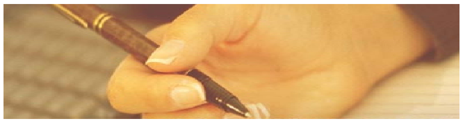
Canaudit Perspective

October 2003
Volume 4, Issue 10

Topics of Interest:

- Computer viruses – Similar in nature as organic viruses
- Blaster or Lovsan Worm
- Sobig.F worm
- Protecting systems from viruses and worms



Viruses and Worms: The Best Defense is Awareness

Written by: Chad Parks
Manager, Technical Audits & Security Services
Canaudit, Inc.

Computer viruses and worms have wreaked havoc on the computer industry for years, costing billions of dollars in lost data, time, and system use. The threat posed by computer viruses and worms is more than just a period aggravation of not being able to access the Internet and is beyond the hype used by antivirus software firms to increase sales. The threat of worms and viruses is real and can affect you in your pocket book, at home, and at work. There are no international borders that will stop the threat of viruses and worms, and there are no limits to the damage and chaos they can offer – from system resource consumption and system reboots to damaged hardware and unrecoverable data loss. It is for this reason that it is the responsibility of every computer user to understand the fundamental nature of computer viruses and worms, the damage that they can do, and the measures that can be taken to reduce exposure.

This article discusses, from a birds eye point of view, several of the most recent viruses and worms to bombard our information systems. It also addresses the nature of viruses and worms and simple controls that can be used to mitigate the risk. The purpose of this article is to refresh what many of you already know, and to try to get those who haven't taken the required steps to protect their systems to do so. Rest assured, by the time you have read this there are new worms and viruses knocking on your front door. The viruses and worms discussed in this paper have already had signatures developed by many of the most popular antivirus software suites. Once a virus is detected, the antivirus software firms create a signature so that the virus can quickly be isolated, usually within hours. This demonstrates the lightning like speed of one facet of information warfare. When dealing with computer viruses and worms we are discussing them relative to hours and minutes not days and weeks.

Computer viruses are similar in nature as organic viruses. They infect a host and use the host's resources to replicate themselves and to infect other hosts. Viruses usually latch onto vulnerable programs, take control of the target program, and use the program's access to the operating system to delete arbitrary or system critical files and/or to spread to other hosts. Computer viruses attempt to propagate to other hosts, often through email attachments by taking control of the hosts email software. Using this technique the virus software will tend to send a copy of itself to all the email addresses it can find after scanning the infected computer for email addresses.

Computer worms are analogous to computer viruses and are often used as a transport medium for viruses. The primary difference between these two tools of destruction is that worms do not require access to programs to replicate themselves. Worms take advantage of shared directories, interconnected machines and vulnerable network services. Computer viruses usually require a user to activate them by opening a file or clicking on the virus executable. Worms generally do not require user activity to infect other hosts and can replicate themselves by taking advantage of open network shares or by exploiting vulnerable services on operating systems.

One of the most recent and widely known worms to wreak havoc on computers around the world is known as the **Blaster or Lovsan Worm**. Chances are that you have already heard about this worm and your organization has already patched this worm/vulnerability. Just mention the Blaster worm to any of the IT folks, and if they look at the ground and shake their heads back and forth in disgust, then they have dealt with it in one-way or another. The Computer Emergency Response Team (CERT) website has reported that the Blaster worm takes advantage of a recently discovered vulnerability on Windows Operating systems, specifically Windows NT 4.0, Windows 2000, Windows XP and Windows Server 2003. The vulnerability exists with the Windows implementation of the DCOM Remote Procedure Call (RPC). Proper execution of the exploit results in remote command line access with administrator rights. The Blaster worm actively scans addresses on the Internet/network for vulnerable hosts to infect. When it finds a host vulnerable to the RPC exploit, it attempts to copy a file called msbalst.exe or teekids.exe or penis32.exe to the vulnerable host. Once the file has been copied, the vulnerable, and now infected host establishes a connection to the target host to execute the msblast.exe code. The infected computer then begins to actively scan for other vulnerable hosts as well as launch a distributed denial of service attack against the Microsoft update website.

If, by chance, your organization has not patched this vulnerability by now, then you are behind the curve and need to do so immediately. The remedy for a computer infected with the Blaster worm can be complicated when applied at the enterprise wide level. While the worm does not appear to be malicious in the sense of deleting files on the infected system, it does take up a significant amount of network resources. The more computers on a network that are infected, the more resources will be consumed, possibly to the point of a Denial of Service at the network level. CERT recommends, first and foremost, installing the patches provided the Microsoft update web site. There have been several mutations of the blaster worm so simply installing the first patch provided by Microsoft is not good enough. These patches should be applied to all computers running the vulnerable operating systems whether or not the machine is infected. CERT also recommends filtering access to TCP ports 135, 139, 445, 593 and 4444 as well as UDP ports 69, 135, 139 and 445 from the Internet through the use of firewalls or packet filters. CERT recommends invoking Microsoft built-in packet filter called ICF (Internet Connection Firewall) and disabling the DCOM service prior to reconnecting to the network to download the patch. This process can be very time consuming for one computer/workstation; consider the ramifications of all the Windows computers on an enterprise network being infected with this, not to mention the different varieties or mutations of the Blaster worm that are also in existence. For more detailed information on this worm visit the CERT web site at http://www.cert.org/advisories/CA-2003-20.html.

Another recent and nasty worm reported by CERT is called the **Sobig.F worm** and is an example of a worm propagated using email as a transport medium. The Sobig.F worm by definition is a combination of a virus and a worm; as it requires a user to open an email attachment in order for it to work, and then replicates itself automatically across Windows operating systems. In some cases, an email program may open the virus automatically if it is configured to do so. In any case, the Sobig.F worm infects computers via an email attachment with a .pif extension (CERT).

The infected emails have subject lines containing one of the following according to CERT web site:

- Re: Thank You!
- Thank You!
- Your details
- Re: Details
- Re: Re: My details
- Re: Approved
- Re: Your application
- Re: Wicked screensaver
- Re: That movie
- movie0045.pif

The infected files attached to the emails have the following names:

- your_document.pif
- document_all.pif
- thank_you.pif
- your_details.pif
- details.pif
- document_9446.pif
- application.pif
- wicked_scr.scr

The Sobig.F worm has to be invoked by a user clicking on the attachment or by an email application that opens email attachments automatically. The worm then installs itself on the computer and scans the computer's files for additional email addresses. Specifically, the worm looks for email address in files with .htm, .html, .dbx, .hlp, .mht, .txt, and .wab extensions. The worm then sends itself to all the email address identified in its scan via the infected computers SMTP (Simple Mail Transfer Protocol) engine.

Another function of the Sobig.F worm is that at certain predetermined times the worm attempts to contact one of twenty IP addresses on UPP port 8998. CERT believes that connection is an attempt to download additional information from or to the infected host. It would be prudent to block these addresses from all inbound and outbound traffic. More information on these addresses can be found at the following URL:

URL: http://www.cert.org/incident_notes/IN-2003-03.html

Most, if not all, antivirus software firms have developed signature-based identification for the Sobig.F worm. CERT recommends installing the latest antivirus update to protect potentially vulnerable systems. CERT also recommends that users not download or run programs from organizations or people that are not trusted. Unless the attachment is expected, it should not be opened until the sender can verify it as a legitimate file. CERT says that blocking Internet traffic from the following UDP ports: 123, 995, 996, 997, 998, 999, and 8998 will also reduce exposure to the effect of this worm.

The CERT team has reported another email-based worm, called Swen.A. The Swen.A worm, however, is more than just an email worm. The Swen.A worm is similar in nature to two other worms called GIBE.F and GIBE.B, all of which are intended to attack Windows-based operating systems. These worms replicate themselves via network shares and email. In order for the worm to be activated, it must be opened by a user or an email application that automatically opens email attachments. This worm is particularly clever as it attempt to disable security and antivirus-related processes running on the infected computer. Much like the Sobig.F worm, the Swen.A worm scans the infected computer for email addresses and attempts to send itself to identified email addresses as an attachment to an email. The infected email looks as though it is an update from Microsoft, with the intention that unsuspecting users will likely open it. As with the Sobig.F worm, CERT says the best line of defense for this worm is updating and running of antivirus software. Additionally, users should be assured that Microsoft will never send updates via email. As mentioned earlier, users should be aware of email attachments that they are not expecting or that cannot be verified by the sender.

When it comes to **protecting systems from viruses and worms**, several common controls come into play. First, it is important to implement a strong antivirus signature update process. Most antivirus applications are capable of automatically checking for updated signatures on a set schedule. Home users need to be equally aware and prudent in updating their antivirus software. Second, organizations should train their employees not to open unexpected email attachments – as if you have never heard that one before! If you have a computer at home, it would also be a good idea to talk to your family about email attachments. Finally, organizational security teams should consult the CERT web site frequently for the most recent information on viruses and worms and other vulnerabilities. The detailed information offered by CERT is invaluable in protecting information systems from viruses, worms, and trojan horses, among other IT security-related subjects. The use of an updated personal firewall or host-based firewall will also offer a degree of protection from worms and viruses. Consider these controls as your computer's immune system. These are the basics; there are many more complicated steps and controls that can be used to secure information systems from viruses and worms as well. The motive of this article is to refresh what you may already know and provide a high level view to a very complicated and technical problem facing organizations and home computer users alike. Keep in mind, the stronger your immune system, the less chance you have of catching a cold.

Please email your comments regarding this email to chad@canaudit.com. I look forward to reviewing them and responding to your questions or comments.

Chad Parks
Manager, Technical Audits & Security Services