Malware

Virus

A computer virus is simply made up of malicious code that's run on a machine without the user's knowledge. And this code allows it to infect the computer whenever it's being run.

Viruses require **user action** in order to reproduce and spread.

Win10 prog to create virus: JPS Virus maker 3.0

Security+ exam is going to separate viruses into 10 different types:

1. boot sector
2. macro
3. program
4. multipartite
5. encrypted
6. polymorphic
7. metamorphic
8. stealth
9. armor
10. hoax

Boot Sector

A boot sector virus is one that's stored in the first sector of a hard drive and is loaded into memory whenever the computer boots up. These are actually very difficult to detect because they're installed before the operating system boots up.

Macro

Macros are a form of code that allows a virus to be embedded inside another document. And when that document is opened by the user, that virus then is executed. The most common examples of macros are ones that are found inside

Word documents or Excel spreadsheets, or PowerPoint presentations. By default, macros aren't malicious.

Program

Program viruses seek out executables or application files to infect. For example, if you went and loaded a virus and was able to install itself into your Microsoft Word program, every time you opened up Word you'd be loading that virus again and again. And that's why a program virus targets programs.

Multipartite

A multipartite virus is a combination of a boot sector type virus and a program virus. By using this combination, the virus is able to place itself in the boot sector and be loaded every time the computer boots. And by doing so, it can then install itself in a program where it can be run each and every time the computer starts up. This allows it to have a persistence and be able to be there over and over again.

Encrypted

This virus is going to use a cipher to encrypt the contents of itself to avoid detection by any antivirus software. Because our antivirus providers are getting better and better all the time at understanding viruses and how they work and how to stop them, encrypted viruses are making it harder for virus makers to find these types of viruses.

Polymorphic

A polymorphic virus is an advanced version of an encrypted virus. But instead of just encrypting the contents, it's actually going to change its code each time it's executed by altering the decryption module in order for it to evade detection. Now, I know this sounds really complicated, but what it's doing is it's trying to morph the way its code looks so that a signature-based antivirus can't detect it anymore.

Metamorphic

Metamorphic viruses are able to rewrite themselves entirely before it attempts to infect a file. And essentially, this is an advanced version of a polymorphic virus. And so we went from encrypted to polymorphic to now metamorphic.

Stealth

And these aren't necessarily a specific type of virus as much as a category of a virus protecting itself. When we talked about encrypted and polymorphic and metamorphic viruses, these are all examples of stealth viruses. They're viruses that are using various different techniques to avoid detection by antivirus software.

Armor

And armored viruses have a layer of protection to confuse a program or a person who's trying to analyze it. Again, this is another way that the virus is trying to protect itself and increase its odds of being able to spread to other users without being detected.

Hoax

Now, a hoax is actually not a virus in the traditional sense. Instead, when we get a virus hoax, we're trying to trick a user into infecting their own machine. This might come in the form of a message or a website that pops up. It may be that we call them on the phone and pretend that we're from Microsoft tech support and tell them that their machine has been infected.

Worms

Well, a worm is a piece of malicious software, much like a virus. But it has a key difference. A worm can **replicate itself** without any user interaction. If you remember when I talked about viruses, I said that a user has to install a program, or open a file, for that virus to be able to take its action. But with worms, that's simply not the case. Worms are able to **self-replicate** and spread throughout your network, **without a user's consent, or their action**.

Trojans

Trojan horses are a piece of malicious software that's disguised as a piece of harmless or desirable software. Basically, a Trojan says, I'm going to perform this function for you. And it will perform that desired function, but it will also perform a malicious one, too.

Remote Access Trojan - RAT

A RAT is a type of Trojan that is in use today, and it's widespread. It provides the attacker with remote control of a victim machine.

Win10 RAT creator: ProRat V1.9

Ransomware

Ransomware is a type of malware that restricts access to a victim's computer or their files until a ransom is received. That's right, someone is going to go break into your computer, encrypt your files or change your password or do something else to hold your system until you pay up. Ransomware is going through and using some vulnerability in a piece of software to gain access to your machine and then encrypting your files and once they do that, you have no way to decrypt them unless you pay the ransom or you restore from a known good back-up.

Spyware

Well, spyware is a type of malicious software that's installed on your system and gathers information about you without your consent. Normally, this will be installed from a website or some third-party software that you've installed on your system.

Adware

Adware is a specific type of spyware where it's going to display advertisements to you, based on what it saw when it spied on you.

Grayware

Grayware isn't really good and it isn't really bad, it's kind of in the middle. Grayware is some kind of software that's usually used to make something behave improperly without any serious consequences. For example, there's one called Crazy Mouse, that if you start this program on your friend's computer, the mouse will start jumping over the screen.

Rootkit

A rootkit is a specific type of software that's designed to gain administrative level control over a given computer system without being detected. Now, this is really important, because when we talk about root or administrative level permissions, this is the highest level permissions that someone can have on a given computer system. If you're using a Windows machine, for example, this is called the Administrator account.

DLL Injection

With a DLL injection, what ends up happening is malicious code is inserted into a running process on a Windows machine by taking advantage of the DLLs, or Dynamic Link Libraries, that are loaded at runtime. This means that the Windows system doesn't even understand the fact that it has a rootkit installed.

Driver Manipulation

This also can occur by doing driver manipulation. This also can occur by doing driver manipulation. This is an attack that relies on compromising the kernel-mode device drivers that operate at a privileged or system level.

Shim

Both DLL injection and driver manipulation occur by the use of a shim. A shim is simply a piece of software code that is placed between two components, and that intercepts the calls and redirects them. So, the rootkit will allow an interception to happen between the Windows operating system and the Dynamic Link Library, and then redirect that call with the malicious code embedded into it.

Summary

Viruses are code that infect a computer when a file is opened or executed. When you think about a virus, remember, if it requires user action to be able to be opened, installed, or spread, it's likely a virus.

Worm.
A worm acts a lot like a virus but instead, it's able to do self-replication. It doesn't need any user action to be able to spread itself.

A Trojan.
A Trojan is a program that appears to do one desirable function but instead it does the desired function and malicious functions as well. Remember, the most common type nowadays is what's known as a RAT, a Remote Access Trojan.

Ransomware.
Ransomware is going to take control of your computer or your data unless you pay them some money. Again, they're holding it for ransom. They usually do this by encrypting your files.

Spyware.
Spyware is a software that collects your information without your consent. They're spying on you and then they're advertising to you or doing other things of that nature.

A rootkit.
A rootkit is going to gain administrative level control over your system by targeting the boot loader or the kernel of the operating system.

And finally, spam.
Spam is the abuse of electronic messaging systems, whether chat, email, or instant message. The most common of these though, is definitely email.

Malware Infections

Threat Vector

A threat vector is the method used by an attacker to access a victim's machine.

Attack Vector

An attack vector is the means by which the attacker is going to gain access to that computer in order to affect you with malware.

Watering Hole

Malware is placed on a website that you know your potential victims will access.

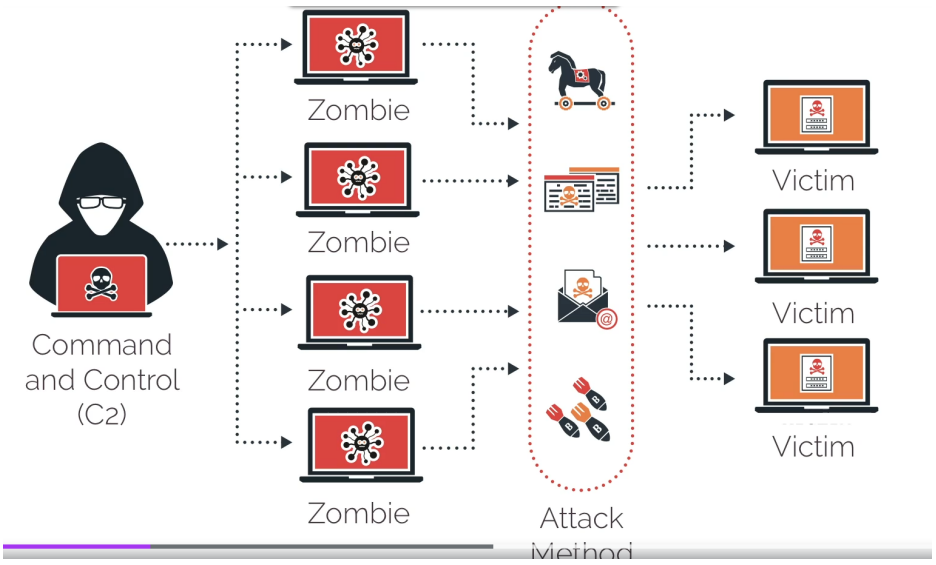
Phishing

Phish Insight - Trend Micro provides phishing testing

Botnet/Zombies

A botnet is simply a collection of compromised computers under the control of a master node.

That's right, a zombie becomes part of the botnet and a botnet is simply a collection of compromised computers under the control of a master node.



Most common attack type of Botnet and Zombies is DDOS attack

Active Interception/Privilege Escalation

Active interception occurs when a computer is placed between your sending computer and your receiving computer.

Now privilege escalation occurs when you're able to exploit a design flaw or a bug in a system to gain access to resources that a normal user isn't able to access.

To Scan network with GUI(uses nmap): ZENMAP

Backdoor/Login Bombs

A backdoor was originally placed in computer programs to bypass the normal security and authentication functions.

But, there is something that acts just like a backdoor. What do you think that might be?Well, it's a remote access trojan.

Logic bombs are a descendant of those earlier Easter Eggs. But logic bombs were designed with malicious intent in mind. Logic bombs are malicious code that's inserted into a program, and it will execute only when certain conditions have been met.

Now, logic bombs and Easter Eggs and backdoors are all things that should not be found inside our code.

Symptoms of Infection

If your computer is acting funny or strange, you may be infected with malware and so it's best to boot up into safe mode or boot from an external drive and then scan your computer with a good antivirus software.

Removing Malware

1. Identify the symptoms of the malware infection
2. Quarantine the infected systems
3. Disable your system restore if you're using a Windows machine
4. Remediate the infected machine
5. Schedule automatic updates and scans
6. Re-enable our system restore and we want to create a new restore point
7. Provide end-user security awareness training

Malware Exploitation

Now, a **dropper** is a specialized type of malware that's designed to install or run other types of malware embedded in a payload on an infected host. Usually, this will be a stage one dropper, it's that code you first got. And once you get that code and run it, it's then going to go out and get some other code, and it uses a downloader to do that

Now, a **downloader** is a piece of code that connects to the Internet to retrieve additional tools after the initial infection happens by a dropper.

Now, **shellcode** is any lightweight code that's designed to run an exploit on a target. This can include any type of code format, it can be scripting languages, all the way down to a compiled binary.

Shellcode originally referred to malware code that would give the attacker a shell or a command prompt on the target system.
If you take the PenTest+ exam, that's how they're going to use that term.

For this exam, they want you to use the definition of the more generic shellcode that I just provided, which is any lightweight code designed to run an exploit on a target.

Code injection is an exploit technique that runs malicious code with the identification number of a legit process.

Living off the land, this is an exploit technique that uses standard system tools and packages to perform their intrusions.