- Filename: eccouncil-ceh31250-v10-7-1-1-malware-threats
- Show Name: CEHv10 (312-50)
- Topic Name: Malware Threats
- Episode Name: Malware Threats
- Description: In this episode, Adam and Wes discuss the various Malware threats that can be used to attack a system.

==========

CEH v10 - Module 07 - Malware Threats

What is Malware?

Any software intentionally designed to cause damage to a computer, server or computer network. 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.

Malware Types:

Virus - A computer virus is designed to spread from host to host and has the ability to replicate itself. Computer viruses cannot reproduce and spread without help. A virus operates by inserting or attaching itself to a legitimate program or document in order to execute its code. Once a virus has successfully attached to a program, file, or document, the virus will lie dormant until circumstances cause the computer or device to execute its code. In order for a virus to infect your computer, you have to run the infected program, which in turn causes the virus code to be executed.

Macro virus - A virus written in a macro language and that is platform independent. Since many applications allow macro programs to be embedded in documents, the programs may be run automatically when the document is opened. This provides a distinct mechanism by which viruses can be spread.

Compression viruses - Another type of virus that appends itself to executables on the system and compresses them by using the user's permissions.

Stealth virus - A virus that hides the modifications it has made. The virus tries to trick antivirus software by intercepting its requests to the operating system and providing false and bogus information.

Polymorphic virus - Produces varied but operational copies of itself. A polymorphic virus may have no parts that remain identical between infections, making it very difficult to detect directly using signatures.

Multipart virus - Also called a multipartite virus, this has several components to it and can be distributed to different parts of the system. It infects and spreads in multiple ways, which makes it harder to eradicate when identified.

Self-garbling (metamorphic) virus - Attempts to hide from antivirus software by modifying its own code so that it does not match predefined signatures.

Meme viruses - These are not actual computer viruses, but types of e-mail messages that are continually forwarded around the Internet.

Bots - Software applications that run automated tasks over the Internet, which perform tasks that are both simple and structurally repetitive. Malicious use of bots is the coordination and operation of an automated attack by a botnet (centrally controlled collection of bots).

Worms - These are different from viruses in that they can reproduce on their own without a host application and are self-contained programs.

Logic bomb - Executes a program, or string of code, when a certain event happens or a date and time arrives.

Rootkit - Set of malicious tools that are loaded on a compromised system through stealthy techniques. The tools are used to carry out more attacks either on the infected systems or surrounding systems.

Trojan horse - A program that is disguised as another program with the goal of carrying out malicious activities in the background without the user knowing.

Remote Access Trojans (RATs) - Malicious programs that run on systems and allow intruders to access and use a system remotely.

Immunizer - Attaches code to a file or application, which would fool a virus into “thinking” it was already infected.

Behavior blocking - Allowing the suspicious code to execute within the operating system and watches its interactions with the operating system, looking for suspicious activities.

Where does Malware come from ---> EVERYWHERE !!

How is Malware distributed?

1. SEO manipulation
2. Social Engineering / Click-Jacking
3. Phishing
4. Malvertising
5. Compromising legitimate sites
6. Drive-by downloads
7. Spam

What are the basic components of Malware?

1. Crypter - protects that malware components from being scanned or found during analysis
2. Downloader - used to download additional malware
3. Dropper - used to install additional malware into the target system
4. Exploit - malicious code used to execute on a specific vulnerability
5. Injector - used to expose vulnerable processes in the target system to the exploit
6. Obfuscator - used to conceal the true purpose of the malware
7. Packer - used to bundle all of the malware files together into a single executable
8. Payload - used to take over the target machine
9. Malicious Code - used to define the abilities of the malware

What is a Trojan?

A Malicious Program that is used to mislead a user about its actual intention by hiding the malicious code inside of a "harmless" program.

Trojans are typically spread through Social Engineering.

Port Number Port Type Trojans

2 TCP Death
20 TCP Senna Spy
21 TCP Blade Runner | Doly Trojan | Fore |
Invisble FTP | WebEx | WinCrash
22 TCP Shaft
23 TCP Tiny Telnet Server
25 TCP Antigen | Email Password Sender |
Terminator | WinPC | WinSpy
31 TCP Hackers Paradise | Masters Paradise
80 TCP Executor
421 TCP TCP Wappers Trojan
456 TCP Hackers Paradise
555 TCP Ini-Killer | Phase Zero | Stealth Spy
666 TCP Satanz backdoor

1001 TCP Silencer | WebEx
1011 TCP Doly Trojan
1095-1098 TCP RAT
1170 TCP Psyber Stream Server | Voice
1234 TCP Ultors Trojan
10000 TCP Dumaru.Y
10080 TCP SubSeven 1.0-1.8 | MyDoom.B
12345 TCP VooDoo Doll | NetBus 1.x | GabanBus |
Pie Bill Gates | X-Bill
17300 TCP NetBus
27374 TCP Kuang2 | SubSeven server (default for
V2.1 Defcon)
65506 TCP SubSeven
53001 TCP Remote Windows Shutdown
65506 TCP PhatBot | Agobot | Gaobot

What are the different types of Trojans?

1. Remote Access Trojans
2. Backdoor Trojans
3. Botnet Trojans
4. Rootkit Trojans
5. E-Banking Trojans
6. Proxy Server Trojans
7. Covert Channel Trojans
8. Defacement Trojans
9. Service Protocol Trojans - VNC | HTTP/HTTPS | ICMP
10. Mobile Trojans
11. IoT Trojans
12. Security Software Disabler Trojans
13. Command Shell Trojans

What does the infection process using a Trojan look like?

It is comprised of the following steps, which are taken by an attacker to infect a target system:

1. Creation of a Trojan using Trojan Construction Kit
2. Create a Dropper
3. Create a Wrapper
4. Propagate the Trojan
5. Execute the Dropper

What are common Trojan countermeasures?

1. Avoid clicking on unusual or suspect e-mail attachments
2. Block unused ports
3. Monitor network traffic
4. Avoid downloading from untrusted sources
5. Install & update Anti-virus software
6. Scan removable media before use
7. Validate file integrity of all externally sourced software
8. Enable Auditing
9. Configure Host-Based Firewalls
10. Use Intrusion Detection Software

What is a Virus?

A virus is a self-replicating program.

The major characteristics of viruses are:

1. Infecting other files
2. Alteration of data
3. Transforms itself
4. Corruption of files and data
5. Encrypts itself
6. Self-Replication

What are the stages of the Virus Lifecycle?

1. Design
2. Replication
3. Launch
4. Detection
5. Incorporation - A.V. figures out the virus pattern & builds signatures to identify and eliminate the virus
6. Execution of the damage routine - A.V. to the rescue

How does a Virus actually Work?

1. Infection Phase - a virus is planted on a target system and replicates itself and attaches to one or more executable files.
2. Attack Phase - the infected file is executed accidentally by the user, or in some way is deployed and activated.

What about malware analysis?

A Sheep-Dip Computer is a dedicated computer which is used to test files on removable media for viruses before they are allowed to be used with other computers.

Malware analysis is the process of reverse engineering malware to understand how it operates.

Malware analysis starts with the preparation of a testbed. A security professional will deploy a virtual machine where dynamic malware analysis will be performed by executing the malware. The virtual machine is isolated from all production networks, to allow for the observation of the behavior of any malware, without the risk of infecting additional machines.

What are the goals of Malware Analysis?

1. Understand/identify the severity of the attack
2. Identify the type of Malware used in the attack
3. Understand/identify the scope of the attack
4. Build defenses to secure the organization's infrastructure
5. Finding a root cause
6. Build incident response capabilities specific to the threat
7. Develop Anti-malware capabilities to eliminate the threat

What are the types of Malware Analysis?

1. Static (Code Analysis) - performed by fragmenting the binary file into individual elements that can be analyzed without executing them. Techniques include:

   a. File fingerprinting
   b. Local & on-line scanning of elements to see if they match known malware profiles
   c. String searching

d. Identifying Packers/Obfuscators used
e. Identifying the Portable Executable (PE) information
f. Identifying the dependencies
g. Malware Disassembly

2. Dynamic (Behavioral Analysis) - performed by executing the malware to see what effect it has on the system.

Two stages:

```
A. System Baselining

B. Host Integrity Monitoring
```

What are methods that I can use to detect a Virus?

1. Scanning
2. Integrity Checking
3. Interception
4. Code Emulation
5. Heuristic Analysis