloudflare Tunnels.

To get your IP address from the RDP connection:

1. Open the Command Prompt by pressing the Windows key + R and typing cmd.
2. Type netstat -n — find ":3389" and press Enter. This will display a list of active connections to the RDP port (3389).
3. 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.

Advanced Usage of Covenant

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/clou
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 BloodHound

5 WinPeas

Windows Privilege Escalation Scripts.

This script dumps a bunch of information about potentially interesting things to look for on the windows machine. It can be found here.

6 SMBGhost / EternalDarkness / CVE-2020-0796

https://blog.zecops.com/research/exploiting-smbghost-cve-2020-0796-for-a-local-privilege-escalation-writeup-and-poc/ https://github.com/carbonblack/tau-tools/tree/master/remediation/Ete https://blogs.vmware.com/security/2020/03/threat-analysis-cve-2020-0796-eternaldarkness-ghostsmb.html https://www.cisa.gov/news-events/alerts/2020/06/05/unpatched-microsoft-systems-vulnerable-cve-2020-0796

7 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, https://github.com/DarkCoderSc/win-brute-logon

8 Legitimate Administration Software

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