CS381 Exercise 17

Name: Zhang Yupeng

Student ID: 5130309468

1. Describe the similarities and differences of Virus, Macro virus and Worms?

Solution:

Virus is a piece of self-replicating code attached to some other code as code to perform some covert task.

Macro virus is macro code attached to some datafile, it blur distinction between data and program files that replicating but not infecting program.

While virus attach themselves to other programs. Worms, in contrast, are stand-alone programs that do not need to attach to other programs, it can propagate like viruses through e-mail, and so on.

2. List the good rules to avoid malware infection.

Solution:

From a website: If you are unsure, leave the site and research the software you are being asked to install. If it is OK, you can always come back to site and install it. If it is not OK, you will avoid a malware headache.

From e-mail: Do not trust anything associated with a spam e-mail. Approach e-mail from people you know with caution when the message contains links or attachments. If you are suspicious of what you are being asked to view or install, don't do it.

From physical media: Your friends, family, and associates may unknowingly give you a disc or flash drive with an infected file on it. Don't blindly accept these files; scan them with security software. If you are still unsure, do not accept the files.

From a pop-up window: Some pop-up windows or boxes will attempt to corner you into downloading software or accepting a free "system scan" of some type. Often these pop-ups will employ scare tactics to make you believe you need what they are offering in order to be safe. Close the pop-up without clicking anything inside it (including the X in the corner). Close the window via Windows Task Manager (press Ctrl-Alt-Delete).

From another piece of software: Some programs attempt to install malware as a part of their own installation process. When installing software, pay close attention to the message boxes before clicking Next, OK, or I Agree. Scan the user agreement for anything that suggests malware may be a part of the

installation. If you are unsure, cancel the installation, check up on the program, and run the installation again if you determine it is safe.

3. How is the hash collision attack used in the Flame malware?

Solution:

The hash collision attack can be used to make rogue certificates. And the rogue certificates can be used to make fake digital signature that cannot be detected by the browser. The usual attack scenario goes like this:

1. Mallory creates two different documents A and B that have an identical hash value, i.e., a collision.
2. Mallory seeks to deceive Bob into accepting document B, ostensibly from Alice.
3. Mallory sends document A to Alice, who agrees to what the document says, signs its hash, and sends the signature to Mallory.
4. Mallory attaches the signature from document A to document B.
5. Mallory then sends the signature and document B to Bob, claiming that Alice signed B. Because the digital signature matches document B's hash, Bob's software is unable to detect the substitution.

This meant that an attacker could impersonate any SSL-secured website as a man-in-the-middle, thereby subverting the certificate validation built in every web browser to protect electronic commerce.

The rogue certificate may not be revokable by real authorities, and could also have an arbitrary forged expiry time.