Run/ Playbook Part 1: Malware

[Arash Golshan]

[CYB/110]

Run/ Playbook Part 1: Malware

**Scenario**

With the increase in technology, Malware attacks are becoming very popular. The most common type of Malware attack these days is Trojan horse. A Trojan horse is a type of malware which misleads the users by bluffing them. It is a malicious program which contains the virus that hackers used to get access to the systems. A recent malware attack occurred to me in which hackers tried to access the sensitive data of the company. The malware attack which they used to attack my system was Trojan horse (Chunming, 2003). I recently installed software which I found useful, but it was designed to access the sensitive data from my system. The system started to crash and freezes repeatedly. There was a weird increase in the usage of internet on the system. Antivirus stopped working and applications opened up unexpectedly. It’s challenging to find Trojan virus because usually people consider every software useful and they don't know what is happening at the backend.

The trojan can be of different types. When they are activated on the system, they may annoy user by deleting their files and destroying their information from their system. Some Trojans are even dangerous then malicious software’s because they are designed to be more annoying. The most important thing to rescue yourself from these viruses is to download software’s which are from verified sources. Don't download or install software's which are not from a verified source because you don't know whether it is a software or Trojan attack if anyone suffers from a Trojan attack that individual should suddenly turn of the internet to avoid severe damage (White et al., 2017). Trojans also provide access at the backend to the hackers so that they can access your personal information. They cannot harm users unless users run them on their systems.

The strategy of cybersecurity is very crucial regarding data protection of the owner's business, confidentiality of their customers and malware attacks in all online businesses (Zhang, 2018). What's more, with information fissures such as Trojan’s virus on the ascent, organization’s security, client, and worker data turned into significantly vital factors for every business in the market.

**List of information and data employees are not to place online**

The company should not place the personal information of the employees online anywhere on the internet. The internet connection (Wi-Fi) should not be open and low secure. Beware of the virus contained files and data before downloading. The employee’s accounts should not contain weak passwords. The employees should not be unaware of the security breaches. They must be trained to maintain and secure their data. Following are some credentials which should not be uploaded online:

1. Client data
2. Administrative communications
3. Intellectual property
4. Worker records

**Guidelines for interacting online**

The online interaction has become so problematical nowadays due to the negative interactions with people. Following are some guidelines to ensure safe and secure online interactions. Always keep the personal information limited and proficient. The privacy settings must be on and always go for safe internet surfing. Always choose strong passwords and secure internet connection. Be aware of the people you meet online and what you post. The antivirus must be updated regularly.

**Guidelines for secure use of email**

There is great danger in using emails when such viruses are on the rising. There are some ways for secure use of email. The first and most important step in data privacy is using strong passwords for your email accounts. For the business companies, the employees should not be able to use email addresses of the company for their messages. Beware of the phishing emails from unknown people and try not to open the emails in your junk folder because most of them contain viruses. These emails must be scanned for malware and spam (Weinstein, 2003) before opening. Try not to check emails when using a public hotspot.

**List of items staff at your company should not place on social media**

We should always know what to post online or on social media, especially as a company's employee. Try not to post or generally reveal secret organization data electronically. The negative audits or remarks of the opponent or another individual posting about the organization should be handled carefully and do not react on them. For employees, they should not give negative remarks about the company's manager, CEO or any other colleague. Try to avoid posting photos or recordings on the social media that could harm the reputation of the company. Do not post any confidential information or anything illegal.

**References**

Chunming, Z. M. X. Q. L. (2003). Analysis of Trojan horse and Its Detection [J]. *Computer Engineering and Applications*, *28*, 053.

White, G. B., Fisch, E. A., & Pooch, U. W. (2017). *Computer system and network security*. CRC press.

Weinstein, L. (2003). Spam wars. *Communications of the ACM*, *46*(8), 136.

Zhang, D. (2018). Big data security and privacy protection. In *8th International Conference on Management and Computer Science (ICMCS 2018)*. Atlantis Press.