Dynamic malware analysis - or: The ~five deadly (anti-)venoms - or: Is this software talking to Asia?

CIRCL
Computer Incident
Response Center
Luxembourg

SECURITY MADE IN LETZEBUERG

Team CIRCL

December 2, 2011

Agenda

- CIRCL Introduction
- Dynamic Malware analysis
  - Introduction
  - Different methods
  - Examples
- Conclusion

CIRCL Mission Statement

- CIRCL is **the national Computer Security Incident Response Team (CSIRT) for the Grand-Duchy of Luxembourg**.
- CIRCL is a team composed of 5 FTEs doing security incident coordination, response and research.
- CIRCL is operated by SMILE ("security made in Lëtzebuerg"), a State funded "groupement d'intérêt économique" (GIE), designed to improve information security and create new opportunities for Luxembourg started in September 2010.

CIRCL - in plain english

- We help you in the (not so unlikely) case of an incident:
  - We do forensic analysis
  - We analyse malware
  - We help you to recover from an incident
  - We give advise for the future
- We do research
- We share our knowledge

Dynamic malware analysis

Introduction

Dynamic malware analysis - Introduction

Driving questions

- Who's behind the attacks?
- What's the motivation?
- What does the malware do?

Dynamic malware analysis - Introduction

Driving questions

- Who's behind the attacks?

$\rightarrow$ The usual cyber criminal

$\rightarrow$ Motivation: money

Dynamic malware analysis - Introduction

Driving questions

- Who's behind the attacks?

$\rightarrow$ Governments or governmental organizations

$\rightarrow$ Motivation: intelligence, sabotage

Dynamic malware analysis - Introduction

Driving questions

- Who's behind the attacks?

$\rightarrow$ Hacktivists: Anonymous, Lulzsec, ...
$\rightarrow$ Motivations: political, 'for the lulz'

Dynamic malware analysis - Introduction

Driving questions

- What does the malware do?
  - Understanding changes on a system:
    - New / changed files,registry
    - Launch / autostart
    - Malicious activity
  - Understanding network activity
    - Communication methods
    - Exfiltration techniques

$\rightarrow$ Necessary for detection and removal

Dynamic malware analysis - Introduction

Why should you be concerned?

- It might be your compromised server / datacenter that is
  → hosting malware to be downloaded / installed by others
  → acting as a C&C server
  → abused as proxy servers

- It might be your customer's computer that is
  → infected and sending information to the attacker

You, your company or your users might
be directly or indirectly a victim

Dynamic malware analysis

Different methods:
Static vs. dynamic analysis

Dynamic malware analysis - Methods

Static analysis

- Looking at a file and concluding about runtime behavior without actually running it
  - File characteristics (GNU strings, meta information, embedded scripts)
  - Result of (multiple) Virus scanners
  - Disassembler
  - Memory forensics
- Problems/Limitations
  - Packers
  - Obfuscated code
  - Encryption
  - Unused code

$\rightarrow$ Necessary step because you cannot trust what you see

Dynamic malware analysis

Static malware analysis examples

1. A current malware variant
2. A 'Screensaver' file

Dynamic malware analysis - Methods

Dynamic analysis

- Running malware in a controlled environment to understand the behavior during runtime
  - Basic training: Mastering the network
  - Drunken boxing: Emulation and shellcode detection
  - Crane technique: Logging API calls, live process information
  - The 36th chamber of Shaolin: Debugger
  - Grand master fight: Virtual machines / sandboxes
- Problems/Limitations
  - Anti-VM
  - Anti-Debugging
  - Turing's Halting problem
  - Need to duplicate the target environment else exploits will not work (OS, patch level, targeted software, mitigation software)

Dynamic malware analysis

Basic training: Mastering the network

- Listening on the network
  - Packet capture
- Faking network services
  - Fake DNS service
  - Accepting and recording traffic on all ports/protocols

$\rightarrow$ Control what kind of data you want to reveal

$\rightarrow$ Don't inform the attacker about your tests

Dynamic malware analysis - Example

Basic training: Mastering the network
Fake-DNS
Socat
Forwarding with IPFW

Dynamic malware analysis

Drunken boxing: Emulation and shellcode detection

- libemu / sctest
  - Detect shellcode by executing code on an emulated x86 processor
- OfficeMalScanner (Frank Boldewin)
  - Dissect MS Office files (Word, Excel, Powerpoint)
  - Find shellcode
  - Build executable containing shell code and payload (works even in cases where an exploit matching environment is not available)
  - Run executable and watch behavior

Dynamic malware analysis - Example

Drunken boxing: Emulation and shellcode detection
Libemu sctest on a Word document
OfficeMalScanner on the same Word document

Dynamic malware analysis

Crane technique: Logging API calls, live process information with MS Sysinternals tools

- Process Explorer
  - Shows detailed information about a running process
    - e.g. icon, command-line, full image path, memory statistics, user account, security attributes, loaded DLLs, operating system resource handles
- Process Monitor
  - API (user-land) monitoring tool
    - Shows real-time file system, registry and process/thread activity, combined with filters

Dynamic malware analysis - Example

Crane technique: Logging API calls, live process information with MS Sysinternal tools
MS Office file from previous example

Dynamic malware analysis

The 36th chamber of Shaolin: Debugger

- OllyDbg, WinDbg, Softice (now Syser), Immunity Debugger
  - Stepping, tracing during execution of a binary
  - Showing all processor registers

Dynamic malware analysis - Example

The 36th chamber of Shaolin: Debugger

Dynamic malware analysis

Grand master fight: Virtual machines / sandboxes

- Putting it all together
  - Virtual machine
  - Host-only networking
  - IP forwarding
  - Fake DNS
- Extend it with
  - Transparent proxy
  - OWASP ZAP
- Capture and control HTTP(S) requests/responses
- Identify Non-HTTP traffic
- Capture all remaining traffic

Dynamic malware analysis - Example

Grand master fight: Virtual machines / sandboxes
Worm.Win32.VBNA.b

Dynamic malware analysis

Conclusion

- Malware analysis is fun
- Try it out
- Protect yourself
  - Don't be careless during analysis
  - You control what you send out and what you accept back
  - Feed your blacklists with your results!
  - Take care of your servers and applications

Q and A - discussion

- Thank you
- info@circl.lu
- `http://www.circl.lu/`
- CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5