THREATS & VULNERABILITIES

SECURITY AND YOUR BUSINESS

Computer Malware: What You Don't Know Can Hurt You

'Computer virus' has become a part of our common vocabulary. Viruses are, however, only one of several types of **mal**icious soft**ware**, or malware. For the casual computer user, business owner or manager, the catch-all term 'virus' is sufficient to describe all of the various types of malware. A deeper understanding of the three flavors of malware and their defining characteristics, however, will allow the reader to gain a better understanding of the real threats posed by malware.

Malware Defined

There are three basic types of malware: viruses, worms and Trojan horses. All three can range on the threat scale from 'annoying' to 'hazardous' and all three can be distributed in a variety of variants with a broad scope of possible risks.

Malware is omnipresent and represents one of the biggest single sources of financial risk associated with the Internet. The International Computer Security Association LABS (www.icsa.net) has identified over 52,000 distinct malware programs and variants. Various tracking agencies put the financial impact of malware globally in the multiple billions of dollars per year. Let's take a look at each variety of malware.

Viruses

Virus is the most commonly used term for malicious software and, in fact, is the most common form. Viruses need a 'host' program in order to operate. An example of a well-known virus is the Melissa, (or Mailissa or Malissa), virus that was propagated via email and infected Microsoft Word files. This is a potent virus. Melissa not only deleted application files such as word processing documents, it also deleted key files required for the proper functioning of the computer's operating system. Melissa was highly disruptive and the cost of virus elimination and system repair was very high. The International Computer Security Association estimates that the global financial impact of Melissa was CDN$ 589 Million.

The term virus can be misapplied, as in the case of the I Love You *virus*, which was, in fact, a worm.

Worms

Worms do not require a host program and can make copies of themselves and move rapidly, effectively clogging up the plumbing of the Internet: its communications lines and servers. This is, in fact, what how the I Love You worm worked. It replicated itself and mailed itself to an infected machine's full Outlook email list. ICSA estimates the global damage of I Love You and its variants at as much as CDN$ 15 Billion.

Trojan horses

Like the well-known horse of Troy, which was a 'gift' actually containing soldiers who stayed inside the hollow horse until they were inside their enemy's castle, Trojan horse software is not what it seems to be. An example of Trojan horse software popular several years ago was an electronic St. Patrick's Day greeting card with a hidden capability. While animated Leprechauns danced and cajoled, the recipients' Quicken™ financial software security and account information was being transferred to the Philippines. The account information was later used to transfer inconsequential amounts of money from hundreds of thousands of bank accounts to accounts in the Philippines. No financial impact estimate is available for this malware, but the impact per individual was less than US$10, while the sum of all transfers is likely to be in the millions.

Virus Hoaxes

Almost as bad as actual malicious software that compromises your information or uses your system for malicious purposes are virus hoaxes - rumors of viruses that cause disruption and lost productivity on a scale similar to an actual virus or worm attack.

Take for instance the disruption of the alleged Good Times 'virus'. Word of the 'virus' was spread via an email that received widespread distribution through the forwarding efforts of individuals with mutual trust relationships. The email was the only thing that existed - the 'virus' it described did not. The email warned, among other things *"if the computer contains a hard drive, that will most likely be destroyed. If the program is not stopped, the computer's processor will be placed in an nth-complexity infinite binary loop -which can severely damage the processor if left running that way too long."* Huh? Pure rubbish in fact, but a call to arms to a non-technical PC user.

There is no financial estimate for the lost work and resources expended on Good Times, but one thing is for sure - the email took a lot less time and expertise to write than an actual virus would have required.

What You Can Do to Protect Yourself

The very best solution is to have professional virus protection software installed on each and every laptop and desktop computer in the organization. The virus software must also be kept up to date, at times on a daily basis. Most good virus checkers automate this function if you are connected to the Internet.

User awareness and diligence are also critical: someone has to be the first to be attacked before the virus software can be updated. Users should be leery of emails with attachments, unusual software performance and anything that is "not quite right". Organizations should have clear guidelines and a well-known procedure for reporting suspected problems.

Conclusion

When it comes to computer malware, what you don't know can hurt you. Do you presently have a working copy of 'anti-virus' program on your PC? Do you have an active subscription to the regular upgrade program for the virus profiles? If not, you are wide open to one of the most common and devastating types of Internet problems and should take action immediately. Your Internet Service Provider (ISP) is often the best source for good sound advice and cost-competitive virus protection.

What else can you do? Designate an individual within your organization, regardless of your organizations' size or status, to champion the cause of malware awareness and eradication. If that individual is the ambassador for virus updates, awareness and swift problem reporting, the organization will benefit immensely from their efforts and will have an effective virus security blanket.

James P. Cavanagh is a global telecom and security consultant and the founder of The Consultant Registry. He is based in Atlanta, Georgia, USA but understands that he is a target for malicious software than can originate anywhere from Tokyo to Tehran.

A series of free security white papers is available at **http://www.consultant-registry.com/**. Email the author at **jcavanagh@consultant-registry.com**.