Alexander Cannell

Professor Robertson

CSIS 3650

Activity 1 Chapter 3

**What OS’s are affected by this worm?**

In an Apple release of Quick Time 7.6, Apple addressed multiple vulnerabilities for both Windows and Mac systems that may allow a remote attacker to execute a arbitrary code (a command of the attacker which choice on a target machine or process) or cause a DOS attack.

A Conficker Worm is a computer worm that targets the Windows OS and uses defects in the Windows software to perform “dictionary attacks” (a technique in defeating an authentication mechanism by determining the decryption key by trying likely possibilities) on an admin password to eventually form a botnet.

The way to get rid or prevent a Conficker Worm is to disable AutoRun on your Windows OS which can prevent the spread of the virus, but this isn’t a fully effective way to prevent the virus and your system is still considered compromised. To effectively do so copy the code below and save as autorun.reg, and save in registry.

“

REGEDIT4  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping\Autorun.inf]  
@="@SYS:DoesNotExist"

“

**Lists of threats**

W32.Disttrack!gen4 – worm

W32.Disttrack!gen6 – worm

Trojan.Zeroaccess!inf9 – Trojan

W32.Fixflo – Virus

Backdoor.Joggver – Trojan

**Backdoor.Joggver**

Is a Trojan horse thsat opens a back door on the compromised computer. Effecting Windows OS’s, and was discovered August 31 2012. To get rid and reduce the threat of an attack run Symantec Power Eraser, and to prevent Disable Autorun, File Sharing Protection, and OS vulnerabilities updates.

Activity 2 Chapter 3

Wikipedia

Boston College Information Technology Service

PC Tool's

http://www.bc.edu/content/bc/offices/help/security/virus/macrovirus.html

A Macro Virus is a series of program commands or instructions designed to simplify repetitive tasks within a program in the Mircosoft Office. your computer can get a macro virus when you open any document that has a macro virus attached to it. as soon as the virus opens the virus spreads corrupt files, and copies itself. you also have a chance to get a virus if you open an attachment in an email.

**To preventing macro virus**

1. Enable macro virus protection in Microsoft Word

2. Find and remove infected Microsoft Word files

3. If you have anti-virus installed run it

**To remove macro virus**

1. Making a copy of the infected Microsoft Word document, locate the file named Normal.dot and rename the file to Normal.old

2.Deleting the macros from the document

3. Recovering your infected document, save your recovered document

Creating a macro virus seems pretty easy to do.

Activity 3 Chapter 3:

Code Red was a computer worm, that attacked computers with Microsoft IIS Web Server. Code red first attempted to connect to tcp port 80 on the web server, attacking host sends a HTTP request to the target pc attempting to overflow the buffer. next it packet floods DOS attack is launched against IP addresses. next the worm hibernates.

port 80 is where code red starts it's attack.

code red defaces by posting HELLO! Welcome to HTTP://WWW.WORM.COM!HACKED BY CHINESE!

To get rid of the code Red because the worm resides in the memory a complete reboot will do the trick, but patching can cause some vulnerabilities.

Activity 4 Chapter 3

Microsoft security

Wikipedia

PC Tools

LavaSoft

Norton

Microsoft Security-

Spyware is often associated with software that display advertisement, or software that tracks personal information.

180 Search Assistant - adware

Program that delivers advertisement on your PC. adware is any software application in which advertising is displayed while the program is running. to remove require an internet connection to uninstall, and can be removed with add/remove programs make sure you remove the host application first.

Activity 5 Chapter 3

http://www.us-cert.gov/cas/techalerts/TA12-240A.html

Oracle Java 7 security manager bypass vulnerability. When updating java 7 a vulnerability in java 7 that restricts the permissions of java applets could allow an attack to be executed arbitrary commands on vulnerable systems. to get rid or prevent disable java plug in, java deployment toolkit, and java web start functionality. Also try uninstalling java 7 and downgrading to java 6. Another prevention is to use No Script which is an extension for firefox that provides the option to block java applets.