INFOSEC INSTITUTE INTENSE SCHOOL CERTIFICATION TRACKER

INFOSEC INSTITUTE

TOPICS ▾ CONTRIBUTORS CONTENT ARCHIVES ▾

JOB BOARD CAREERS PHISH.IO

MALWARE RESEARCHER'S HANDBOOK - PART 1

Malware Researcher's Handbook: Introduction

JUMP TO SELECT POST SECTION ▾

Tweet 7 Share 111 Share 1 reddit 113 Like

All the Stuff You Know Before Starting Research

Malware research contains a lot of information like reverse engineering, exploit-kit, exploit analysis, botnet analysis, emulation, sandbox, Trojan, Virus, key logger and much more. This is an overview of the research topics in the field of information security. However, before exploring research, we should understand the basics of malware research. So first, we will discuss some of the basics and will go in-depth later on.

Therefore, I will discuss some basic terminology.

Malware: malicious software with unknown functionality that is resident on a system. Any software that does something that causes harm to a user, computer, or network can be considered malware, including viruses, Trojan horses, worms, rootkits, shareware, and spyware.

Virus: A type of malware that replicates, commonly by infecting other files in the computer, thus execution of malware code and its propagation when those files are activated.

Worm: A worm is self-propagating programs that can run automatically to distribute itself from one computer to another. Worms may propagate themselves using agents like Trojan, Backdoor etc…

Typical examples are below:

- Bagle
- Blaster
- Conflicker etc.

Trojan: A malicious software that is able to replicate or spread contain malicious code, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. Typical examples are below:

1. Netbus Advance System Care(by Carl-Fredrik Neikter)

2. Subseven or Sub7(by Mobman)
3. Back Orifice (Sir Dystic)
4. Beast
5. Zeus
6. Flashback Trojan (Trojan BackDoor.Flashback)
7. ZeroAccess
8. Koobface
9. Vundo and many more

The various malicious activities by Trojans are:

- Crashing the computer, e.g. with "blue screen of death" (BSOD)
- Data corruption
- Formatting disks, destroying all contents
- Use of the machine as part of a botnet (e.g. to perform automated spamming or to distribute Denial-of-service attacks)
- Electronic money theft
- Infects entire Network banking information and other connected devices
- Data theft, including confidential files, sometimes for industrial espionage, and information with financial implications such as passwords and payment card information
- Modification or deletion of files
- Downloading or uploading of files for various purposes
- Downloading and installing software, including third-party malware and ransomware
- Keystroke logging

- Watching the user's screen
- Viewing the user's webcam
- Controlling the computer system remotely

Backdoor: Malicious code that installs itself onto the computer as the part of malware that spreads to allow the attacker access. It usually let the attacker to connect the computer or victim with or without authentication to execution command.

Ex: backoffice etc..

Bot: A malicious program installed on a computer that is a part of bot network (BOTNET) command and control center. Bots are generally backdoor Trojans that allow unauthorized access and control of an affected computer. They are often IRC channel bots in the network.

EX: Zeus botnet, Torpig etc..

We will discuss types of botnet attacks with real examples and how to identify them.

Downloader: Malicious code that exists only to download other malicious code. Downloaders are commonly installed by attackers when they first gain access to a system. This attack can easily be created with some kind of JavaScript on a live website that has vulnerabilities.

Rootkit: Malicious code designed to conceal the existence of other code. Rootkits are usually paired with other malware, such as a backdoor, to allow remote access to the attacker and make the code difficult for the victim to detect. We will discuss more about rootkit in the upcoming article.

Scareware: Malware designed to frighten an infected user into buying something. It usually has a user interface that makes it look like an antivirus or other security program. It informs users that there is malicious code on their system and that the only way to get rid of it is to buy their “software,” when in reality, the software it’s selling does nothing more than remove the scareware.

Spam-sending malware: Malware that infects a user’s machine and then uses that machine to send spam. This malware generates income for attackers by allowing them to sell spam-sending services.

Exploit: An exploit is a piece of software, a command, or a methodology that attacks a particular security vulnerability. Exploits are not always malicious in intent—they are sometimes used only as a way of demonstrating that vulnerability exists. However, they are a common component of malware.

Exploit Kit/Exploit Packs: An exploit kit, sometimes called an exploit pack, is a toolkit that automates the exploitation of client-side vulnerabilities, targeting browsers and programs that a website can invoke through the browser. Common exploit targets have been vulnerabilities in Adobe Reader, Java Runtime Environment, and Adobe Flash Player:

Reverse Engineering Malware: Reverse engineering malware is a process of examining malicious executable by reading instruction. We are reading assembly language instruction by IDA pro or debugging through Immunity or Ollydbg, we will discuss Reverse engineering separately as a series. Here we are trying to read machine level language by the Disassembler.

Why Malware Analysis is required:

If you still don’t know why, then you are at risk. Malware analysis is the art of dissecting malware to understand how it works, how to identify it, and how to defeat or eliminate it. In addition, you don’t need to be an uber-hacker to perform malware analysis.it gives the below answers:

- Knowing how to analyze malware can help you understand the context of the incident, its severity, and repercussions. It can help you

plan your response to contain the incident's scope and, in some cases, understand what entities might be behind the intrusion.
- Knowing how to analyze malware can bring an element of control into an otherwise chaotic environment that exists around a security incident. It's also a critical aspect of modern forensic analysis actions, because it's all too frequent for investigators to discover malware on the compromised systems.
- To assess damage
- To discover indicators of damage
- Properly handle Incident and how to respond it
- What did they steal
- How did it get here
- Purpose of malware
- To catch the bad guy and so on…

Types of Malware Analysis:

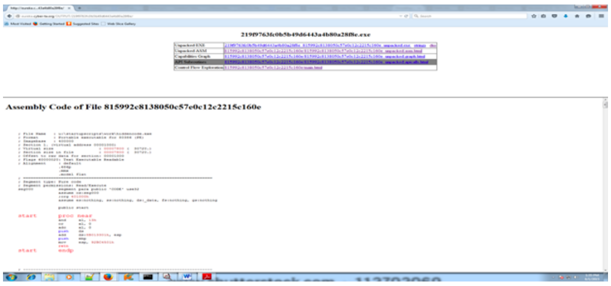
After being infected by malware, as Incident Responder or forensic analyst how to find the root cause of attack.so here we will discuss the steps of malware analysis.

Fully Automated Analysis:

The easiest way to assess the nature of a suspicious file is to scan it using fully automated tools, some of which are available as commercial products and some as free ones. These utilities are designed to quickly assess what the specimen might do if it ran on a system.

They typically produce reports with details such as the registry keys used by the malicious program, its mutex values, file activity, network traffic, etc.but we can't know the internal behaviors of malware. Some of tools are Cooko, XecScan

The below is snapshot of online scanner by eureka.same services can be available by Threat Expert etc..



219f9763fc0b5b49d6443a4b80a28f8e.exe

Unpacked EXE	[illegible]
Unpacked ASM	[illegible]
Capabilities Graph	[illegible]
API Subroutines	[illegible]
Control Flow Exploration	[illegible]

Assembly Code of File 815992e8138050e57e0c12e2215c160e

Static Properties Analysis:

An analyst interested in taking a closer look at the suspicious file might proceed by examining its static properties. Such details can be obtained relatively quickly, because they don't involve running the potentially malicious program. Static properties include the strings embedded into the file, header details, hashes, embedded resources, packer signatures, metadata such as the creation date, etc.

Manual Code Reversing/Dynamic Analysis:

Reverse engineering the code that comprises the specimen can add valuable insights to the findings available after completing interactive behavior analysis.

Manual code reversing involves the use of a disassembler and a debugger, which

could be aided by a decompiler and a variety of plugins and specialized tools that automate some aspects of these efforts. Memory forensics can assist at this stage of the pyramid as well.
it provides the below benefits

- Decoding encrypted data stored or transferred by the sample;
- Determining the logic of the malicious program’s domain generation algorithm;
- Understanding other capabilities of the sample that didn’t exhibit themselves during behavior analysis.

Behavioral Analysis:

Behavioral analysis involves examining how sample runs in the lab to understand its registry, file system, process, and network activities. Understanding how the program uses memory (e.g., performing memory forensics) can bring additional insights. This malware analysis stage is especially fruitful when the researcher interacts with the malicious program, rather than passively observing the specimen

Next Section: We will discuss about PE file format details.

NEXT: MAL...

Revers3r is a Information Security Researcher with

AUTHOR

Revers3r

considerable experience in Web Application Security, Vulnerability Assessment, Penetration Testing. He is also well-versed in Reverse Engineering, Malware Analysis. He's been a contributor to international magazines like Hakin9, Pentest, and E-Forensics. In his free time, he's contributed to the Response Disclosure Program. website: www.vulnerableghost.com

Malware Researcher's Handbook (Demystifying PE File)

When Your CEO Won’t Take Security...

InfoSec Institute: Top Training Company 2015

What Is a SIEM?

Comments for this thread are now closed. ×

0 Comments InfoSec Institute Resources Login

Recommend Share Sort by Best

This discussion has been closed.

ALSO ON **INFOSEC INSTITUTE RESOURCES** WHAT'S THIS?

ISIL, Terrorism and Technology: A Dangerous Mix

2 comments • 10 days ago

Pierluigi Paganini — Regarding the Snowden's case there is no political discussion about it, I just just observed …

Analyzing a DDoS Trojan

1 comment • 10 days ago

Eduard Abramovich — Hi, I am just starting with these kind of security analysis. My questions are, where did you get the …

Subscribe Add Disqus to your site Privacy DISQUS

About InfoSec

InfoSec Institute is the best source for high quality information security training. We have been training Information Security and IT Professionals since 1998 with a diverse lineup of relevant training courses. In the past 16 years, over 50,000 individuals have trusted InfoSec Institute for their professional development needs!

Connect with us

Stay up to date with InfoSec Institute and Intense School - at info@infosecinstitute.com

Like 555

Follow @infosecedu

Join our newsletter

Get the latest news, updates & offers straight to your inbox.

ENTER Y(SUBSCRIBE