Malware Analysis Primer

CYBR473 – Malware and Reverse Engineering (2024/T1)

Lecturers: Arman Khouzani (course coordinator), Alvin Valera

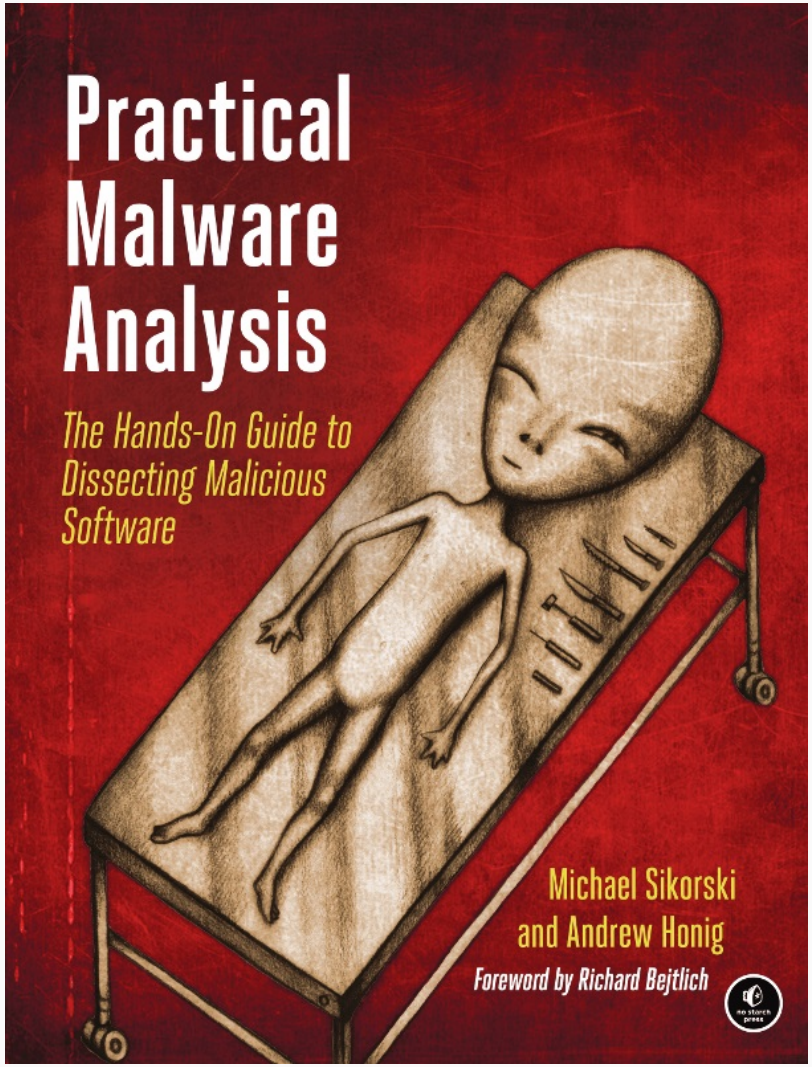
Victoria University of Wellington – School of Engineering and Computer Science

Table of contents

Reading Material

- **Part I: Basic Analysis**
  - Ch.0: Malware Analysis Primer

"Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software", Michael Sikorski and Andrew Honig, 2012



Incident Response

Case history

- A medical clinic with 10 offices found malware on one of their workstations.
- Hired a consultant to clean & re-image that machine.

All done – case closed?

Incident Response

After malware is found, you need to know:

- Is the attacker really gone?
  - Did an attacker implant a rootkit or trojan/backdoor on your systems?
- What did the attacker steal or add?
- How did the attack get in?
  - Root-cause analysis

Breach clean-up cost LinkedIn nearly $1 million, another $2-3 million in upgrades

Summary: LinkedIn executives reveal on quarterly earnings call just what the June theft of 6.5 million passwords cost the company in forensic work and on-going security updates.

By John Fontana for Identity Matters | August 3, 2012 -- 17:10 GMT (10:10 PDT)

Follow @johnfontana

Comments 0 Vote 1 Like 4 Tweet 51 Share more +

LinkedIn spent nearly $1 million investigating and unraveling the theft of 6.5 million passwords in June and plans to spend up to $3 million more updating security on its social networking site.

Malware Analysis

Dissecting malware to understand:

- How it works;
- How to identify it;
- How to defeat or eliminate it.

A critical part of incident response.

The Goals of Malware Analysis

Information required to respond to a network intrusion:

- Exactly what happened;
- Ensure you've located all infected machines and files;
- How to measure and contain the damage;
- Find signatures for intrusion detection systems.
  - *signatures here mean "patterns", and has nothing to do with digital signatures!*

Signatures

Host-based signatures

- Identify files or registry keys on a victim's computer that indicate an infection.
- Focus on what the malware did to the system, not the malware itself.
  - *Different from antivirus signature.*

Network signatures

- Detect malware by analysing network traffic.
- More effective when made using malware analysis.

False Positives

Secret, proprietary network forensics tool;

Found 200 Windows viruses on Linux DNS servers!

CBS San Francisco Your Home Buy Tickets More FOLLOW US LOGIN

City College Of San Francisco Computer Lab Security Breached

January 13, 2012 1:56 PM

Share this Like 1 Tweet 3 +1 0 Share 2 View Comments

Share CBS Local with your friends. Add us to your Timeline. What's this?

SAN FRANCISCO (KCBS) – The personal banking data from thousands of City College of San Francisco students, faculty and staff may be at risk because of a virus that infiltrated one computer lab – perhaps years ago.

Incredibly, the breach was only discovered recently – over the Thanksgiving holiday weekend.

KCBS' Holly Quan Reports:

City College of San Francisco (CCSF)

Malware Analysis Techniques

Malware Analysis Techniques

Types of Malware

General Rules for Malware Analysis

Static vs. Dynamic Analysis

Static Analysis

- Examines malware **without running** it.
- Tools: `VirusTotal`, `strings` (or `BinText`), a *disassembler* like `IDA Pro`, `Ghidra`, ...

Dynamic Analysis

- **Run the malware** in a virtual machine
- Monitor its effects
- Tools: `RegShot`, `Process Monitor`, `Process Explorer`, `Wireshark`. ...
- RAM Analysis: `Volatility`
- Debuggers: `ollydbg`, `x64dbg`, `windbg`, `Ghidra`, ...

Basic Analysis

Basic static analysis:

- View malware without looking at instructions.
- Tools: `VirusTotal`, `strings`
- Quick and easy but fails for advanced malware and can miss important behaviour.

Basic dynamic analysis:

- Easy but requires a safe test environment.
- Not effective on all malware.

Advanced Analysis

Advanced static analysis:

- Reverse-engineering with a **disassembler**.
- Complex, requires understanding of assembly code.

Advanced dynamic analysis:

- Run code in a **debugger**.
- Examine the internal state of a running malicious executable.

Types of Malware

Malware Analysis Techniques

Types of Malware

General Rules for Malware Analysis

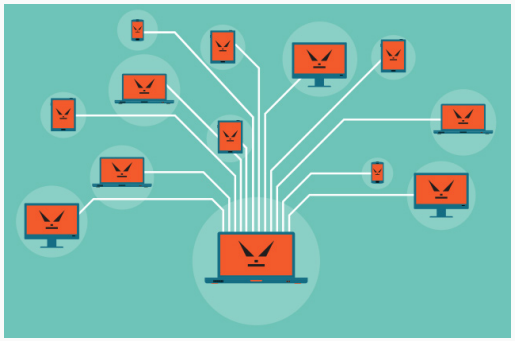
Types of Malware

Backdoor

- Allows attacker to control the system

Botnet

- All infected computers receive instructions from the same Command-and-Control (C&C) server



Downloader

- Malicious code that exists only to download other malicious code.
- Used when attacker first gains access.

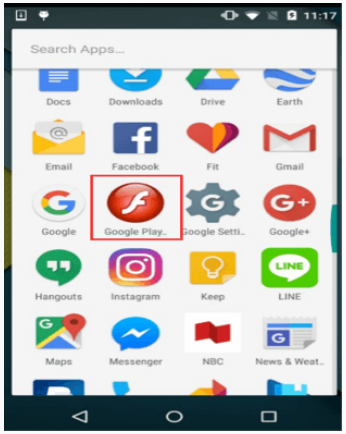
Types of Malware (cont.)

Information-stealing malware

- Sniffers, keyloggers, password hash grabbers.

Launcher

- Malicious program used to launch other malicious programs.
- Often uses non-traditional techniques to ensure stealth or greater access to a system.



Rootkit

- Malware that conceals the existence of other code.
- Usually paired with a backdoor.

Types of Malware (cont.)

Scareware

- Frightens user into doing/buying something.

Fake FBI warning tricks man into surrendering himself for possession of child porn

29 Jul, 2013 | by Nishtha Kanal | Like 3 +1 0 Tweet 3 Share

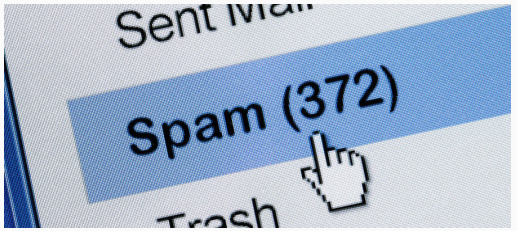
Here's a weird one. We've heard of viruses and malware bringing harm to computers but in a rare instance, a "ransomware" has brought a positive outcome. A man in the US turned himself in to the police after a pop-up caused by a ransomware informed him that child porn had been identified on his machine.

Jay Matthew Riley, a 21-year-old from Virginia was browsing the Internet, when a pop-up containing an "FBI warning" informed him that it had detected child pornography on his machine. The message went on to tell Riley to pay up a fine online or face the consequences.

Types of Malware (cont.)

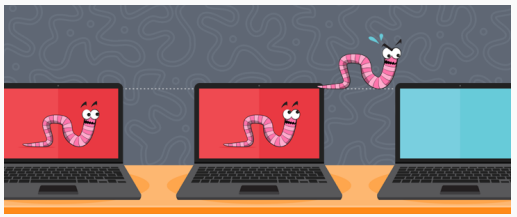
Spam-sending malware

- Attacker rents machine to spammers.



Worms or viruses

- Malicious code that can copy itself and infect additional computers.



Ransomware

- Encrypts files, demands ransom in Bitcoin.

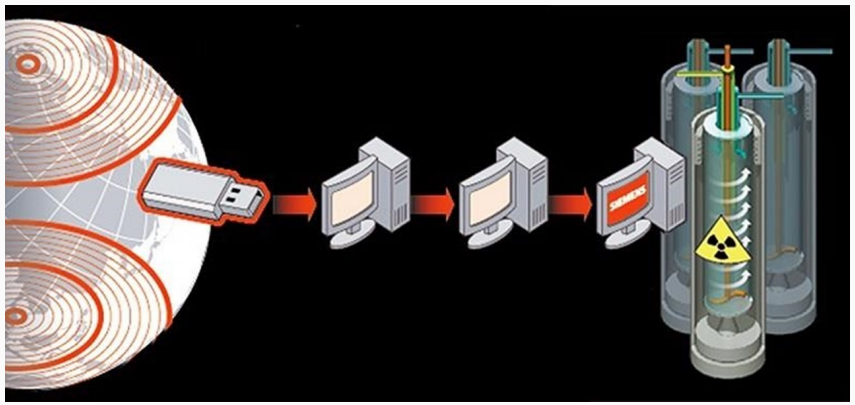
Mass vs. Targeted Malware

Mass malware

- Intended to infect as many machines as possible.
- Most common type.

Targeted malware

- Tailored to a specific target.
- Very difficult to detect, prevent, and remove.
- Requires advanced analysis.
- E.g.: `Stuxnet`



General Rules for Malware Analysis

Malware Analysis Techniques

Types of Malware

General Rules for Malware Analysis

General Rules for Malware Analysis

Don’t Get Caught in Details.

- You do **NOT** need to understand 100% of the code.
- Focus on key features.

Try Several Tools.

- If one tool fails, try another.
- Do **NOT** get stuck on a hard issue, move along.

Malware authors are constantly raising the bar.

Next: Basic Static Analysis