Reversing Threat Intelligence - Fun with Strings in Malware
Ronnie Tokazowski, Senior Malware Analyst

Hacker of things

@iHeartMalware

I <3 cooking, too

BEC, Crimeware, APT, Trolling
What We’ll Cover

• Deep and Dark Web (more than a buzzword)
• Malware defined
• Strings defined
• Yara, VT, and you
• Programmatically generate Yara sigs
• Closing
What is the Deep & Dark Web?

**Surface Web**
- Crowded social commentary
- News reports
- Opinion pieces
- Mainstream perspectives

**Deep & Dark Web**
- Dialogue between threat actors
- Black market products and services
- Malicious tactics, techniques, and procedures (TTPs)
- Weapons and training manuals
- Illicit community perspectives

**Easy-to-Gather**
Low Signal-to-Noise

**Hard-to-Obtain**
High Signal-to-Noise
What is a Malware?

• If a solution can be sold to protect against it…it’s probably a malware
• Threat, cyber, APT, cloud, synergy, DLP (exfil, yo!), intelligence, ThreatButt, cyber, nextgen, etc.
What are Strings?

• Things reverse engineers use to cheat
• Ways attackers communicate with RE’s
• Places attackers slip-up
• Where we can gain extra insight into malware and authors
Our Tools

- Windows VM
- Notepad++
- Yara
- Sys Internals (dynamic analysis)
- .NET decompilers (muahahaha!)
- XORsearch
Pro-ISIS Tools and Malware

- Pro-ISIS programmer created .NET program for encrypting communications
- Very rudimentary coding
- .NET == sauce. :D
Who is Turgeman Khwarizmi?

- French speaker (based on coding names)
- Named project “Infos Encrypter”
- Install path: C:\Program Files (x86)\Turgeman Khwarizmi\Infos Encrypter – By Turgeman Khwarizmi\
Very Drag and Drop…

- Code analysis shows very “drag and drop” knowledge of coding
- Used for sending letters and messages
- Encryption is RSA, can change the size in TextBox4. Has to be > 4096
• Offers to securely delete files
• Doesn’t account for other forensic artifacts
• Seems to “work” off the cuff, but very buggy. (Crashes if spaces used)
• IoT DDoS malware used for well...DDoS
• Used in many large scale attacks
• Also “accidentally” broke many things
• Originated from the booter / DDoS / HackForum community

• So many red herrings in Mirai … it’s insane

• Attackers use the key “0xdeadbeef”, false flag
By “slamming” the values together, we can identify the XOR key.

This XOR key is used for most variants of Mirai.

Other groups have picked up on the XOR key and changed it.

```
>>> a = \"\x41\x4C\x41\x0C\x41\x4A\x43\x4C\x45\x47\x4F\x47\x0C\x41\x4D\x4F\x22\"
>>> b = \"cnc.changeme.com\"
>>> i = 0
>>> for each in b:
...    print hex(ord(each)^ord(a[i]))
...    i+=1
...
0x22
0x22
0x22
0x22
0x22
0x22
0x22
0x22
0x22
0x22
0x22
0x22
0x22
0x22
0x22
0x22
0x22
0x22
```
But Wait…What is an XOR?

• Bitwise operation
• Can be used for parity
• Cheap on CPU
• Easy way to obfuscate in binaries, shellcode, documents, Rick Roll videos…etc

YOU GET AN XOR
AND YOU GET AN XOR
EVERYONE GETS AN XOR!!!!
• If you XOR data with itself, it’s 0

• If you XOR the key with encrypted data, it’s the decrypted data

• If you XOR “data” 42 times, it’s still “data”

• Multiple passes aren't effective
Guessing Encoded Data

• With knowing the key and decoded data, we can create signatures looking for encoded data
• Good for Mirai samples, word documents, etc.
• Seriously. If you take nothing away from this presentation…THIS!!!
• Yara is a language for creating signatures in different patterns
• Got hex? Sure, that works too
• Magic bytes? “Rar!” at 0
• Think IDS for binary data
Which Strings for Sigs?
We’ll be using python to XOR our data

Loop it, and loop it good!

Don’t forget your ascii love

inb4oneliners
• By using script, we can calculate XOR values (0x0 - 0xff)

• Can detect strangeness in files

• “This program” == MONEY !!!
• Malware authors try to be one step ahead
• Be one step ahead of them
• Think one step ahead of your attacker
Questions?

DONE WITH MY PRESENTATION

NOW I HAVE TO ANSWER QUESTIONS
Thank You!