[Reprinted from Flotilla 47 5NR Newsletter, Volume 1, Issue 2]

Awareness of Vulnerabilities on our Computers and Consumer Electronics

For the month of January, there were over 18 low severity, 14 medium severity and 29 high severity vulnerabilities reported on computers running Windows operating systems. These vulnerabilities included worms, trojans, viruses and holes, but not all vulnerabilities were exploited.

Different strains of Zar, Baba and MyDoom worms returned in January. Zar.a duped recipients into opening the attachment and launching the worm. It took advantage of users by its subject "Tsunami Donation! Please help". Baba.c claimed that its attachment "Evidence Cleaner" can hide any traces of pornography. The attached file ran the worm that opened a backdoor to give the hacker access to the PC. MyDoom.ai spread via e-mail and popular file-sharing software and tried to disable security software to block access to anti-virus update sites preventing infected machines from being purged (Keizer, 1/18/05).

Although Windows is a large target for exploiting vulnerabilities, below are examples of other issues reported last month.

- iTunes 4.x suffered from a vulnerability caused by a boundary error within the handling of .m3u and .pls playlists. This could cause a buffer overflow allowing a hacker to gain complete control on the users machine (Courtesy of TechWeb News).
- A California man hacked into T-Mobile's network and stole hundreds of names and social security numbers (Reuters).
- The ownership of the domain name Panix.com for the New York based ISP had been moved to a company in Australia, the DNS records had been moved to the United Kingdom and the company's email was redirected to a company in Canada (Musil).
- Several Lexus cars have GPS systems that connect to mobile phones to allow hands-free calling using Bluetooth. Potentially, this could also be used to transmit a virus to infect the onboard computer. Antivirus companies are researching these reports (Ilett).

Based on these types of attacks and vulnerabilities, it is predicted that there could be at least one devastating attack on the Internet in the next 10 years. This is according to the Pew Internet & American Life Project's survey. One expert wrote "Given the current terrorist context we live in and the interest in hackers to show off their skills this is inevitable, as is the unfortunate human quality to only fix the problem once it has occurred" (Keizer, 1/10/05). So what do we do to protect ourselves?

A great place to start is at the US-CERT web site (www.us-cert.gov) that is also under the Department of Homeland Security. You can join a mailing list for CERT alerts, read articles on how to protect yourself, plus find out much more information. Not only do we protect our computers and electronics against exposure to these vulnerabilities, but also we help protect everyone else.

References

Weekly Security Bulletins, www.us-cert.gov

Keizer, G. (Jan 18, 2005), "Trio Of Pesky 'Firsts' Threaten Computer Users", InternetWeek, http://www.internetweek.com/story/showArticle.jhtml?articleID=57702024

Courtesy of TechWeb News (Jan 12, 2005), "iTunes Bug Leaves Users Vulnerable To Hack", Internetweek, http://www.internetweek.com/story/showArticle.jhtml?articleID=57700911

Reuters, (Jan 13, 2005), "T-Mobile Says Hacker Penetrated Computer Network", Yahoo! News, http://news.yahoo.com/news?tmpl=story&u=/nm/20050113/us_nm/telecoms_tmobile_dc_6

Musil, S. (Jan 16, 2005), "ISP suffers apparent domain hijacking", ZDNet News, http://news.zdnet.com/2100-9588_22-5538227.html

Ilett, D. (Jan 26, 2005), "Lexus a nexus between cars and phone viruses?", ZDNet News, http://news.zdnet.com/2100-1009_22-5551367.html

Keizer, G. (Jan 10, 2005), "Devastating Attack In The Net's Near Future, Experts Say", InternetWeek, http://www.internetweek.com/story/showArticle.jhtml?articleID=57700341

Mike Rzucidlo, FSO-CS 47 5NR
mikerz@yahoo.com