Introduction

Arvind S Raj
(arvindsraj@am.amrita.edu)

16SN708 Malware Analysis

M.Tech CSN Jul-Nov 2017

Lecture overview

- Malware analysis goals
- Two popular approaches for analysis
- Some popular malware categories
- General tips to remember during analysis

Goals of malware analysis

- Determine what the malware does and how it spreads.
- Issue an advisory on new malware and how it spreads to local network users.
- Develop a signature for the malware and detect infected machines to isolate and fix.
- Perform a more detailed analysis of the malware for presentation to management on the infection.

Goals of malware analysis(cont.)

- Goals and associated activities depend on exact nature of analysis required.
- Eg: Signature development not needed if you buy signatures.
- Eg: Detailed analysis done usually by anti-malware product vendors.
- Extent of some activities(eg: analysis of malware functioning) also depends on goal.

Malware analysis techniques

- Two popular techniques: static and dynamic analysis.
- **Static analysis**: No executing the malware. Simply study the sample and infer information.
- **Dynamic analysis**: Execute the malware, observe it's behaviour when executed and infer information.
- Both techniques have a set of tools commonly used.

Static analysis

- Analyse by observing sample only. No execution.
- Basic version: quickly confirms if sample is malicious and provides some information on functionality and for generating quick signature.
- Advanced version: Requires analysing instructions and finding out what malware does. No execution again.
- Advanced reveals more information but more difficult and requires more knowledge to perform.

Dynamic analysis

- Analyse by executing malware. Typically done in protected environments like sandboxes and virtual machines.
- View functions executed, system components modified and other effects on the system. Useful for quick understanding and signature generation.
- Advanced - inspect execution, program state etc more closely using a debugger.
- More time consuming and requires very close analysis but reveal more information.

What to choose: static or dynamic?

- **Static**: Reveals lot of information on careful study.
- Requires complex reasoning of program execution since no execution is performed.
- Difficult to perform because manually understanding CPU code is slow process.
- Malware authors use anti-static analysis techniques $\Longrightarrow$ more difficult. Also, somewhat difficult to defeat them.

What to choose: static or dynamic?(cont.)

- **Dynamic**: Easy to reason since program behaviour directly observed.
- Anti-static analysis easily defeated.
- Code coverage is small: code needs to be executed to understand it.
- Anti-dynamic analysis also exist. Easier to overcome than anti-static analysis but definitely slows down process.

What to choose: static or dynamic?(cont.)

- Need both static and dynamic analysis techniques.
- Static can reveal some anti-dynamic analysis techniques and dynamic analysis overcomes some anti-static analysis techniques.
- Often both might need to be performed repeatedly with results from one used for progressing in the other.
- Depends on the goal of analysis.

Malware types

- **Backdoor**: Enables access to computer bypassing existing authentication process.
- **Botnet**: Set of computers infected by an attacker. Controlled through series of commands issued from a control server.
- **Downloader**: Malware that download and installs other malware.
- **Information stealer**: Steal sensitive information(passwords, bank account details or files). Eg: keylogger, sniffer.

Malware types(cont.)

- **Rootkit**: Designed to conceal existence of malware.
- **Worm/virus**: Quickly replicating malware.
- **Spam sender**: Infect a machine and send spam for generating income for spammer.
- **Scareware**: Scare a user into paying money for removing non-existent malware.
- **Launcher**: Used to launch other malware.

Malware types(cont.)

- Broad overview of many possible behaviour in malware.
- Combinations sometime occur. Eg: A botnet used as a downloader to download a backdoor worm with a rootkit.
- Not easy to classify but useful to identify capabilities.
- So don't spend time debating malware classification. Instead focus on more containing the infection.

General tips when analysing malware

- Remember the goal and choose analysis to perform accordingly.
- Not necessary to understand all malware behaviour: focus on key parts. Eg: Malware sleeps 358 times vs malware sends encrypted key presses to attacker every half an hour.
- Many analysis techniques exist: use the best possible and switch if it doesn't work, takes too long etc.
- New anti-analysis techniques developed regularly: need to adapt to these quickly.