Black-box analysis of malware

Vít Bukač

CROCS, Faculty of Informatics, Masaryk University

Supervisor IT Security, CIRT, Honeywell Global Security

CR CS

Centre for Research on
Cryptography and Security

Black-box analysis of malware – Outline

- Lecture
  - Malware
  - Black-box principle
  - Tools
  - Automatic sandbox analysis
- Hands-on lab
  - Analysis of provided malware samples

Malware

Malware definition

"Malware, short for malicious software, is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other intentionally harmful programs. It can take the form of executable code, scripts, active content, and other software. Malware is defined by its malicious intent, acting against the requirements of the computer user — and so does not include software that causes unintentional harm due to some deficiency."
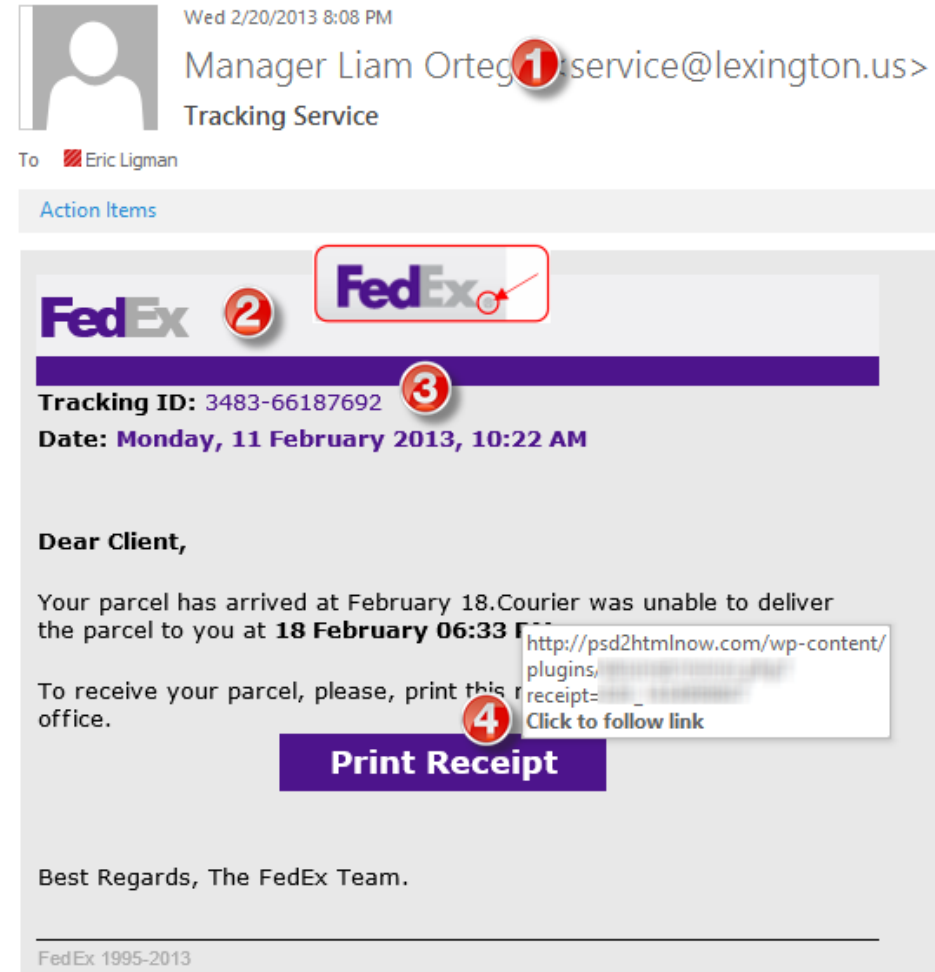
Malware types

- Trojan
- Fake AV
- Backdoor
- Remote Access Tool (RAT)
- Dropper
- Downloader
- Information stealer
- Keylogger

- Ransomware
- Coinminer
- Sniffer
- Virus
- Worm
- Spyware
- Adware
- Botnet

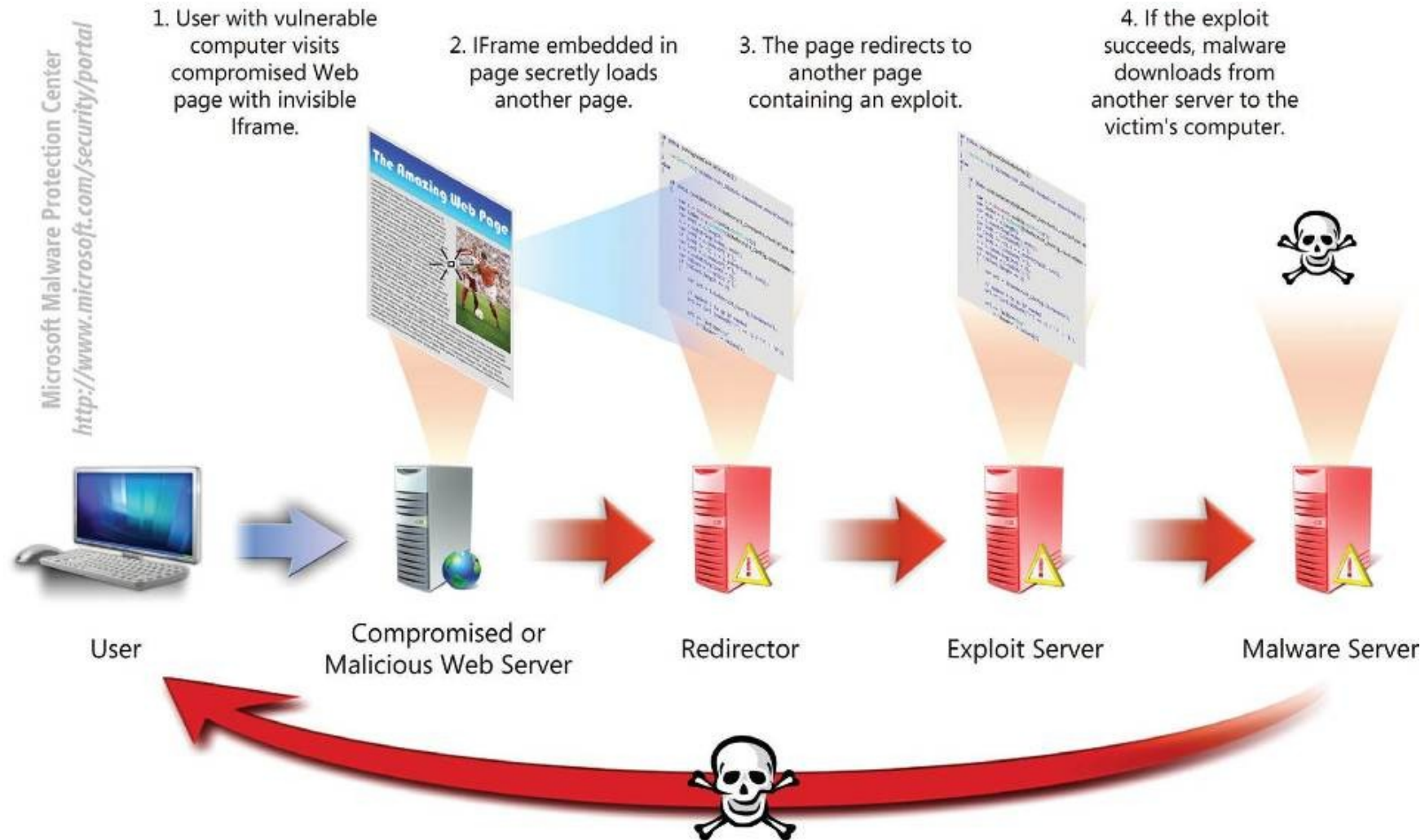# Malware infection vectors

- Email
  - Link
  - Attachment
  - Link + document download
- Malicious website
  - Drive-by download
- USB
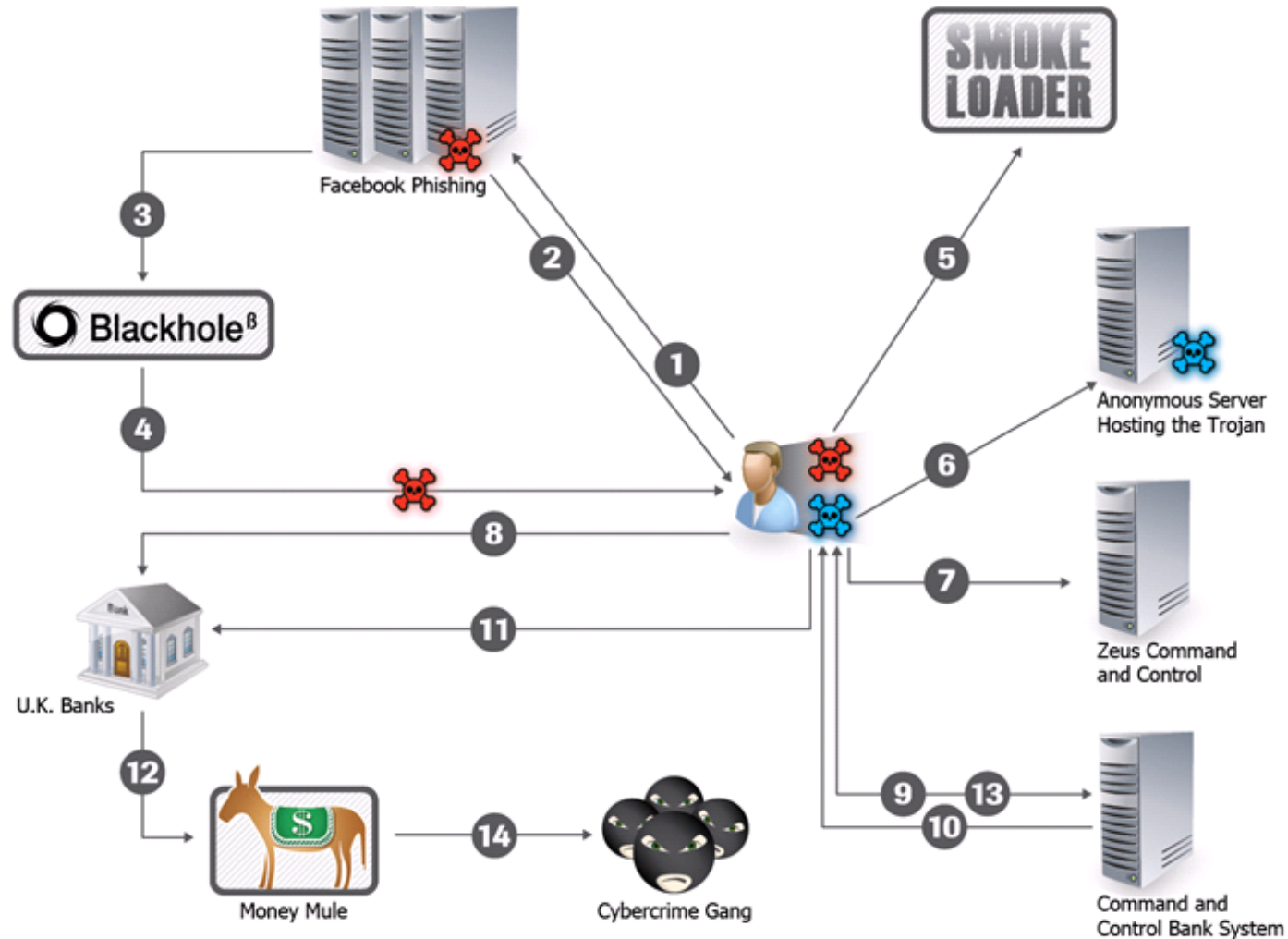- Cracked software
- Worms

Infection vector – Phishing

- Subject
  - "Account blocked"
  - "Package to be delivered"
  - "Expiring subscription"
  - "Invoice" / "Receipt" / "Parchment"
- Signs
  - Unexpected sender address (1)
  - Graphic errors (2)
  - Erroneous info (3)
  - Links to unexpected URL (4)
  - Links to same URL
  - Generic salutation
  - Use of threats, sense of urgency

Infection vector – Drive-by download

1. User with vulnerable computer visits compromised Web page with invisible Iframe.

2. IFrame embedded in page secretly loads another page.

3. The page redirects to another page containing an exploit.

4. If the exploit succeeds, malware downloads from another server to the victim's computer.

The Amazing Web Page

Microsoft Malware Protection Center
http://www.microsoft.com/security/portal

User

Compromised or Malicious Web Server

Redirector

Exploit Server

Malware Server

Example – Zeus infection

Malware Kill Chain + Defense in Depth

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Black box malware analysis

Motivation – Ask the right questions

- What is the scope of compromise? What are 2nd stage callbacks?
- Communication between local file server and an unknown IP address in China has been observed. What process is responsible for the communication?
- Malware is creating temporary files. Where are these files located?
- Malware executable is created again after system reboot. How is it possible and what is causing it?
- A new type of malware has been spreading through internal network. How to quickly assess the malware capabilities? What is its purpose? Is it based on any well-known tool?

Black box malware analysis

- Dynamic analysis – file is executed
- Analysis without internal knowledge
  - Observable inputs
  - Observable outputs
- Quick, simple
- Common monitoring tools
- Collected indicators about
  - Filenames, process names, process parent/child relationships, temporal relationships, domain names, IP addresses, registry keys, persistence methods, cleanup operations etc.
- Can be highly automated

Black box malware analysis – Principle

1. Prepare analysis environment
2. Create snapshot
3. Run monitoring tools
4. Run malware
5. Collect and observe interactions between malware and VM
6. Restore snapshot
7. Repeat 3-6 as needed

Analysis environment

- Virtual Machine
  - Limited/no connectivity
  - Virtualized services (DNS, HTTP,…)
  - Several VMs for various host types
- Software
  - Monitoring tools
  - Often exploited applications
- Risks
  - VM isolation breach
  - Malware inactivity in VM
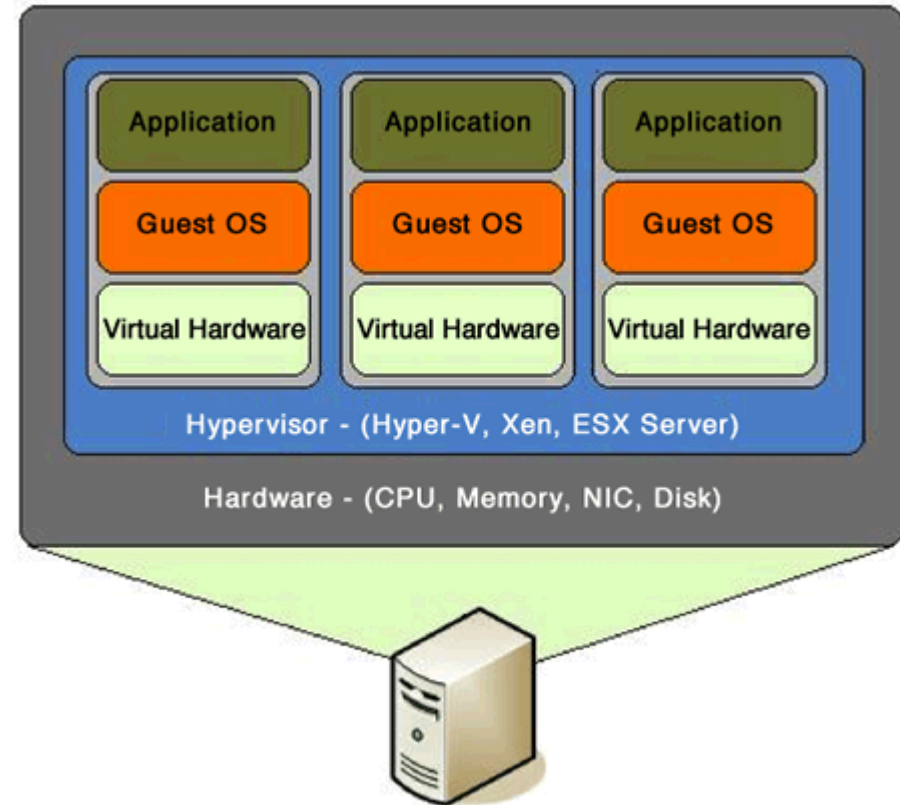
Virtual machine snapshot

- Snapshots
  - Saved state of VM
  - Disk state, memory state
- Quick restoration of previous state
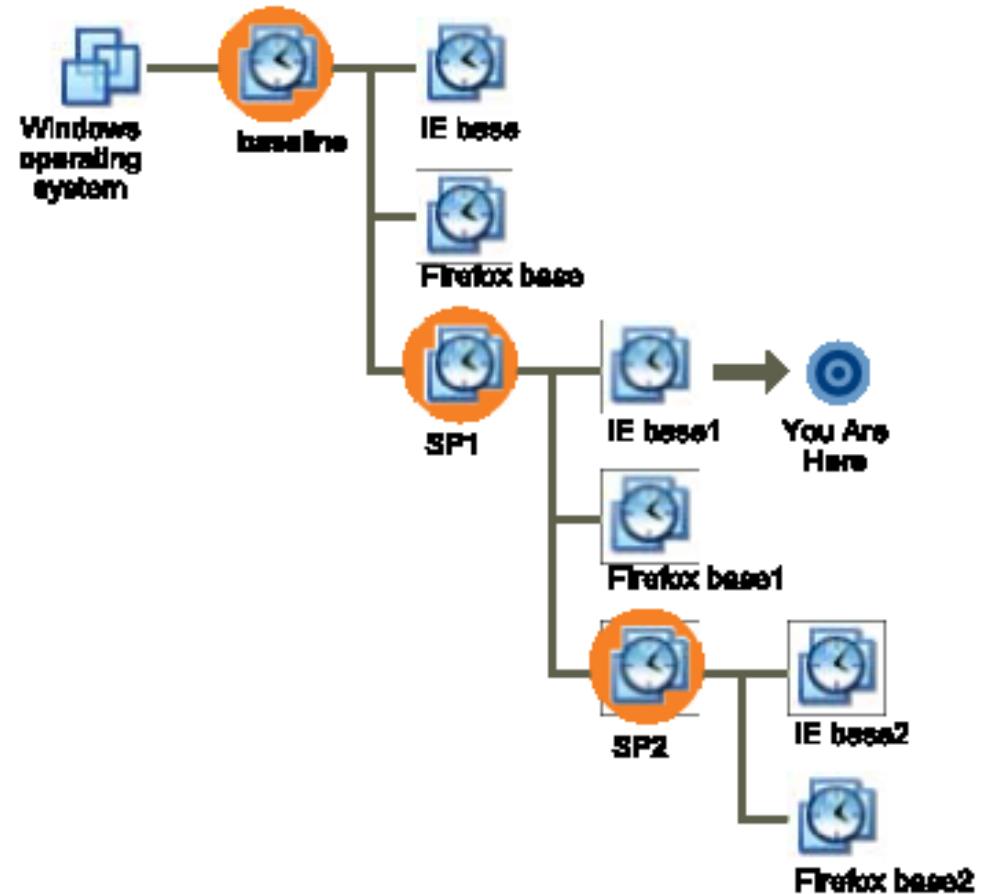
Tools

Network analysis

- Capturing sent/received packets
- Protocol dissection
- Promiscuous mode
- Tools
  - Tcpdump, Wireshark, NetworkMiner
- Indicators
  - Domain names, IP addresses, protocols, ports, HTTP parameters
- Q&A
  - Who is this program communicating with? What reputation does the partner have? What data is exchanged? Is it encrypted or obfuscated?

Network analysis – What to look for

- New established connections – HTTP 80/8080
  - Direct calls for domains without DNS lookup
  - Random domain names (e.g., rpxiodffd.biz)
  - Suspicious domain names (e.g., gooogle.org)
  - Similarly looking domain names (e.g., osinstall.biz, swinstall.biz, swinstall.com)
- Outgoing portscans
- Ping/DNS request for well known services
  - Connection availability test
- Be aware of background OS/processes activities!

Example – Wireshark

File system

- Observing file accesses and modifications
- Background file manipulation
- Tools
  - Procmon, Handle
- Indicators
  - File names, folder names, order of actions, compromise spread through local system
- Q&A
  - Where is malware copied after the initial infection? What filenames are used? Where is the collected data stored?

File system – What to look for

- New file names & folders
  - New created files and folders
  - Batch files (.cmd, .bat, .vbs, .ps1)
  - Known favorite malware file names (e.g., 1.exe, test.exe, new.exe)
  - Known file names in uncommon folders (e.g., C:\Temp\svchost.exe)
  - Recycler
- Modifications of system files
- Temporary storage files, encrypted archives

Example – Procmon

Registry

- Regedit
- RegRipper
- Autoruns

Registry – What to look for

- Well-known locations
  - Autorun locations
  - Task scheduler
- Changes tracking
- Keywords fulltext search
 - Filenames
  - Processes
  - Domain names

ThreatExpert

Submission Summary:

- The newly created Registry Values are:
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center]
    - UacDisableNotify = 0x00000001
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center\Svc]
    - AntiVirusOverride = 0x00000001
    - AntiVirusDisableNotify = 0x00000001
    - FirewallDisableNotify = 0x00000001
    - FirewallOverride = 0x00000001
    - UpdatesDisableNotify = 0x00000001
    - UacDisableNotify = 0x00000001

to disable notification of firewall, antivirus and/or update status through the Windows Security Center
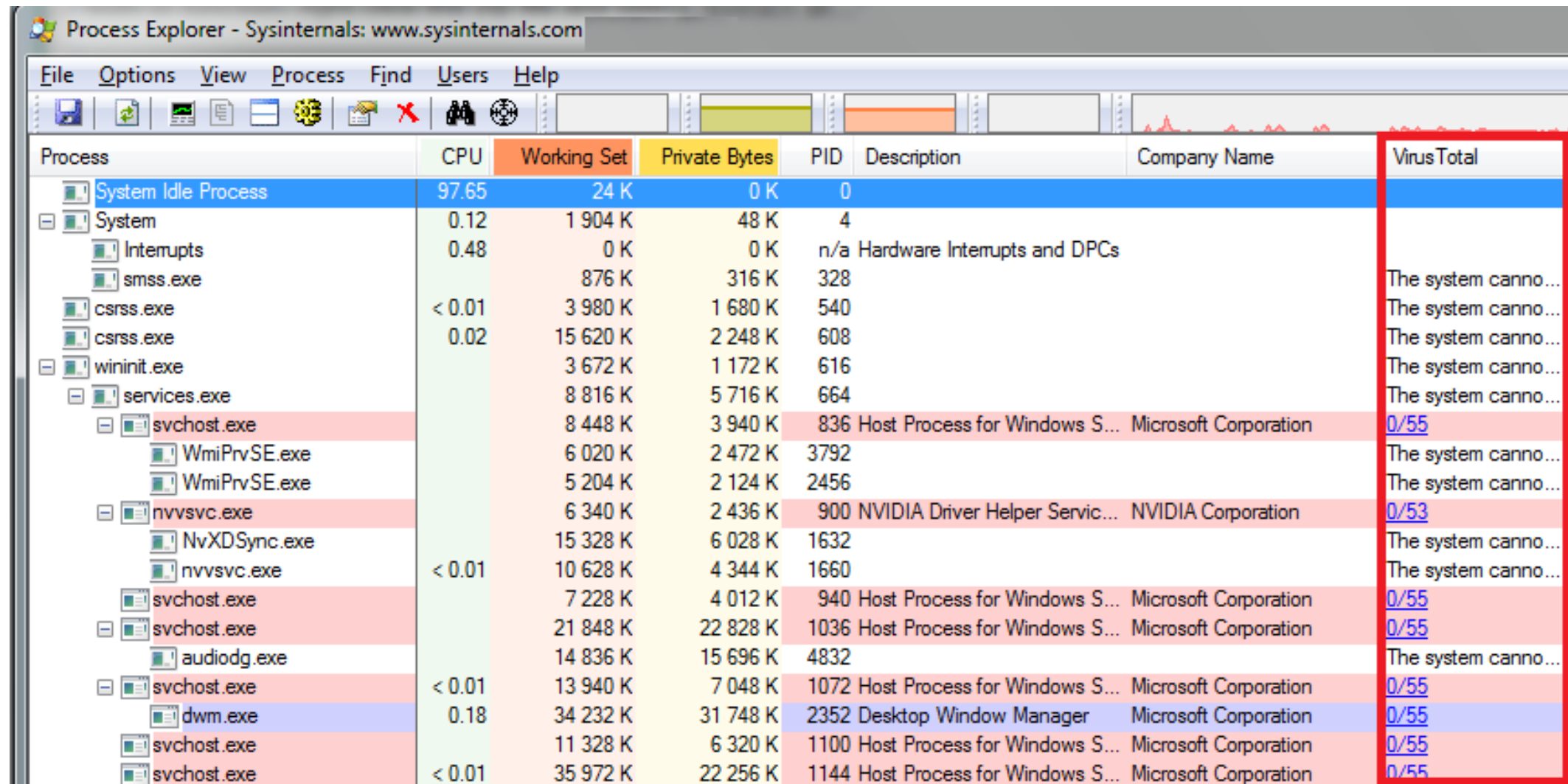
Registry – Regedit
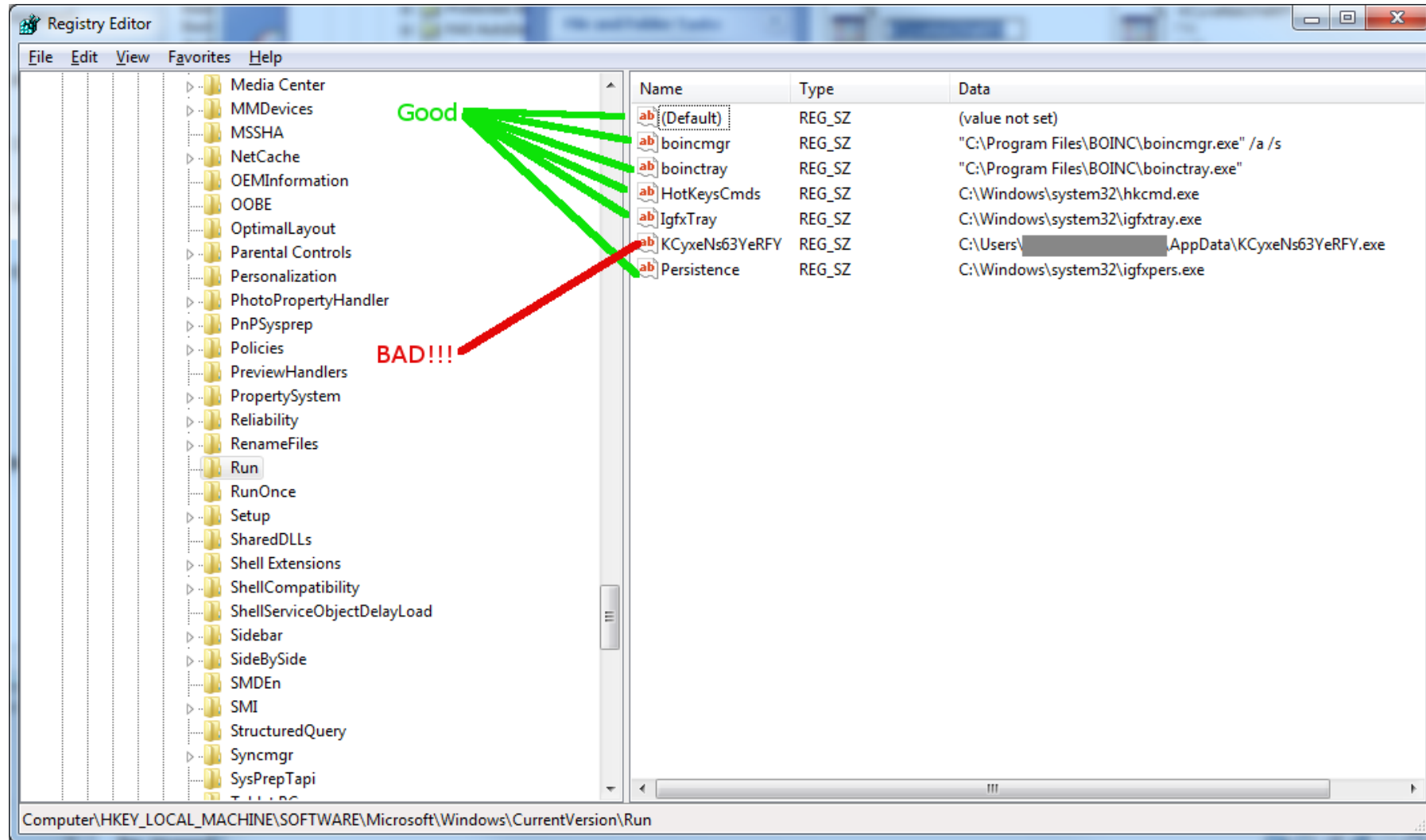
Processes

- Observing initial system compromise
- Processes parent/child relationships
- Tools
  - Process Explorer, Procmon
- Indicators
  - Process names, order of execution, dropper activity
- Q&A
  - What processes are run after malware binary is executed? Are batch files involved? Are there watcher processes?

Processes – What to look for

- Order of executables
  - Initial malware
  - Dropper/downloader
  - Persistence executable
  - Final malware
- Command line interpreters
  - cmd.exe
  - **Powershell**
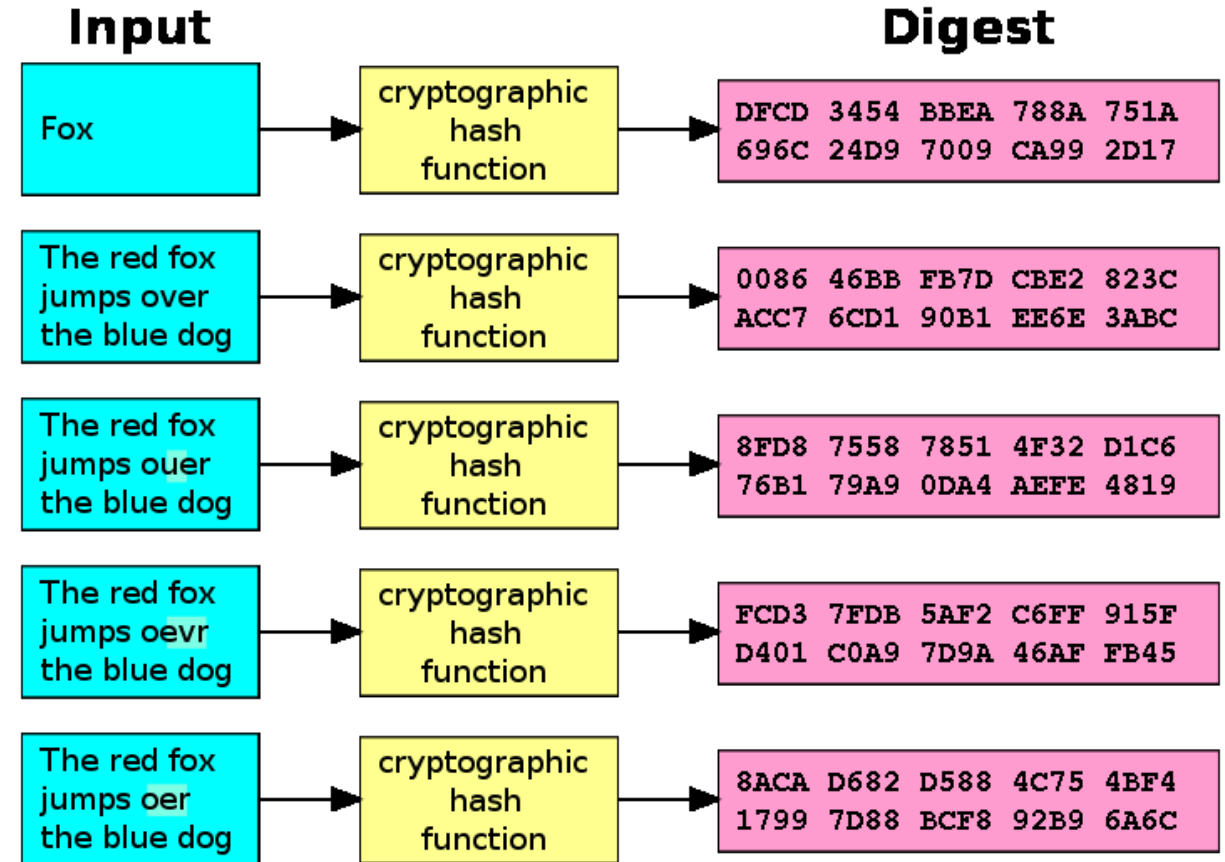 - Cscript, wscript

Example – Process Explorer

Executable file analysis

- Cryptographic hash
  - Hash function which is considered practically impossible to invert
  - Unique identification of file
  - Counter: Polymorphism
  - MD5, SHA1
- Fuzzy hash
  - Context triggered piecewise hash
  - Families of files
  - ssdeep
- Strings

Input

| Fox |
| cryptographic hash function |

Digest

DFCD 3454 BBEA 788A 751A
696C 24D9 7009 CA99 2D17

The red fox jumps over the blue dog

cryptographic hash function

0086 46BB FB7D CBE2 823C
ACC7 6CD1 90B1 EE6E 3ABC

The red fox jumps ouer the blue dog

cryptographic hash function

8FD8 7558 7851 4F32 D1C6
76B1 79A9 0DA4 AEFE 4819

The red fox jumps oevr the blue dog

cryptographic hash function

FCD3 7FDB 5AF2 C6FF 915F
D401 C0A9 7D9A 46AF FB45

The red fox jumps oer the blue dog

cryptographic hash function

8ACA D682 D588 4C75 4BF4
1799 7D88 BCF8 92B9 6A6C

Example – Strings

server.exe

AppData

4bcce4de98bcdb4d29f66c0fe1ffe002

hackerhani.no-ip.biz   Domain name

Software\Microsoft\Windows\CurrentVersion\Run   Persistence registry key

Software\

yy-MM-dd

??-??-??

Microsoft

Windows

SystemDrive

netsh firewall delete allowedprogram "   Commands to be executed

Software

cmd.exe /c ping 0 -n 2 & del "

SEE_MASK_NOZONECHECKS

netsh firewall add allowedprogram "

MD5: 5d347384ea978a96bc842ad9f29e95f2

Analysis

Black box analysis – indicator interpretation

- Network analysis – domain & IP verification, processes communicating
- Hash comparison
  - Collisions, same-hash files
- Behavior analysis
  - System processes, created processes, persistence
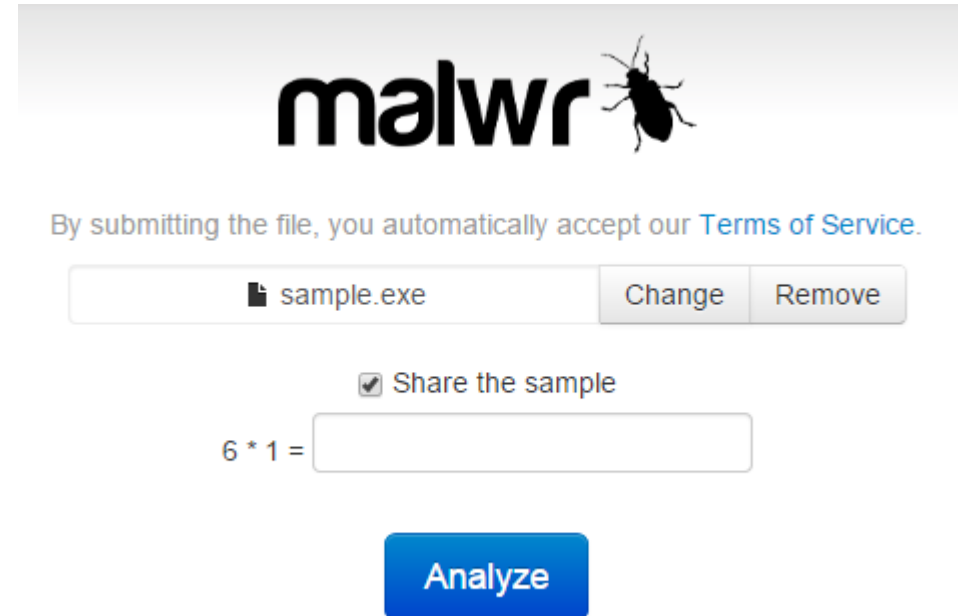- File manipulation

Document analysis – Quick insight

- EXIF information

- File metadata

- Document sandboxing

- Document interpretation ambiguity

- Practical examples
  - Double extensions, different content in different viewers, code block obfuscation & hiding

Automated sandbox analysis

Automated sandboxing

- Automated
  1. Execute malware in sandbox
  2. Wait a few seconds
  3. Receive summary report
  4. Investigate report
- Non-interactive
- Known tools
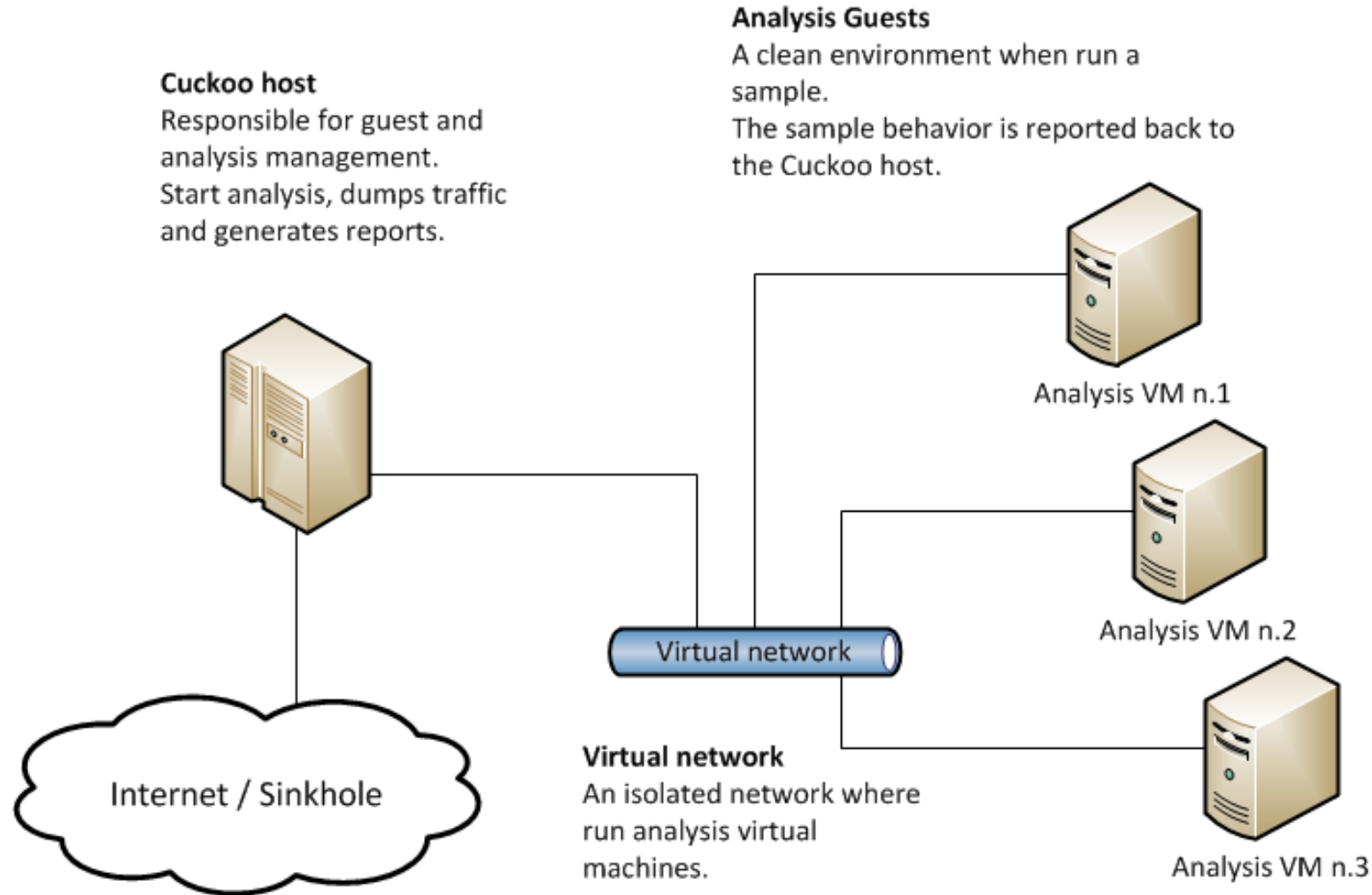 - Cuckoo, Norman, Anubis etc.

malwr

By submitting the file, you automatically accept our Terms of Service.

sample.exe | Change | Remove

☑ Share the sample

6 * 1 =

Analyze

Cuckoo sandbox

- Open source malware analysis system
- Can analyze
  - Windows executables, DLLs, PDF documents, URLs, HTML files, PHP scripts, Visual Basic scripts, ZIP archives, Python files, etc.
- Modular, scriptable
- Full memory dump (for Volatility Framework)
- Django web interface
- Mongo (NoSQL) database

Cuckoo – Architecture

Cuckoo host
Responsible for guest and analysis management.
Start analysis, dumps traffic and generates reports.

Analysis Guests
A clean environment when run a sample.
The sample behavior is reported back to the Cuckoo host.

Analysis VM n.1

Analysis VM n.2

Virtual network

Virtual network
An isolated network where run analysis virtual machines.

Internet / Sinkhole

Analysis VM n.3

Cuckoo – GUI

	Info	File	Signatures	Screenshots	Static	Dropped	Network	Behavior

Category	Started On	Completed On	Duration	Cuckoo Version
FILE	2013-05-09 20:47:13	2013-05-09 20:49:56	163 seconds	0.5

File Details file indicators

File name	7351eaee39eb672c00c1dbe1e525a9e0
File size	303104 bytes
File type	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
CRC32	D45DD4BC
MD5	7351eaee39eb672c00c1dbe1e525a9e0
SHA1	f5f06f53f270f1fd044da1da9eea5b59794bc346
SHA256	078ae46df0b431c7d423568495ee01caaf9d024aaf880061c739cfeb4dbf4490
SHA512	950a5e85b4f161578660179eb2afe95798edaebf1b2998702c1250fea613c3b95b9143e643994ebad67e08702ddab47a6accb4b25c9f2d7a3d19fa3ca1b8cbf7
Ssdeep	None
PEiD Signatures	None matched
Yara Signatures	
Antivirus Results	25/46 (collapse)

Internet sandbox services

- Public service
  - OpSEC issues
- Huge comparison database
- Exact match by hash
- Similarity search by keywords

- Malwr.com (public Cuckoo sandbox)
- VirusTotal.com
- ThreatExpert.com
- Hybrid-Analysis.com

Operational security (OpSec)

- Advanced attackers monitor victim's actions
  - Unique indicators visible on Google?
  - Attacker host monitoring for incoming traffic
  - Keywords search in mails, PDFs…
- Basics of OpSec
  - "Think before you act" mentality
  - Limited information sharing
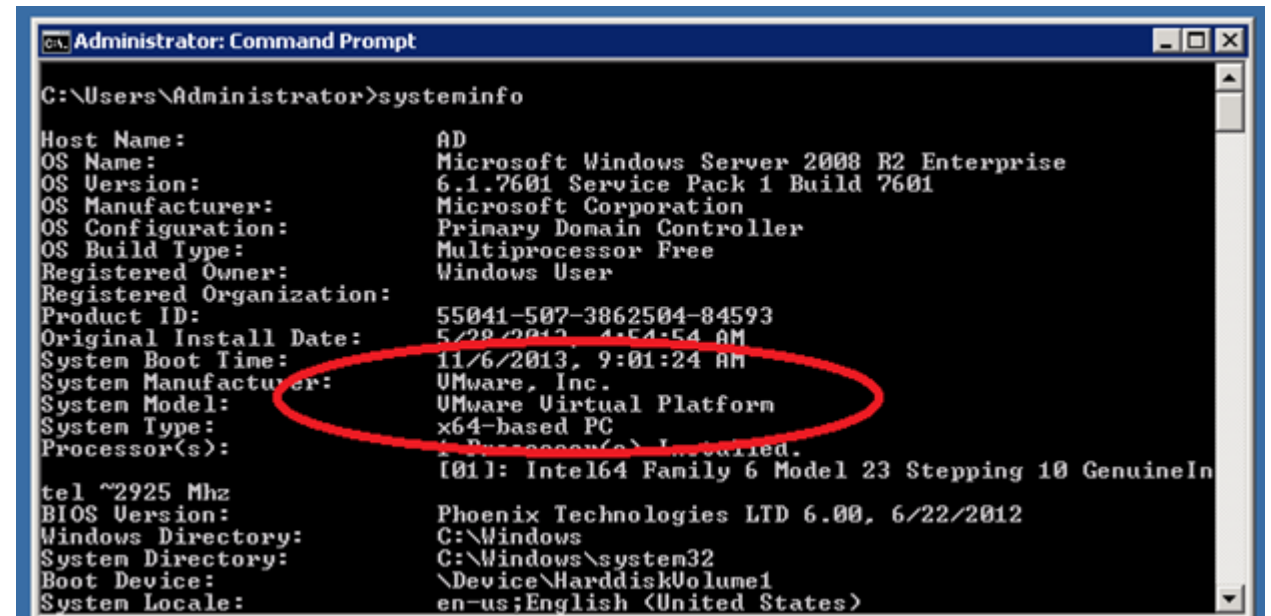 - Trace removal
- PassiveTotal.org

OpSec – Basic rules

- No ping
- No DNS lookup
- No accessing to suspicious domains
- No premature remediation steps (reboot, antivirus scan, OS reinstall)
- No upload of samples
- No indicator validation on external sources

- NOT EVEN through 3rd parties

Anti-sandbox techniques

- Continuous development – sandbox vs. anti-sandbox
- Malware inactive in analysis environment
- Tools presence detection (Wireshark, etc.)
- Virtualization detection
  - Registry (key existence, key value)
  - File system (file existence, drivers)
  - Processes (syscall response)
- Human presence detection
  - Mouse movement
  - Keyboard activity
  - File artefacts

Lab

Lab – Overview

- Hands-on experience of manual black-box analysis
- Guided analysis of selected malware samples
- Tools
  - Wireshark – Network activity
  - Process Monitor – File system activity, process creation
  - Autoruns – Persistence
  - Regshot – Registry changes
  - Process explorer – Process map

Lab – Samples

- 2-3 samples from different malware families
  - Commodity malware – Zeus, ZeroAccess, Generic Trojans,...
- Students will execute samples in virtual environment
  - Provided simple analysis virtual machine (Windows)
  - Indicators collected – network, files, persistence
  - Discussion about interpretation of facts
- Homework
  - 2 samples for analysis independently
  - Write a cohesive report and present key information to the reader