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.