Malware Analysis (CS6038)

Week 01.2 Intro to Malware

Scott Nusbaum
nusbausa@ucmail.uc.edu

January 17, 2019

University of CINCINNATI

Overview

- Distribute the Windows OVA and Kali Linux
- What is Malware
- Types of Malware
- Types of Malware Analysis (Overview)
- Indicators of Compromise (IOCs)

University of CINCINNATI

Windows OVA’s

- Microsoft provides free virtual images for their browsers
  - These VM images are good for 90 days
- When developing a home lab it is nice to have an image that is up to date and valid
- This will be used throughout the rest of the class.
  - The first homework assignment is to setup a safe working environment.
    - This will be repeated after the 90 days has expired.

University of CINCINNATI

Kali Linux

- A linux distribution designed to aid in Security Related “Research”
- https://www.kali.org/
- Contains a large number of free or open source tools

Malware

- What is Malware?

Malware

WIKI’s Definition:

> “**Malware** (**malicious software**) is any software intentionally designed to cause damage to a computer, server, client, or computer network.[1] Malware does the damage after it is implanted or introduced in some way into a target's computer and can take the form of executable code, scripts, active content, and other software.[2] The code is described as computer viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware, among other terms. Malware has a malicious intent, acting against the interest of the computer user—and so does not include software that causes unintentional harm due to some deficiency, which is typically described as a software bug.”

Malware

My definition is simpler

“Any software that can be used maliciously”

- Mis-configured applications can grant attackers access to the system
- Once attackers have system access, they can use the default system applications to
  - Gather Information about the system
  - Pivot to other connected system
  - Elevate privileges on the existing system
  - Hide their actions

Malware

Is only the Windows OS affected by Malware?

Malware

Types of system that can be affected

- IOT
- Networking Equipment
- Android
- iOS
- iPhone
- Linux
- Web Applications

Processors that can be affected

- x86/x64
- arm
- powerPC
- mips

* Lists are not comprehensive

Types of Malware

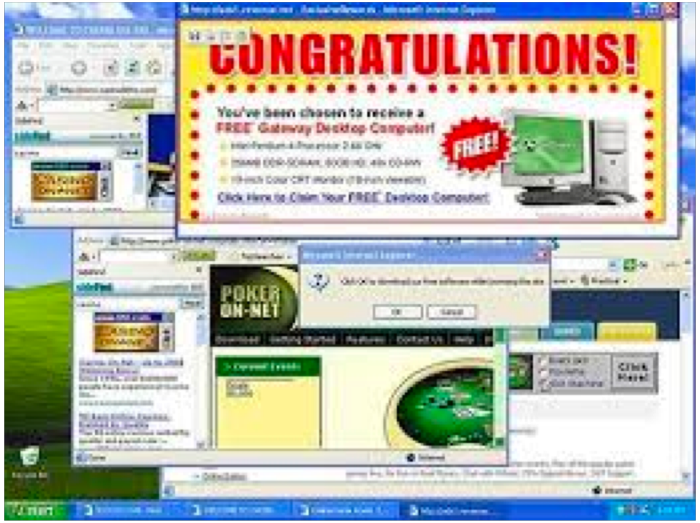
University of CINCINNATI

Types of Malware

- Adware
- Bots
- Ransomware
- Rootkit
- Spyware
- Trojan Horse
- POS
- Virus
- Worm
- Keyloggers
- Memory Scrapers
- Browser Hijacker
- Rogue Security Software

Adware

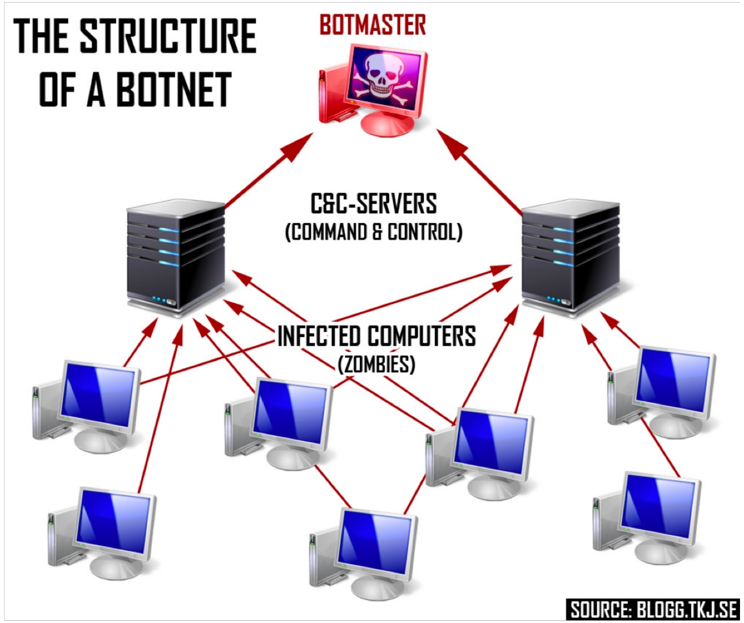
Displays annoying advertisements on the infected system


CONGRATULATIONS!
You've been chosen to receive a FREE* Gateway Desktop Computer!
FREE!
Click Here to Claim Your FREE* Desktop Computer!
POKER ON-NET
Click Here!

University of CINCINNATI

Bots

- A bot is simply an automated operation.
- BotNets are when the bots are combined in a distributed network.
- These networks can be used to perform DDOS, send mass emails or automated exploitations



SOURCE: BLOGG.TKJ.SE

University of CINCINNATI

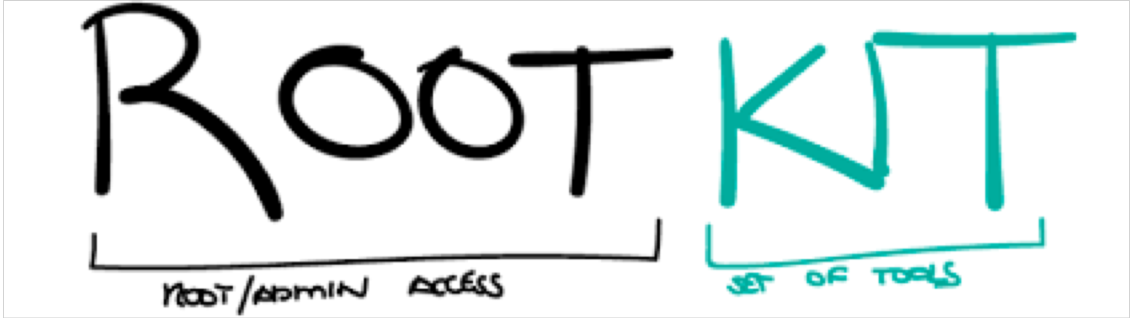
Ransomware

- Encrypts the files on the target system.
- Targets specific file types.
- Leaves a message with instructions on how to receive the decryption key.

University of CINCINNATI

Rootkit

- Designed to install itself into the Kernel of the OS and patch hooks that would be able to detect it.



Spyware

- Designed to gather information about the user and the systems they infect

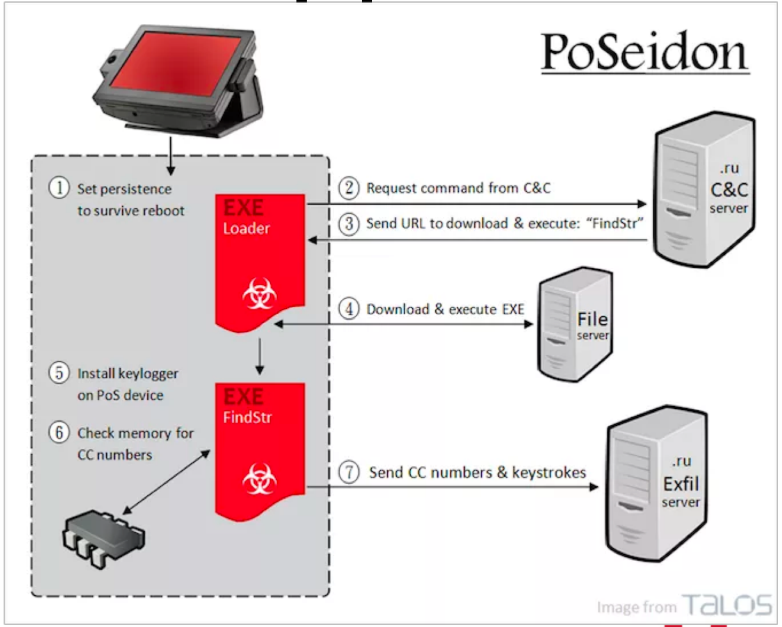
Trojan

- Malicious software that is presented as benign software.
- Can be in the form of:
  - Attachment
  - Links
  - Fake advertisements
  - Games
  - Executables
  - Security Products

University of CINCINNATI

POS / Memory Scrappers

- Point of Sale (POS) Malware target the retail industry.
- In general scans memory of the infected system searching for credit card numbers.


PoSeidon
1 Set persistence to survive reboot
EXE Loader
2 Request command from C&C
3 Send URL to download & execute: "FindStr"
.ru C&C server
4 Download & execute EXE
File server
5 Install keylogger on PoS device
6 Check memory for CC numbers
EXE FindStr
7 Send CC numbers & keystrokes
.ru Exfil server
Image from TALOS

University of CINCINNATI

Virus

- Software that when executed attempts to replicate itself by modifying other computer programs by adding its own code.

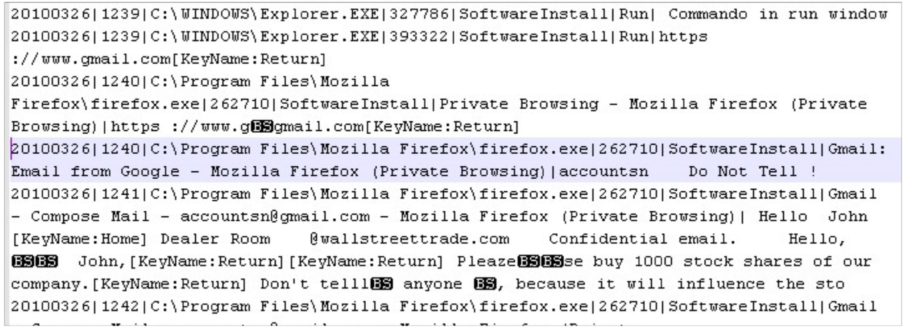
Worm

- Software with the main purpose of replicating.
- Worms will normally search a network looking for a specific known security vulnerably and then attack infecting that system(s)

University of CINCINNATI

Keylogger

- Software that logs all keys pressed by the user
- Output is normally logged to a txt file or an encrypted file on the system until ready to exfil
- They range in sophistication
- Keyloggers can be software or physical
- They can also be targeted against specific apps.
  - Web based: ie Form Grabbing
  - Kernel or Userland
  - Hypervisor based
- Output can often be difficult to read



```
20100326|1239|C:\WINDOWS\Explorer.EXE|327786|SoftwareInstall|Run| Commando in run window
20100326|1239|C:\WINDOWS\Explorer.EXE|393322|SoftwareInstall|Run|https
://www.gmail.com[KeyName:Return]
20100326|1240|C:\Program Files\Mozilla
Firefox\firefox.exe|262710|SoftwareInstall|Private Browsing - Mozilla Firefox (Private
Browsing)|https ://www.gBSgmail.com[KeyName:Return]
20100326|1240|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail:
Email from Google - Mozilla Firefox (Private Browsing)|accountsn    Do Not Tell !
20100326|1241|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
- Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)| Hello  John
[KeyName:Home] Dealer Room    @wallstreettrade.com    Confidential email.     Hello,
BSBS  John,[KeyName:Return][KeyName:Return] PleazeBSBSse buy 1000 stock shares of our
company.[KeyName:Return] Don't telllBS anyone BS, because it will influence the sto
20100326|1242|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
```

Browser Hijacking

- Software that modifies the browsers
- Modifications can include:
  - Injecting Advertisements
  - Site Scrappers
  - New Search engines
  - Generate traffic to specific sites

Rogue Security Software

An application that pretends to be an anti-virus or some other utility to help the user. Instead it is contains malware.

- I’ve seen samples that do clean up the system
- They look in the registry for autorun and remove them

Modern Malware

- More modular
- More developed infrastructure
- More complex communication protocol

Malware Phases

- Exploitation
- Installation
- Command and Control (C&C, C2)
  - Malicious actions

Exploitation

- Weaponization of an vulnerability
  - 0-day
- Initial interaction between the attacker and the target
- Often initiated through phishing or drive by downloads
- Exploit code will gain remote code execution (RCE)
  - Next step is to install a stager to gain persistence (Installation)

Installation

- Persistence
  - The method of gaining permanent execution on a target system.
- Exploit code doesn’t provide persistence
  - This is done by downloading a stager.
  - The stager can work in multiple ways.
    - Download more malware in the form of an exe
    - Download shellcode (SC) that installs itself and dumps an exe
- Droppers
  - Goal is to either extract from itself an executable or to download, from the C&C, an executable then write it to disk

Command & Control

- This is how the attacker controls the malware.
- C&C's is controlled by the attacker and is used to send commands to the infected systems
- Download of modules that are specific to the attackers goals
  - Modules can be stored on disk or in memory

Malware Infrastructure

- Walk through the Trickbot Infrastructure
  - Infected system contains config files of known C2’s
  - C2’s instruct system what to do and where to down load other components, configs, or even new version of malware
  - Each Module downloaded contains a config file with addresses of their own C2’s and where to upload information.
  - Exfil of data doesn’t have to be the normal C2

Types of Malware Analysis

- Static
  - Study of the malware sample without execution
- Dynamic
  - Study of the malware sample through execution and recording or logging its execution path and generated artifacts
- Hybrid
  - Study using both static and dynamic methods. Normally involves multiple rounds of execution.

Indicators of Compromise

- Files, resources, URL, IP addresses, registry entries, System events, network traffic or any artifact that indicate a potential infection