MALWARE

Virus

You go to your client's email and open it. You may tell right away that your client has opened certain emails coming from strange email addresses. When you open the emails, you can see that the client probably downloaded files and clicked on links in the dubious emails. Uh oh. Has your client downloaded any malware?

A harmful self-replacing program that affixes itself to other programs and executables without the user's consent is known as a virus. Data on the computer might be altered or deleted by a downloaded virus.

If the virus was able to access or alter data, the confidentiality and integrity of that data is now in question.

- Just like with adware, avoid suspicious links and install trustworthy antivirus software.
- Immediately report suspicious emails to your IT department and never open them.

Trojan Horses

There is another kind of infection that is not spyware, even if the existence of spyware makes it clear something malicious was placed on the computer. it's a Trojan Horse.

While the Trojan Horse, commonly just referred to as a "Trojan," is like Spyware in that it monitors activity on a system, it also performs other functions. Trojans are a sort of contained, non-replicating malware that impersonates trustworthy programs to gain access to a user's system and commit fraud. This malware infiltrated your client's PC by posing as a trustworthy antivirus program, just like the Greeks did when they crept into the city of Troy inside a huge wooden horse! Just like the Greeks did when they snuck into the city of Troy inside a massive wooden horse, this spyware entered your client's PC by pretending to be a reliable antivirus tool!

Spyware

Spyware is malicious software that users unknowingly download and use to steal personal data and transmit it to other parties in ways that are harmful to the original user. A threat actor might be able to obtain private data if the spyware included a keylogger, a tool that can record what a victim writes onto their computer.

This implies that any private information, including passwords, will soon be in the hands of an evil third party. Although spyware is typically not used to alter data, it nonetheless violates the confidentiality principle. It's possible that a hostile actor watched your customer type confidential information.

- Be careful what you click on and install that trustworthy antivirus already!

Worms

This virus is what kind? When you look through your client's "Sent Emails" folder, you discover that they recently sent the same email to all of their contacts. The emails are malicious, and the subject lines are identical. The email nearly looks to have copied itself...

You might have discovered a worm as opposed to a virus, which needs a file or application to spread.

Self-replicating software, or a worm, copies itself automatically from computer to computer. This worm might be as harmful as a virus.

The worm might also reproduce innumerably to the point where it overwhelms your client's system. The worm may disrupt the system and breach availability if it did this.

- Follow the previous suggestions for adware and viruses.
- Monitor the computer for any unexpected changes! Is it slower than usual? Is there less hard drive space than expected? Have files mysteriously appeared or disappeared? These could all be signs of worms.

Adware

You start by launching the web browser. It opens to an odd page promoting a computer cleaner that is "guaranteed to make your machine perform 10X quicker!!" on the first visit. What a strange selection for a homepage.

You observe several advertisements appearing everywhere as you browse the internet. Your screen is being overrun with them to the point where the website is actually loading more slowly.

This machine obviously has adware. Adware is unwanted software that is made to bombard your screen with advertising. Although not particularly nasty at first glance, adware occasionally is attached to other, more dangerous software.

This can actually affect performance if there is enough adware on your computer.

- Make sure to not click on any strange links or download any untrustworthy files.
- A trustworthy antivirus software could also help with this issue.

Fileless Malware

Fileless malware is a sort of malware that "lives off the land" and employs reputable programs and the operating system of the user to carry out harmful operations like privilege escalation, information gathering, and other things. Antivirus software nearly never picks it up since it is so difficult to detect.

In contrast to a Trojan Horse, fileless malware is a component of legitimate software rather than acting as if it were separate from it. Fileless malware blends in with normal software's code, frequently changing the existing code to make it dangerous.

These assaults are particularly susceptible to certain software, such as Microsoft PowerShell. This attack vector could be used by someone to obtain information, install malware, or mine bitcoin using the resources of your device.

- Did you download that antivirus yet? Still, avoiding those suspicious links?
- Disable command-line applications and macros, not in use on the device.
- Keep your applications and system up to date for the latest security updates.
- Reboot the computer.

Rootkits

What is the Trojan Horse doing exactly? What did it strive to accomplish? You must ascertain the solution.

When you scan the device, you discover that it is an awful device that keeps becoming worse since a rootkit was installed on the system via a Trojan horse.

A group of harmful applications known as rootkits allow unauthorized users to silently maintain privileged access to a system. Using a rootkit, a hacker can gain access to a computer by opening a backdoor. This rootkit managed to get administrative access to the machine, and it would be quite challenging to get rid of.

In this instance, the Trojan Horse impersonated a reliable antivirus program in order to set up a rootkit. This indicates that this computer's files are accessible by an evil third party who is located someplace. The confidentiality and integrity of your client's system are in grave danger in this circumstance. A rootkit can be removed with some specialist tools, but it is difficult.

- Back up any important data on this system and reimage it.

Ransomware

Someone had access to this machine thanks to the rootkit. With such access, what did they do? You notice that the rootkit was utilized to prevent the user from accessing system files that house a significant amount of crucial firm info.

Ransomware may be present if the bad actors restrict access to data or make threats to make the private information public unless the client pays them money. As threat actors have recognized it's safer and simpler to rob a virtual place rather than a physical one, the use of ransomware has been soaring! One of the biggest cybersecurity dangers now facing businesses is ransomware.

Data availability is seriously threatened by denying a user access. Even though availability might not seem crucial, for some firms, it can be disastrous. Imagine losing access to a hospital's system or a flying system's data!

- Regularly back up important files.
- Have a procedure in place for ransom requests. They should include a step in which the authorities are alerted.

TERMS

- **Malware:** Malicious code inserted into a system to cause damage or gain unauthorized access to a network
- **Adware:** Unwanted software designed to throw advertisements on your screen
- **Virus:** A malicious self-replacing application that attaches itself to other programs and executables without the permission of the user
- **Worm:** Self-replicating code that copies itself from computer to computer without user intervention
- **Spyware:** Malicious code downloaded without a user's authorization which is then used to steal sensitive information and relay it to an outside party in a way that harms the original user
- **Trojan Horse:** A type of contained, non-replicating malware that disguises itself as legitimate software to allow scammers and hackers access to a user's system
- **Rootkit:** A collection of malicious programs that secretly provide continued, privileged access to a system for an unauthorized user
- **Ransomware:** Malicious code that will block a user's access to data or threaten to publish sensitive data until they pay money to the malicious actor
- **Fileless Malware:** A type of malware that 'lives off the land' and uses legitimate tools and the user's operating system to perform malicious activities like privilege escalation, data collection, and more. It's incredibly hard to detect and almost always missed by antivirus software