Vedh Reddy, Heding Liu

4.2.1 Activity: Technology-Based Attacks

Goal: As a group, research a specific type of technology-based attack and one real-world example of the attack occurring. Share your findings with the class.

Attack Type: Trojan Horse

Instructions: Answer the questions listed below based on your given technology-based attack type. Create an informative product that you can present to the class to discuss your specific type of attack in detail.

1. How is your attack carried out on the victim's device(s)?

Trojans are usually spread because of social engineering. This is because they disguise themselves as a "good" program, and if society is beginning to accept the program, then it becomes seen as "safe". Society or cyber-criminals can coerce others into downloading Trojan horses. Once the program is seen as safe, the Trojan will be downloaded onto the device. These programs can range from email attachments or free-download files and applications.

2. What information or data is compromised during this type of attack?

Any data can be compromised due to the malware's ability to appear like legitimate software. Data often stolen by this malware include login credentials, financial records, personal files, and system configurations

3. What is a historical example of your attack type?

A historical example of the Trojan attack can be seen in the Trojan named SpyEye. This trojan would take control of people's and use keystroke logging and form grabbing in order to steal information.

4. Who carried out this attack?

The authors of SpyEye were Alexander Andreevich Panin and Hamza Bendelladj. The malware first spread in Russia in 2009 and was sold on underground forums.

5. Who was the victim and what data was targeted during the attack?

The victims of this attack were widespread. Many people would download this trojan through email, fake security alerts, as well as downloadable software that included the Trojan. The data primarily targeted was sensitive data such as card information. Because the Trojan could manipulate the html form fields on the websites that people would access, whenever they entered any sensitive information like card numbers and CVC's, it would be picked up by the keylogger part of the malware.

6. Was the attack successful and why/ why not?

The attack was successful because the malware was used to infect more than 50 million computers and caused nearly $1 billion in damage. It was able to go unnoticed for long periods of time because it wasn't evident that the form data was being stolen. In addition, the ability to modify websites also gave them the ability to create fraudulent transactions and then modify the UI to not show the fraudulent transactions, meaning money was being drained out of people's accounts without them knowing. The multifaceted way in which this Trojan was able to target people was the reason it was so powerful.

7. What was done, if anything, to prevent further attacks such as this?

The authors Panin and Bendelladj were arrested and imprisoned. In addition, anti malware software was designed around these Trojans that lived in the browser. This was a well designed Trojan so a full standard solution has yet to come, and SpyEye can only be fought with modern anti-malware installation as well as advanced EDR (Endpoint Detection and Response) solutions.

Attack Type: Trojan

1. Trojans are usually spread because of social engineering. This is because they disguise themselves as a “good” program, and if society is beginning to accept the program, then it becomes seen as “safe”. Society or cyber-criminals can coerce others into downloading Trojan horses. Once the program is seen as safe, the Trojan will be downloaded onto the device. These programs can range from email attachments or free-download files and applications.
2. Any data can be compromised due to the malware’s ability to appear like legitimate software. Data often stolen by this malware include login credentials, financial records, personal files, and system configurations
3. A historical example of the Trojan attack can be seen in the Trojan named SpyEye. This trojan would take control of people’s and use keystroke logging and form grabbing in order to steal information.
4. The authors of SpyEye were Alexander Andreevich Panin and Hamza Bendelladj. The malware first spread in Russia in 2009 and was sold on underground forums.
5. The victims of this attack were widespread. Many people would download this trojan through email, fake security alerts, as well as downloadable software that included the Trojan. The data primarily targeted was sensitive data such as card information. Because the Trojan could manipulate the html form fields on the websites that people would access, whenever they entered any sensitive information like card numbers and CVC’s, it would be picked up by the keylogger part of the malware.
6. The attack was successful because the malware was used to infect more than 50 million computers and caused nearly $1 billion in damage. It was able to go unnoticed for long periods of time because it wasn’t evident that the form data was being stolen. In addition, the ability to modify websites also gave them the ability to create fraudulent transactions and then modify the UI to not show the fraudulent transactions, meaning money was being drained out of people’s accounts without them knowing. The multifaceted way in which this Trojan was able to target people was the reason it was so powerful.
7. The authors Panin and Bendelladj were arrested and imprisoned. In addition, anti malware software was designed around these Trojans that lived in the browser. This was a well designed Trojan so a full standard solution has yet to come, and SpyEye can only be fought with modern anti-malware installation as well as advanced EDR (Endpoint Detection and Response) solutions.