Malware 101

Introduction to Malware Basics and Research

What do you know about malware?

From NIST SP 800-83, malware:

"…also known as malicious code and malicious software, refers to a program is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim."

It’s a broad topic

Scareware

Spamming Malware

Browser Hijackers

Downloaders

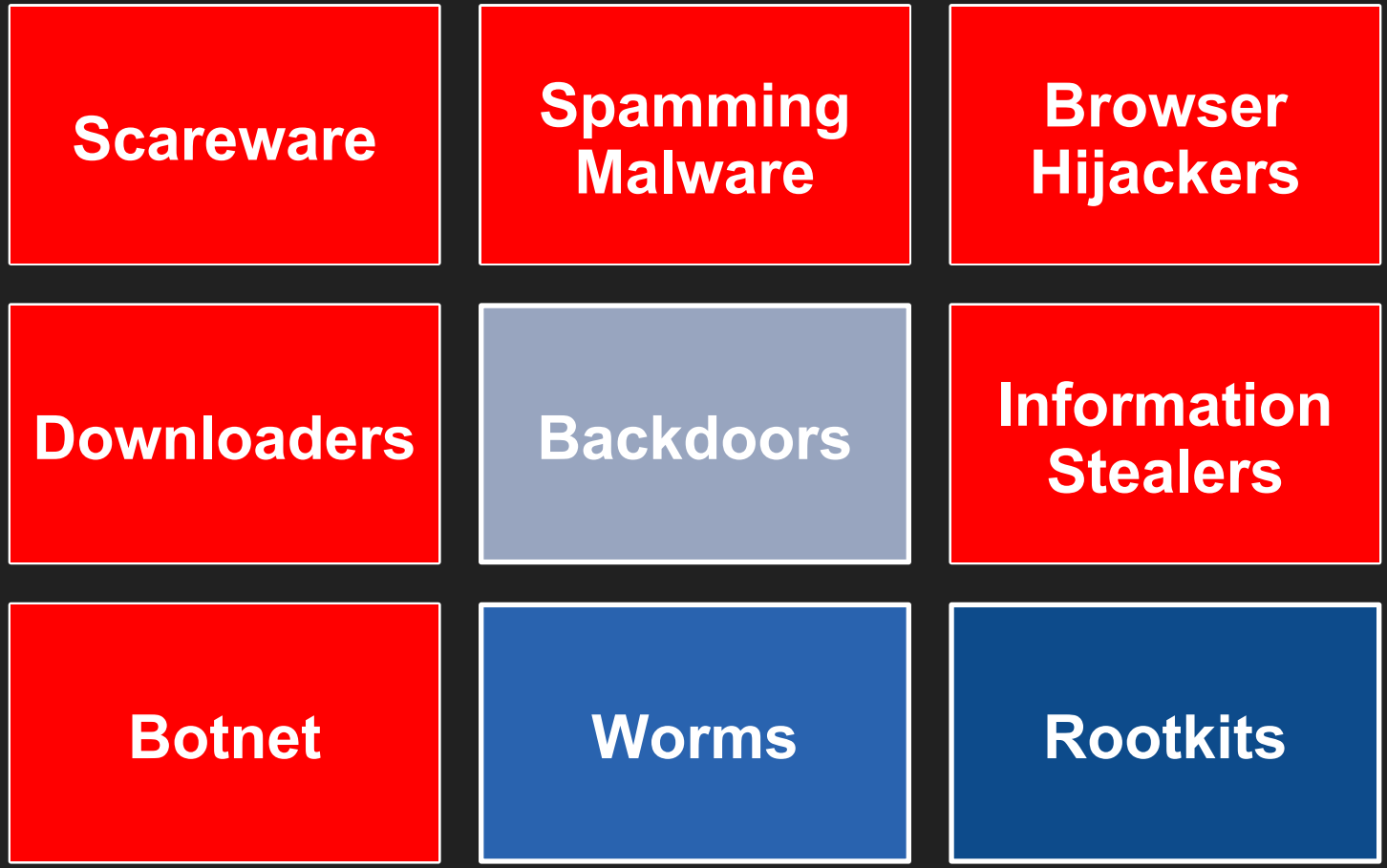
Backdoors

Information Stealers

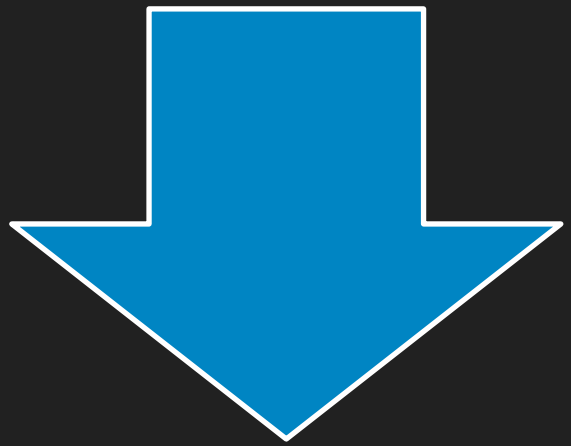
Botnet

Worms

Rootkits


Scareware
Spamming Malware
Browser Hijackers
Downloaders
Backdoors
Information Stealers
Botnet
Worms
Rootkits

advanced threats, which are custom-built by a particular threat group to exploit the most recent vulnerabilities and bypass network or host defenses

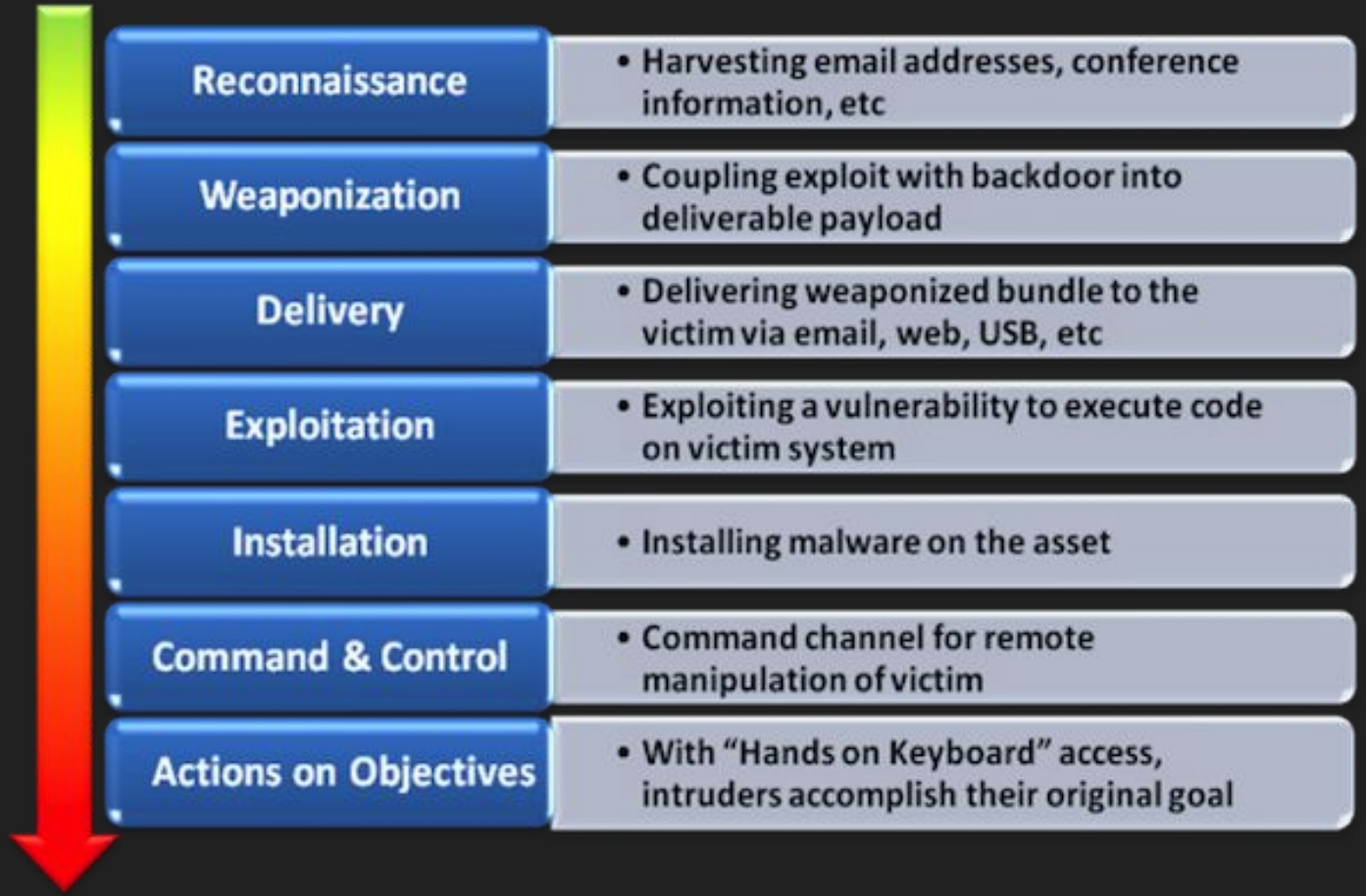


commodity threats, which represent the most common malware families

So how do people get infected? Typically

- Phishing
- Compromised Web Sites (Malvertising, Exploit Kits)

It comes in stages (Cyber Kill Chain)



Characterizing Malware

- Fingerprinting
  - Hashing
  - PE features
  - Strings
- Functionality
  -

Let’s Talk Research

Goals of Malware Research

(generally…)

- Identification
  - What is it?
- Analysis
  - What does it do?
- Classification
  - How bad is it?
- Remediation
  - What can you do with this information?
  - How do you detect/stop/prevent?

Malware Research Life Cycle

1. Observe Trends
2. Gather Samples
3. Analyze
4. Extract Data
5. Apply Knowledge

Observing Malware Trends

Monitor Malware Feeds

Follow others on social media

Gathering Malware Samples

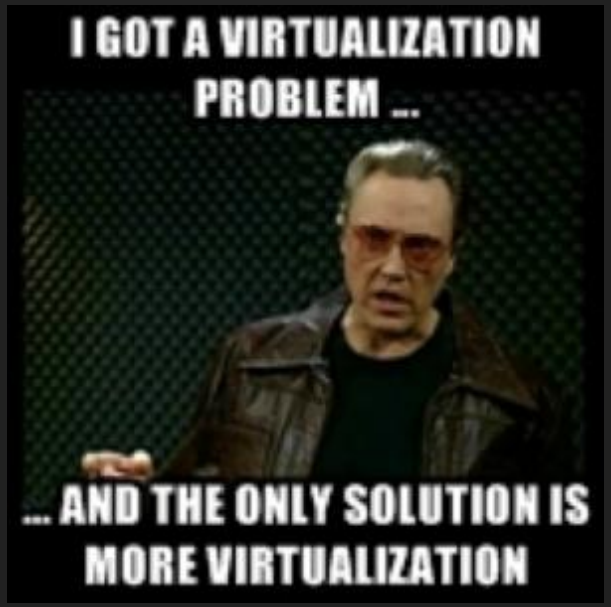
Going back to those feeds and pulling the interesting ones for analysis.


STOP
MALWARE
FOUND

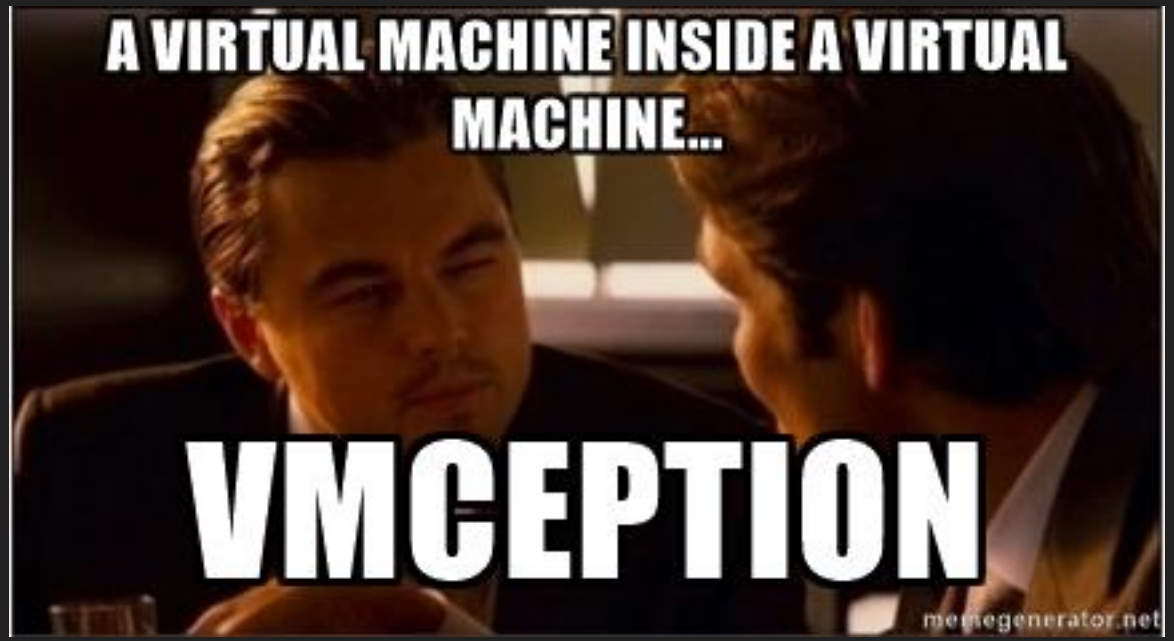
Always deal with malware in a safe environment

Typical VM Configurations

- **Windows 7 or Target OS**
  - **Minimum Requirements**
    - **1 GB Ram (2 Recommended)**
    - **16 GB local storage**
- **VM Tools**
- **Snapshots**
- **Disable Windows Firewall**
- **Disable ASLR/UAC**
- **Disable Windows Updates**
- **Disable any installed Anti-Virus software**
- **Isolated Virtual Network VLAN**
- **Consider using VMCloak or another**



DO IT IN A VM!!!!!!!


A VIRTUAL MACHINE INSIDE A VIRTUAL MACHINE...
VMCEPTION
memegenerator.net

Analyzing Malware

Basic Static Analysis

- The examination of a suspicious binary without actually running the code

Basic Dynamic Analysis

- Involves the analysis of a suspicious binary's behavior during run-time

Basic Static Analysis

Profiling your sample

Name

The name of a malicious file should be analyzed for classification, in addition to using the name for identification and referencing

Location

The location of malicious files should be documented to facilitate searches for similar files on other systems that may be infected

Size

Malware can be embedded within files of various sizes and types. Techniques such as padding and packing can both increase or decrease the size of malware without changing the functionality

Timestamps

Timestamps allow you to determine the potential created, modified, access times of the malicious file

Hashes

Hashes provide a ‘fingerprint’ for a given file, meaning if two files have the same hash, then the files must have the same binary content (exact copies).

Strings

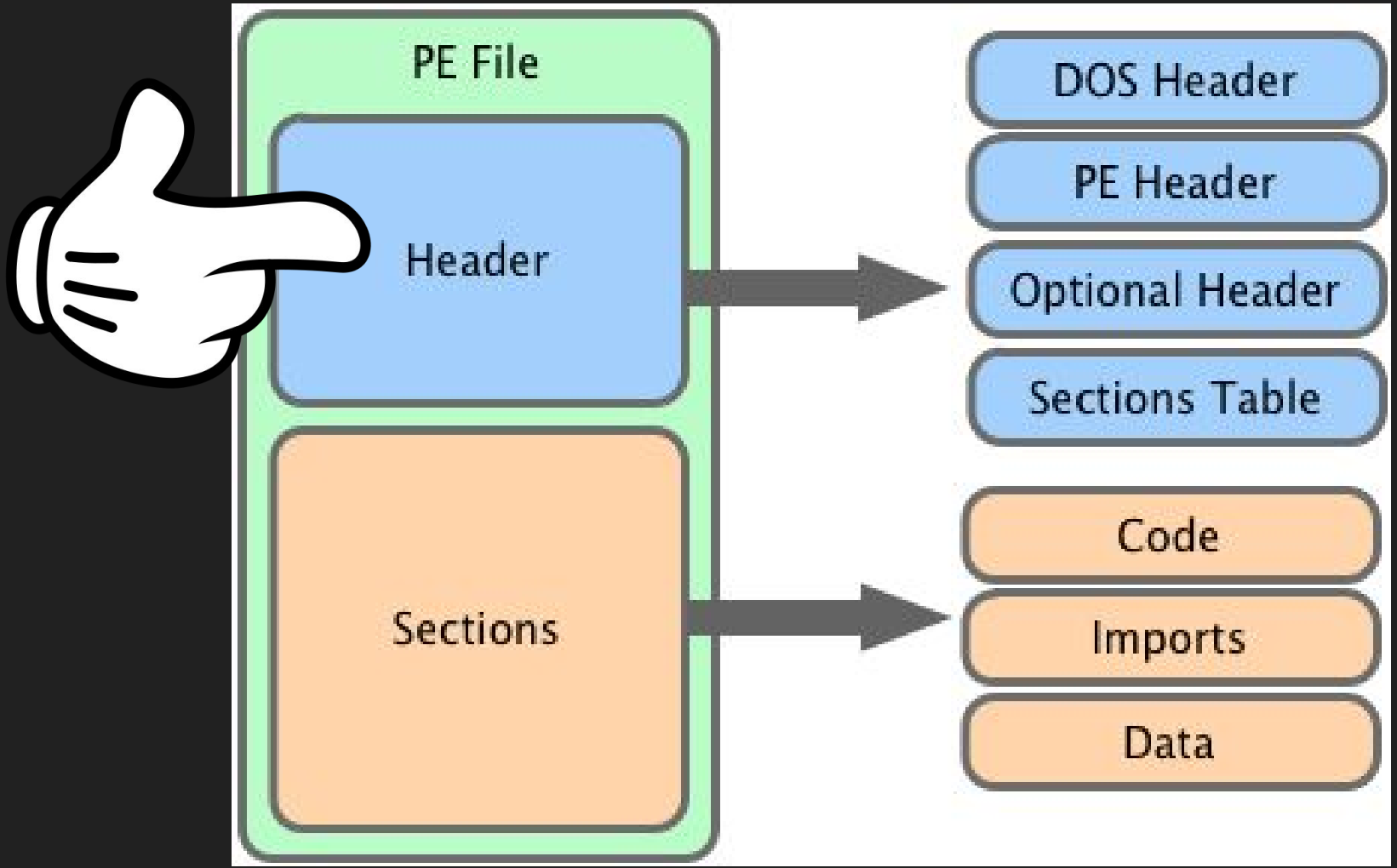
Strings are human-readable text embedded within binary files. Strings can provide a wealth of contextual information, such as IP addresses, URLs, files, registry keys, etc.

However this stuff can be used by malware distributors to mislead you!

- All of these can be crafted using different techniques to represent different values
- Use caution when looking at these values

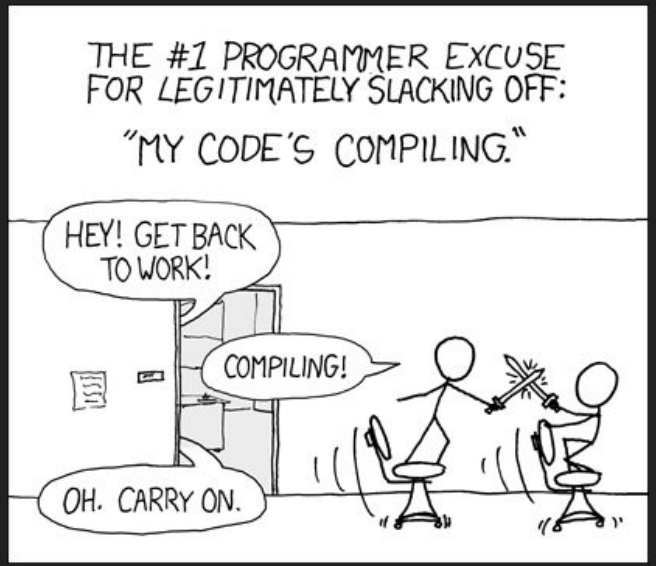
A look into the PE File Format

- Binaries that can execute on a Windows system conform to a standardized format called **portable executables**. The portable executable (PE) format contains a plethora of metadata that help categorize and analyze malware samples.


PE File
Header
Sections
DOS Header
PE Header
Optional Header
Sections Table
Code
Imports
Data

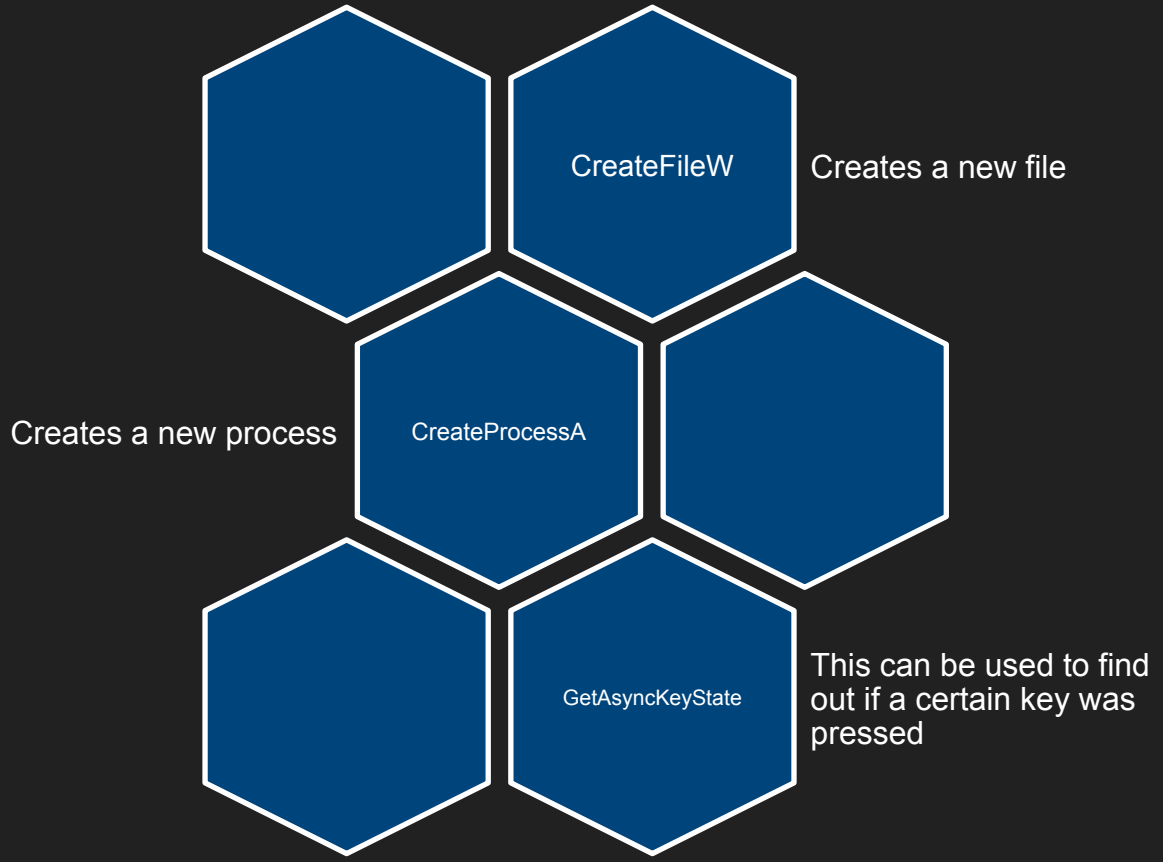
Compile Time

- An older compile time suggests the attack method is old and some antiviruses may have counters measures for it
- New compile times may indicate a new attack method or targeted attack
- These values can be faked by malware authors, it the timing looks strange it is most likely fake
  - Examples
    - Compile time after created time
    - Compile time in the far past
    - Compile time in the future
- *All Delphi programs use a compile time of **June 19, 1992***

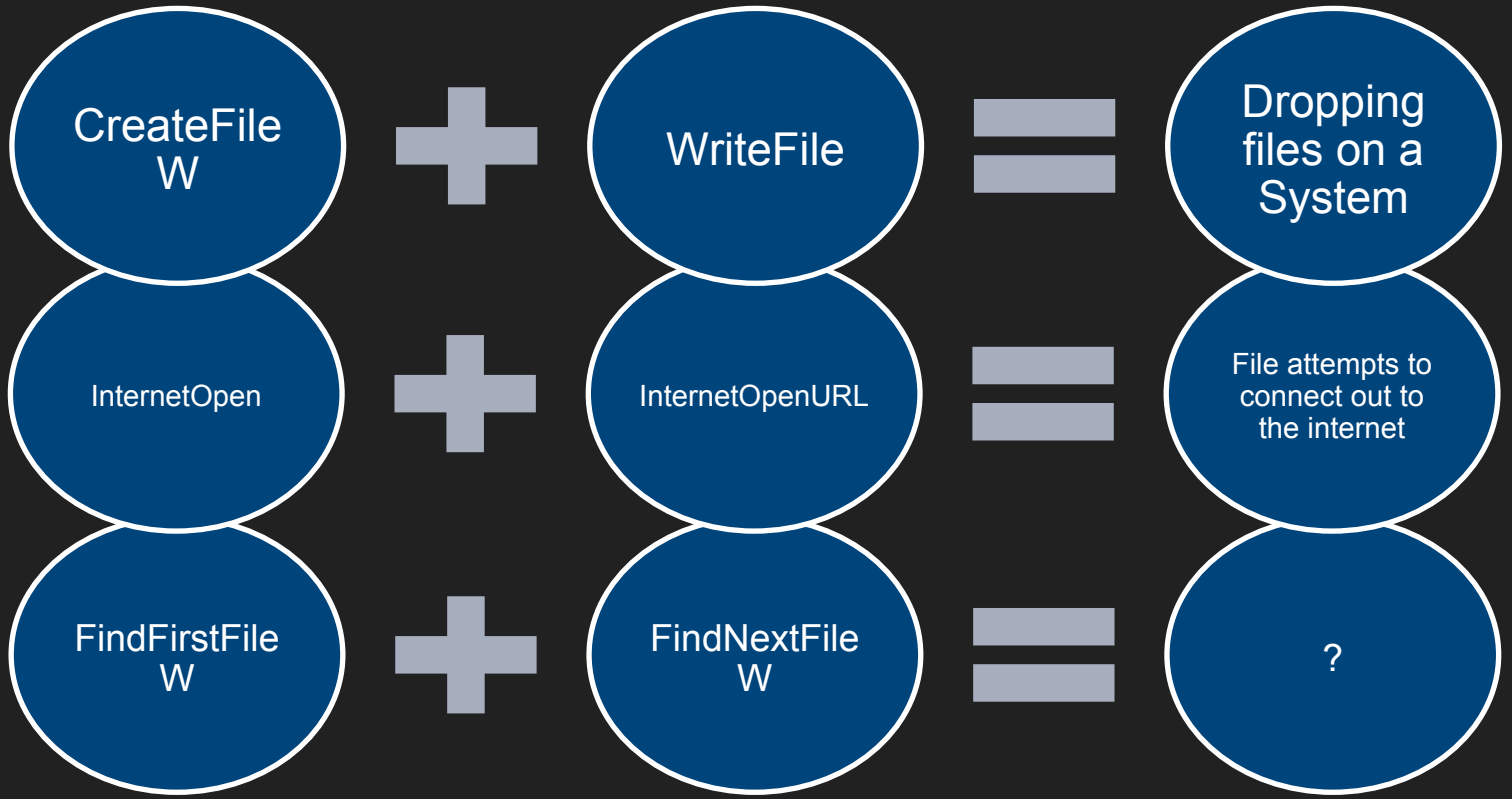


Import and Export Functions

- They are functions from the OS that are used by the sample
- Can lead to hits on functionality (many times the name is pretty self explanatory)
- Don’t know what they are… ask Google.



It all adds up!



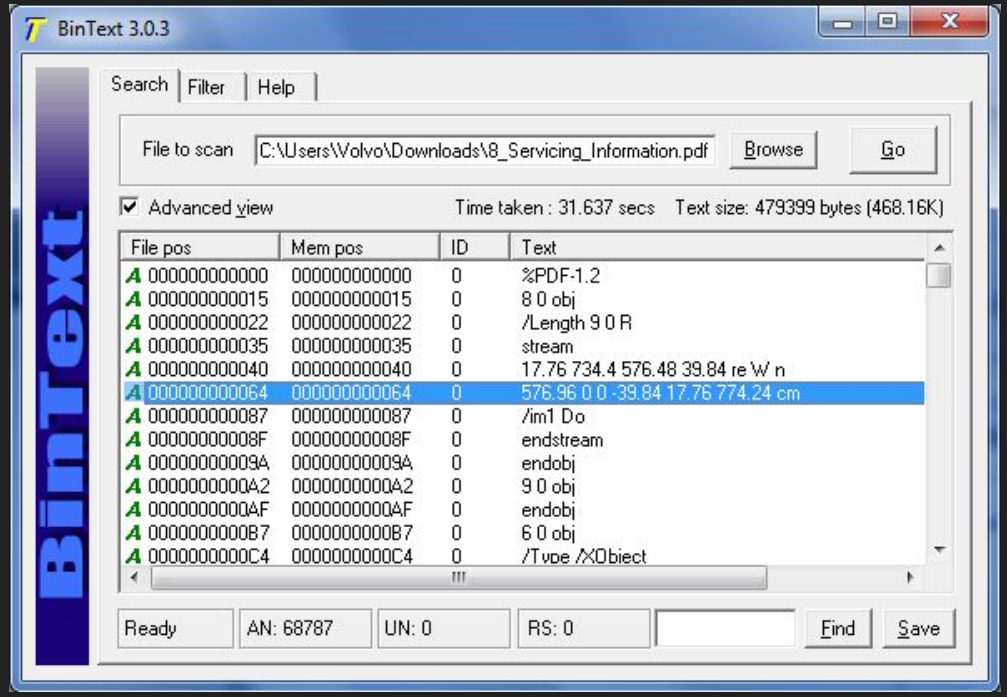
Look at the resources

- Contains all the resources included in the PE
  - Icons
  - Menus
  - Dialogs
  - Strings
  - Version information

- The PE has a GUI, you will be able to see elements of it here and potentially determine functionality from what you see

Looking at the strings!

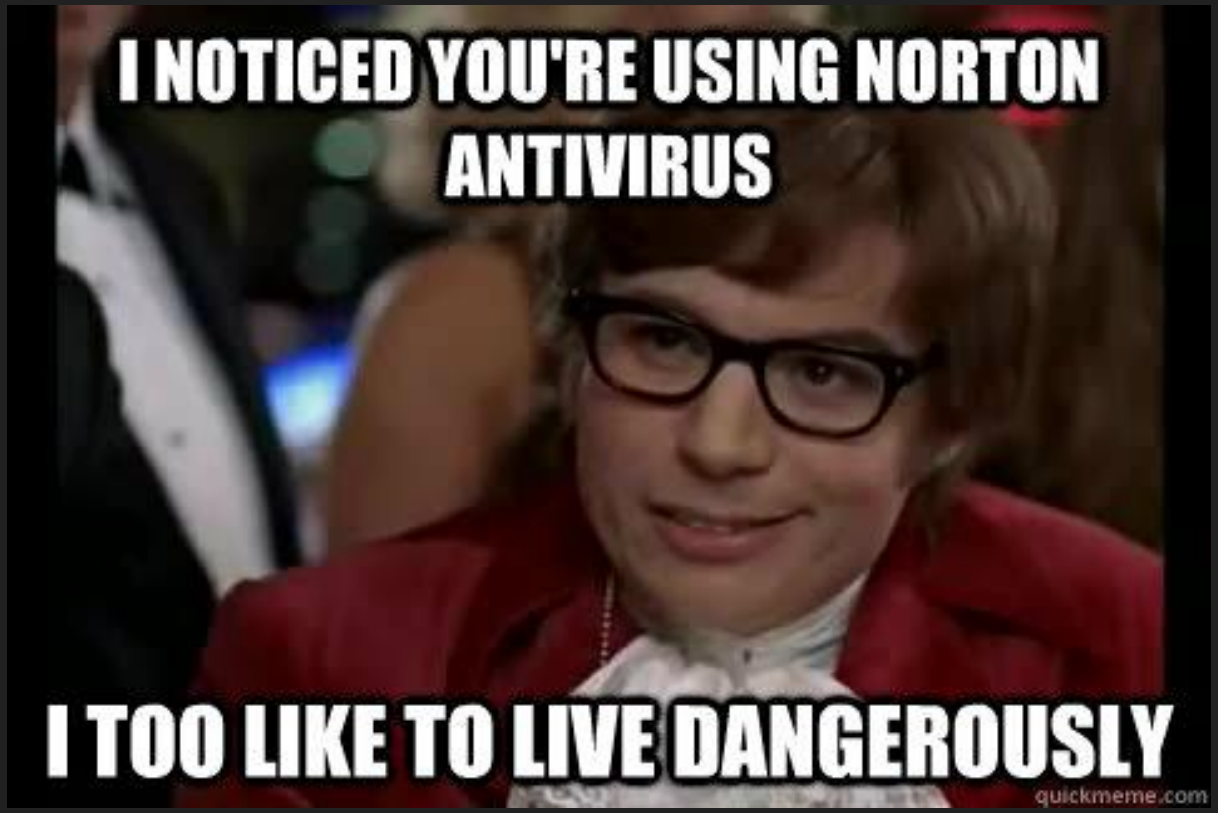
- Can provide context
- Message box contents
- IPs
- URLs
- Licensing Information
- Even functionality hints



There's this thing called Yara...

Check it against A/Vs

virustotal



Basic Dynamic Analysis

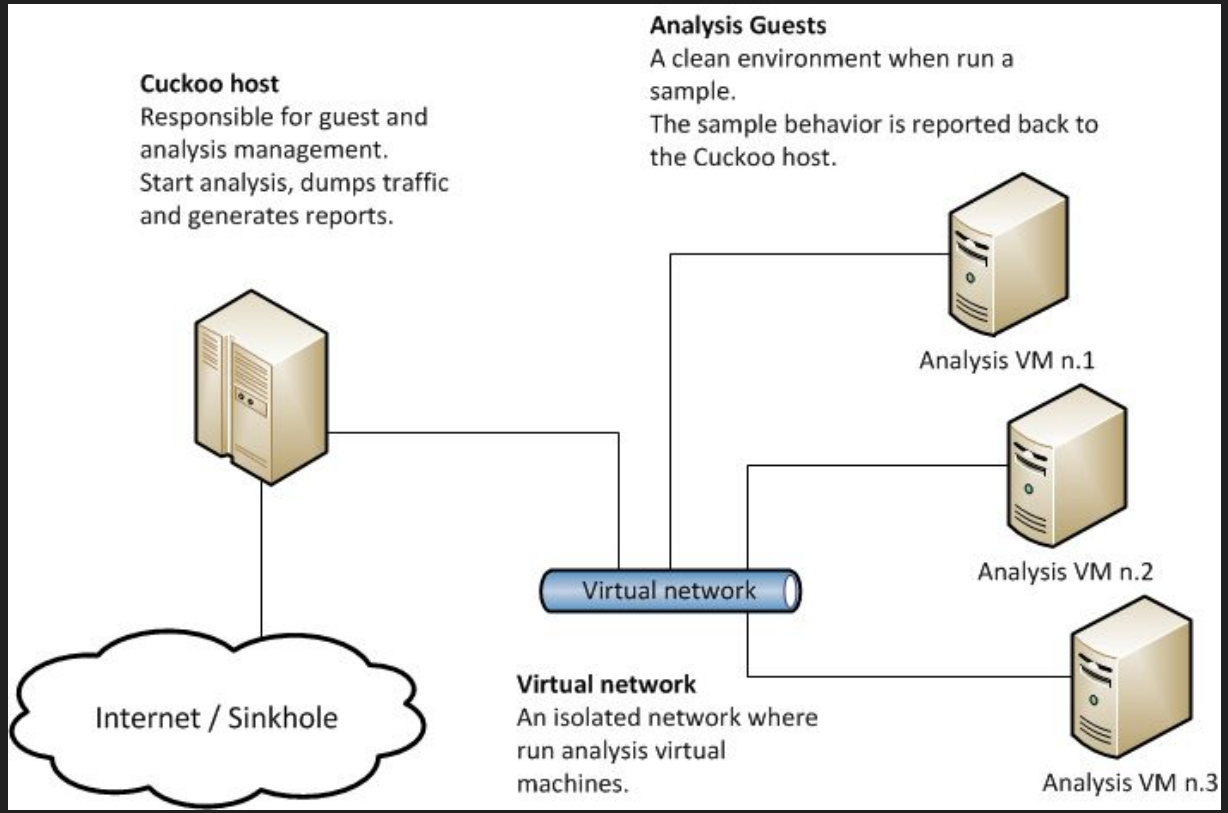
Scanning your File

Uploading the file to online sandboxes like:

Will give you insight to what type of sample you are dealing with

Roll your own!

How does a sandbox work?



Run it in a VM see what it does.. There are tools to help you!

- Process Monitor
- Regshot
- Capture Bat
- FakeNet
- Wireshark
- Noriben

Applying this knowledge

- Dropped Files -> IR
- IP Addresses -> Firewall / IDS/IPS
- URLs -> Web Proxy
- MD5s -> IR
- Registry Keys -> IR

Finally the talking is done!
Let’s Profile a Sample

Be sure to check out
www.CHSINFOSEC.org