**911 Worm**

Antoinette Binning

It was about 5:00 p.m. on Saturday April 1, 2000, I'm reading my email. I got a message from SANS Institute warning me of a computer virus. If this message was from a friend or family member, I would have thought it to be yet another hoax. (How many times did you get an email warning you of the virus in the Budweiser frogs screensaver?) This warning turned out to be legit. I went to http://www.sans.org/newlook/alerts/911worm.htm. Sure enough, the FBI had posted in all capital letters an advisory that morning, www.nipc.gov/nipc/advis00-038.htm.

Malicious code strikes again, only it is not a virus this time, worse, it is a worm.

A worm doesn't need the help of person to propagate. You need not have doubled clicked on an email attachment to become infected. According to the FBI advisory, this worm spreads by searching computers attached to the internet with file and print sharing set up. It then copies itself to these machines. Next it overwrites the hard drive and dials 911 emergency services. The worm has several versions and is known by many names: firkin.worm, 911 share virus, bat/911, bat/chode.worm and foreskin.

Here is what happens in the bat/chode version of the worm according to Symantec's web site, www.symantec.com/avcenter/venc/data/bat.chode.worm.html. Once the worm locates a computer with a shared drive that doesn't require a password, "it will check for the presence of the file c:\windows\win.com. If such a file [exists], it assumes the shared drive is the c:\ drive of the other computer." Next the worm will map a drive to that machine. It will search and remove vbs.network along with verifying that it can write to the drive. It then proceeds to copy its files to the newly created c:\progra~1\chode directory. This directory is where the main batch file assumes it is running from. Here's what else the worm will do. It will make a "call to a batch file" placed in the c:\autoexec.bat to dial 911 using the infected computer's modem. This modification appears to happen only in "one out of five times". Next the following files are all added to the program-startup menu: ashield.pif, netstat.pif and winsock.vbs. The first file, ashield, "hides the worm when it is launched". Netstat.pif "hides the netstat utility" that the worm uses and winsock.vbs "carries its payload". This infection will be logged in a file on the source computer.

Now on the 19th of the month winsock.vbs will be launched when "windows starts on [the] infected computer". The "vbs script [will] delete files in the following directories: c:\windows, c:\windows\system c:\windows\command and c:\". Once the files have been delete two message boxes appear: "`You Have Been Infected By Chode` and "`You may now turn this piece of sh*t off`!"

To protect your machine from this new worm, Symantec advises deleting the following: c:\program files\chode directory, c:\windows\startup ashield.pif, c:\windows\startup netstart.pif, and c:\windows\startup winsock.vbs from your hard drive.

The creator of this worm has yet to be found. ABC news reports http://abcnews.go.com/sections/tech/dailynews/virus000404.html "a computer has been seized, but so far no arrests have been made." The 911 worm was first detected in the Houston area. "Officials at 911 centers in Texas are reviewing their calls to see if a computer [has] been calling up a voice line. Sonya Lopez, spokeswoman for the Greater Harris County 911 Network, said that all 40 of the Texas 911 centers were warned of the virus Monday morning and told that "they may be receiving calls from a modem [and] if they do, can they print out a screen capture" of the call. So far, two, possibly three, bogus calls have been detected." The FBI believes this virus/worm is not widespread. Vesselin Bontchev, of FRISK software, agrees with the FBI and his comments can be found at http://archives.neohapsis.com/archives/ntbugtraq/current/0020.html Vesselin thinks this worm "is rather stupid, very limited, and doesn't spread well." He also believes "it is extremely unlikely that you're infected with it or that you will be in the future".

You decide. In the mean time, I am relieved it is not another hoax taking up space in my email inbox.