# Software Reverse Engineering

COMP 272 | Spring 2022 | University of the Pacific | Jeff Shafer

# Malware Analysis Basics


# Malware

# Malware

- Malware = **Mal**icious Soft**ware**
- **Adware**
  - Inject popup ads in your browser
- **Ransomware**
  - Encrypt your hard drive, demand bitcoins for key
- **Spyware**
  - Harvest user data without their knowledge (keystrokes, files, …)

# Motivations

- **Besides fun (or “fun”), why are we digging into these malware samples anyway?**
- Ans: Profit!
  - You’re being paid $$ to do so
- Final result of your labor: *Malware Analysis Report*

# Malware Analysis Report

- **What would your *boss* like to know about the malware?**
  - What are its capabilities?
  - How can the program be detected across enterprise systems?
  - What would data exfiltration (if purpose) look like on our network monitoring infrastructure?
    - Can we see *if* data was taken? Can we see *what* data was taken?
  - Does the program reveal anything about our adversaries?
    - Are they targeting *us* specifically?
    - What are their capabilities?

# Malware Analysis Report

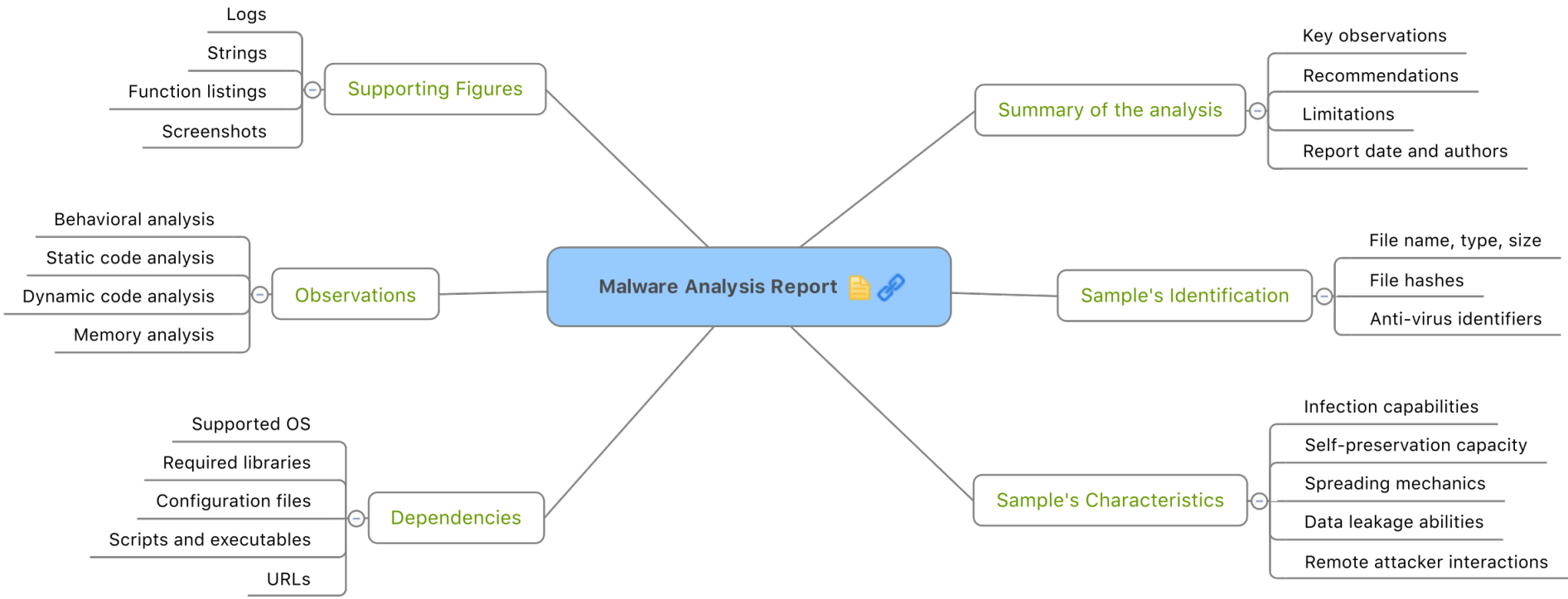
- **Executive Summary (for your boss)**
  - Capabilities, origin, …
- **Identification**
  - File name
  - File size
  - MD5 and SHA1 hashes (of file and code sections)
- **Characteristics** – What can malware do?
  - Infect files?
  - Persist across reboots?
  - Spread to other systems?
  - Leak/exfiltrate data?
  - Communicate with attacker?
  - Resist analysis?
- **Dependencies** for operation
  - OS version?
  - Network access? (URLs/IPs)
- **Behavioral and code analysis**
  - Static analysis
  - Dynamic analysis
  - *The heart of the analysis report*
- **Tables and Figures** (lots!)
  - Support your analysis above
- **Indicators of Compromise** (IOC)
  - Can you recognize this malware elsewhere?
  - Useful for NOC

https://zeltser.com/malware-analysis-report/

# Example Indicators of Compromise (IOCs)

- IP addresses
- Domains
- Hostnames (subdomains)
- Email addresses
- URL
- URI
- File Hashes: MD5, SHA1, SHA256, PEHASH, IMPHASH
- CIDR Rules
- File Paths
- MUTEX name
- CVE number

# Malware Analysis Report – Mind Map




https://zeltser.com/malware-analysis-report/

## Malware Analysis Template

| BACKGROUND | |
|---|---|
| **Date:** | |
| **Workstation:** | |
| **File Name:** | |
| **File Location:** | |
| **File Timestamps:** | |
| **Notification Vector:** | |
| **STATIC ANALYSIS** | |
| **File Size (bytes):** | |
| **Icon Graphic:** | |
| **Signed?:** | |
| **File Hash:** | |
| **Imp Hash:** | |
| **PE Section Hashes:** | |
| | |
| **Compile Time** (pescanner, PEView): | |
| | |
| **File Properties** (PEStudio, PeView): Description, version, file header characteristics | |
| | |
| **Strings** (strings, strings2, BinText): Functions, domains, IP addresses, commands, error msgs | |
| | |
| **Packed** (pescanner, PEiD, ExeInfo): | |
| | |
| **Entropy** (ByteHist, pescanner): File, sections | |
| | |
| **Imported/Exported Functions** (PEStudio, Dependency Walker): | |
| | |
| **Open Source Research** (VirusTotal, search engines, malware repositories): | |
| | |
| **BEHAVIORAL ANALYSIS** | |
| **File System Artifacts** (Regshot, CaptureBAT, Process Monitor, Cuckoo):<br>*Triggers:* Browser, mail client, specific web pages (google, bank), time, reboot, user/admin privs<br>*Dependencies:* DNS, HTTP, IRC, ARP | |
| | |
| **Network Artifacts** (SmartSniff, Fakedns, INetSim, NetworkMiner Wireshark): C2 domains/IP addresses, protocols, user-agent | |
| | |
| **Memory Analysis** (Volatility, Rekall, Redline, Process Hacker): rogue processes, code injection, rootkits, network artifacts | |
| | |
| **Open Source Research** (centralops, robtex, urlvoid, ipvoid, TrustedSource): | |
| | |

*Don't like Mind Maps? How about a template to fill in?*

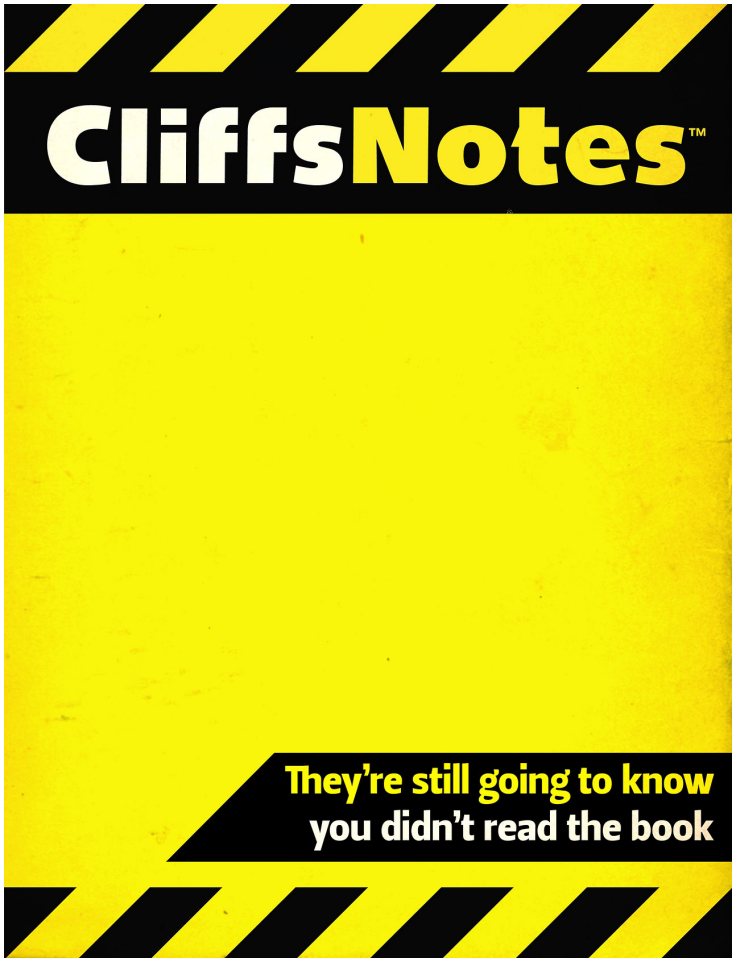
https://www.sans.org/blog/how-to-track-your-malware-analysis-findings/

# Malware Analysis Report

- Tip: Keep a running log in your notes of **what you know** and **what you need to know**.
  - Try to avoid running down rabbit holes decoding technical challenges that don't *actually* answer any questions you need!
  - *For example, you don't need to understand how the packed binary is unpacked/deobfuscated. You just need to steal it from memory right after the malware code finishes doing that.*

# Life as a Malware Analyst

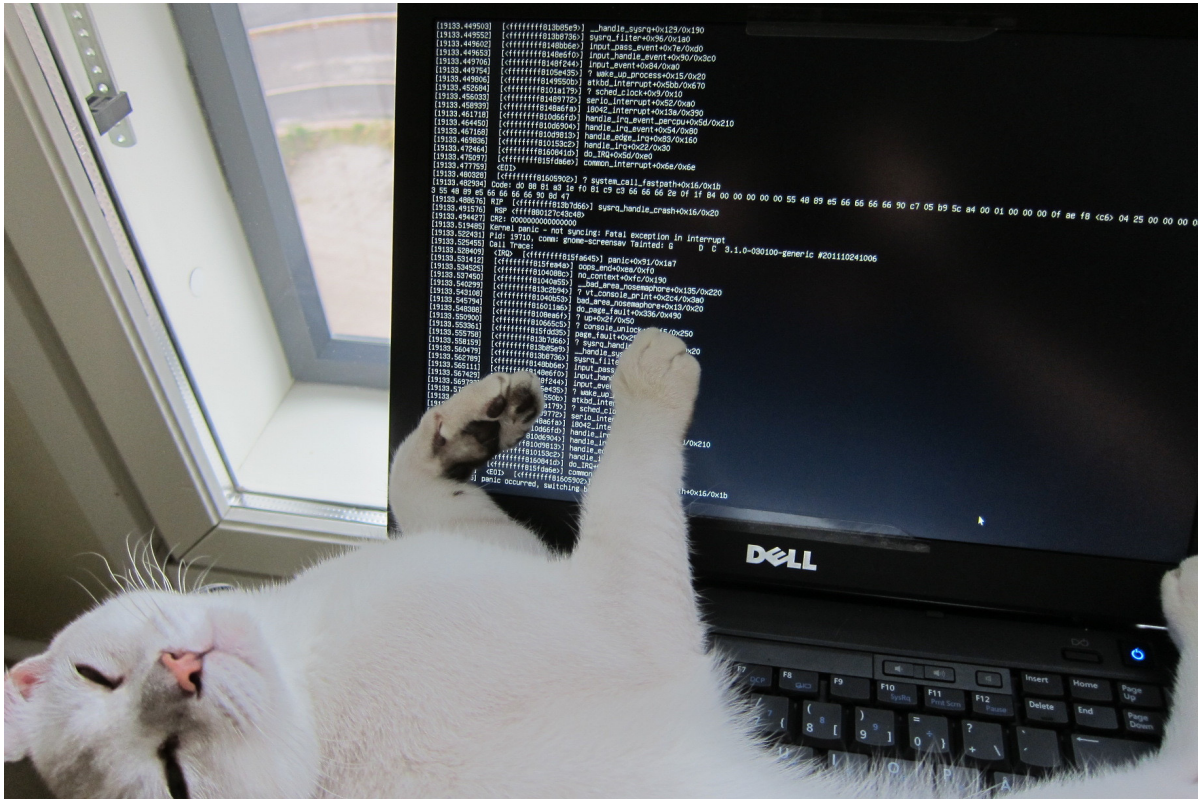
# Life as a Malware Analyst




- **There is <u>no answer key</u> with all of the answers in it**
- *At least, not for any malware people will pay you to examine*
  - For old malware, there's Google and VirusTotal…

# Life as a Malware Analyst

- **The malware authors are <u>actively trying to subvert you</u>** 😡




- *At a minimum, they want to obfuscate their malware to avoid automated detection*
- *And they really don't like you analyzing their code either…*

# Life as a Malware Analyst

- **There are always more suspicious binaries to examine than engineer hours available**

# Life as a Malware Analyst

- **Your boss always wants your reports faster**
- **Your boss will only read the executive summary**
  - *But you need the* **details** *to write the* **summary***…*

# Malware Samples

# Malware Samples

- Where do we get our malware samples from *in industry?*
  - Clients send it to us
    - *"Here's an executable. Timmy the intern thinks it's suspicious"*
  - Recovered from servers or end-user devices by IT staff after suspicious behavior observed
    - Machine was locked for ransom
    - Machine was sending spam
    - Machine was DDOS'ing victim off-site
    - Machine was scanning network
  - Honeypots that we control (on our network or clients)

# Malware Samples


https://www.honeynet.unam.mx/

# Malware Samples

https://www.honeynet.unam.mx/

# Malware Samples

- Where can we get malware samples from to practice with?

https://cyberlab.pacific.edu/resources/malware-samples-for-students

  - VirusShare: https://virusshare.com/
  - Contagio: http://contagiodump.blogspot.com/
  - The Zoo: https://github.com/ytisf/theZoo
- Note: Services come and go each year!

# Malware Sharing

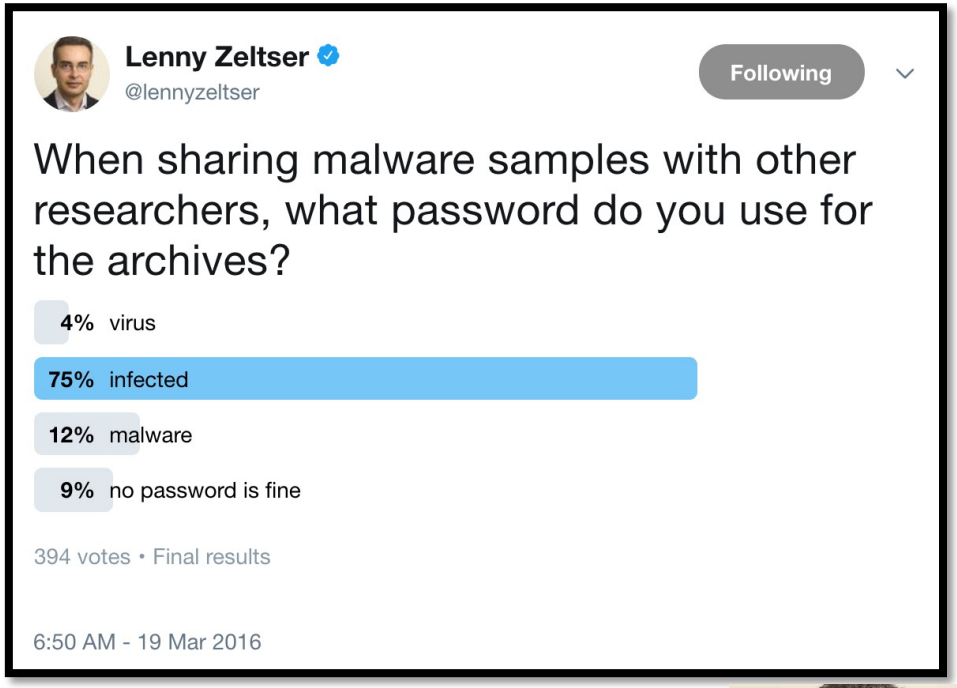
# Malware Sharing

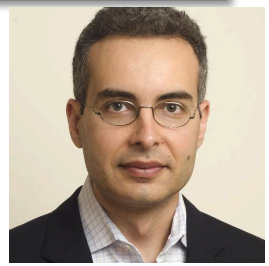
- Most malware is exchanged via password-protected zip files
  - Prevents annoying AV scanners from blocking our work
  - Prevents you from being flagged/blacklisted as “infected”
  - Prevents recipient from accidentally infecting themselves with one stray click
- Problem with password-protected zip files?
  - *Contents* are encrypted but the *file names* and *CRC* checksums are not! May unintentionally reveal too much
  - Suggest 7-Zip format with header encryption

https://zeltser.com/share-malware-with-researchers/

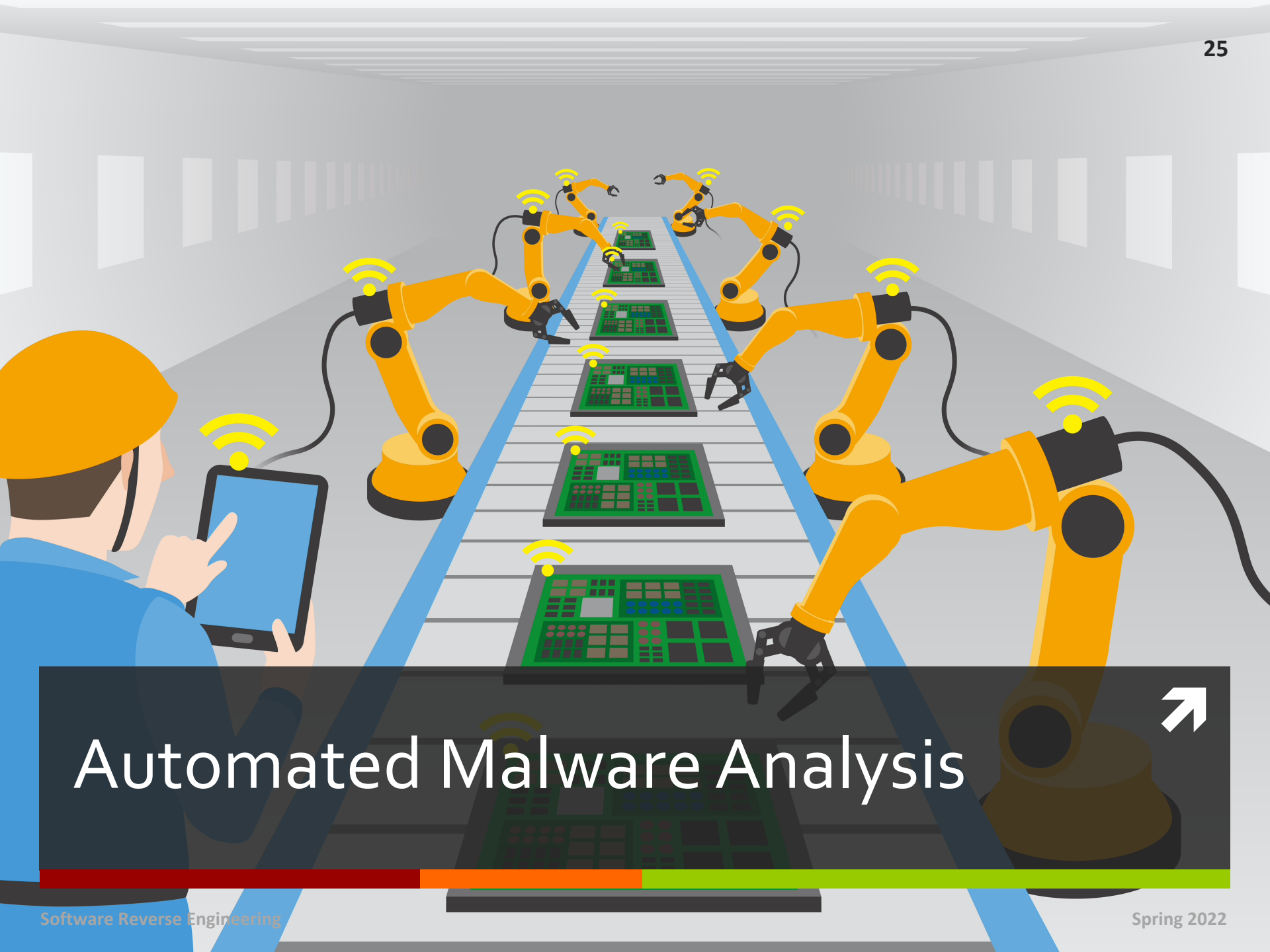
# Malware Sharing

- Common passwords?
- "*infected*" is such a popular password that many anti-virus tools (such as those used by cloud email vendors) might try it automatically… ☹



https://zeltser.com/share-malware-with-researchers/



# Automated Malware Analysis

# Automated Malware Analysis

- **Multi-AV scanners**
  - Does an anti-virus product think your sample is malicious? Check a bunch in parallel!
- Numerous Examples
  - VirusTotal - https://www.virustotal.com - 66 engines
  - VirScan - http://virscan.org/ - 51 engines
  - Malware Hash Registry - https://team-cymru.com/community-services/mhr/ - 30 engines
  - MetaDefender - https://metadefender.opswat.com

# Automated Malware Analysis

- **File Reputation**
  - Is this file a legitimate part of Windows, or OS X, or Adobe Acrobat, or Google Chrome, or … ?
- Examples
  - National Software Reference Library: https://www.nist.gov/software-quality-group/national-software-reference-library-nsrl
  - HashSets: https://www.hashsets.com/ - $$$
- Inverse Example
  - Malware Hash Registry: https://team-cymru.com/community-services/mhr/

# Automated Malware Analysis

- **Malware Data Repositories**
  - Run static analysis on malware and view detailed results
- Numerous Examples
  - VirusTotal - https://www.virustotal.com
  - Malware Hash Registry - https://team-cymru.com/community-services/mhr/

# Automated Malware Analysis

- **Automated Sandbox**
  - What happens if the malware is run ("detonated") in a controlled and monitored environment? What does it do?
- Examples
  - CuckooSandbox: https://cuckoosandbox.org/
  - Hybrid Analysis: https://www.hybrid-analysis.com/
    - Interesting article on implementation challenges: https://zeltser.com/jan-miller-hybrid-analysis-sandbox/
    - "Hybrid" because it combines static and dynamic techniques
  - Joe Sandbox: https://www.joesandbox.com/

# Automated Malware Analysis

- **Demo with SHA-1:**
  `4db5a8e237937b6d7b435a8506b8584121a7e9e3`
- Sites to test with:
  - https://www.virustotal.com
  - https://www.hybrid-analysis.com
    Do a “Report Search”
  - https://www.joesandbox.com/

virustotal.com

VirusTotal - File - f470... | Free Automated Malw... | Automated Malware A... | Automated Malware A... | Automated Malware A... | Malware Hash Registry

f47060d0f7de5ee651878eb18dd2d24b5003bdb03ef4f49879f448f05034a21e

Sign in | Sign up

50 / 66

Community Score

50 security vendors and 1 sandbox flagged this file as malicious

f47060d0f7de5ee651878eb18dd2d24b5003bdb03ef4f49879f448f05034a21e

executable.exe

64bits | assembly | direct-cpu-clock-access | peexe | persistence | runtime-modules

74.00 KB
Size

2021-12-21 08:26:08 UTC
1 month ago

EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 10

| | | | |
|---|---|---|---|
| Ad-Aware | Gen:Variant.Fugrafa.10989 | AhnLab-V3 | Trojan/Win.Blocker.R448988 |
| Alibaba | Ransom:Win32/Blocker.863e972d | ALYac | Trojan.Ransom.Blocker.gen |
| Antiy-AVL | Trojan/Generic.ASMalwS.215EF90 | Arcabit | Trojan.Fugrafa.D2AED |
| Avast | Win32:Agent-BCKN [Trj] | AVG | Win32:Agent-BCKN [Trj] |
| Avira (no cloud) | TR/Blocker.svrdv | BitDefender | Gen:Variant.Fugrafa.10989 |
| Comodo | Malware@#27qzfujyxzofk | CrowdStrike Falcon | Win/malicious_confidence_100% (W) |
| Cylance | Unsafe | Cynet | Malicious (score: 100) |
| DrWeb | Trojan.Encoder.27924 | Elastic | Malicious (high Confidence) |
| Emsisoft | Gen:Variant.Fugrafa.10989 (B) | eScan | Gen:Variant.Fugrafa.10989 |
| ESET-NOD32 | Win64/Agent.HQ | FireEye | Generic.mg.1c7243c8f3586b79 |
| Fortinet | W64/Agent.HQ!tr | GData | Gen:Variant.Fugrafa.10989 |

hybrid-analysis.com

VirusTotal - File - f470... | Free Automated Malw... | Automated Malware A... | Automated Malware A... | Automated Malware A... | Malware Hash Registry

HYBRID ANALYSIS | Request Info | IP, Domain, Hash...

# brbbot.exe

malicious

This report is generated from a file or URL submitted to this webservice on January 28th 2020 02:21:46 (UTC)
Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v8.30 © Hybrid Analysis

Threat Score: 84/100
AV Detection: 81%
Labeled as: Trojan.Generic

Overview | Sample unavailable | Downloads | External Reports | Re-analyze | Hash Seen Before | Show Similar Samples | Request Report Deletion

Link | Twitter | E-Mail



## Additional Context

### Related Sandbox Artifacts

**Associated SHA256s**

fcdf4f910130603bd1f034f7893fc691b7566215af5e210285a31e94099abca8
d65165279105ca6773180500688df4bdc69a2c7b771752f0a46ef120b7fd8ec3
b157ec4f2dabbfc60fce89ebdf64e0d70371d5dfc0b7c13a544e1913ee167c99
8ab826491b5c20edfc5d5547ea21915664389a618f04a0b607f493b0f0812fa8
e3ef74e515185ce5dd73e81eac9cc365391e2a194f5056a090be687ca25d85a7
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
96d587140d742054d44e69fe01d345a46cfef49f36e2fcab863080e359fae6bb
74694443e1068dda8cb89e61b380ea27bcf410293bb68b4680e9d1253da73d4d
c6b9800c7c69f11d6cce9c86037a93f78c4a32fbafcd33775a399746d256898f
8c68a5e725daa88a9322007dfaaa5c7fb2492910f3b714332e5f28862e9f3d09

## Indicators

Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

joesandbox.com

VirusTotal - File - f470... | Free Automated Malw... | Automated Malware A... | Automated Malware A... | Automated Malware A... | Malware Hash Registry

JoeSandbox Cloud BASIC

Create Interactive Tour

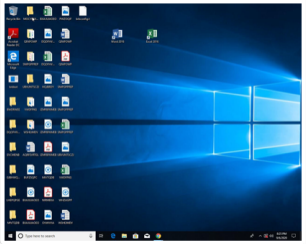
# Analysis Report brbbot.exe

## Overview

### General Information

| | |
|---|---|
| Sample Name: | brbbot.exe |
| Analysis ID: | 282687 |
| MD5: | 1c7243c8f35... |
| SHA1: | 4db5a8e237... |
| SHA256: | f47060d0f7d... |

Most interesting Screenshot:



### Detection

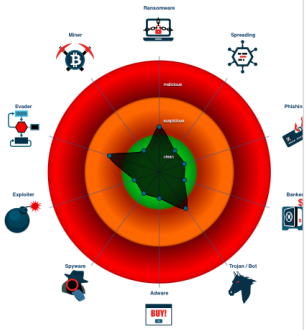
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

| | |
|---|---|
| Score: | 88 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Antivirus / Scanner detecti...
- Antivirus detection for dro...
- Multi AV Scanner detectio...
- Multi AV Scanner detectio...
- Snort IDS alert for network...
- Machine Learning detectio...
- Machine Learning detectio...
- Contains functionality to c...
- Contains functionality to c...
- Contains functionality to d...
- Contains functionality whi...
- Detected potential crypto ...

### Classification



## Startup

- System is w10x64

# Automated Malware Analysis

- **Why might I *not* want to use these tools?**

# Automated Malware Analysis

- **Why might I *not* want to use these tools?**
- File may have sensitive data embedded in it – don't want to publicly release
  - Suggest looking up by hash instead of uploading file
- Attacker may be checking the major sites to see if they have been detected yet
  - Highly relevant for a *targeted* attack
  - Irrelevant for mass-market malware
  - Searching by hash may risk tipping off attacker
  - *You could run your own, private, automated tool set*
- Malware may be too well obfuscated and/or fail to do anything in automated sandbox

# Lab 1 Pre-Lab

- Install a virtual machine manager (VMware recommended) on your laptop
- Go to https://remnux.org/ and download latest installer file
  - `remnux-v7-focal.ova`
- Import Remnux OVA file into a new VM
  - **O**pen **V**irtual **A**ppliance
- Download **takes time**!
  Updating packages takes **MORE time**!

Ready by **Tuesday**