

Viruses, Worms and Vaccines...

Introduction

IT users constantly live under the threat of viruses and worms and many other forms of malicious software – we scan just about everything these days – even mobile phones are prone to viruses! While viruses are destructive computer programs that attach themselves to other programs, worms do not need user intervention and do not have to attach themselves to other programs as they move through a machine or networks – both cause similar levels of damage.

The challenge

With the widely dispersed and virtual IT environments that we operate in, we are exposed to several type of security threats to the IT infrastructure – there can be many single point of failure and hence it is very difficult to have a foolproof method especially if you use the internet – e.g. out of date virus scanners, weak passwords, shared computing resources...the list is endless.

History of viruses and types

The first computer virus, called the Brain virus was created in 1986 by 2 Pakistani brothers – Amjad and Basit Farooq Alvi – this was essentially a virus for destroying boot records on floppies. Then came the Lehigh virus in the US at a university which was a memory resident virus that attached executable viruses and took control when a file was opened. Then came the Jerusalem virus at Hebrew University, Isarel and the Cascade virus in Germany.

The basic types of viruses can be classified into 3 types – Trojans, Worms and Email viruses. Trojans mask themselves as harmless programs / files; worms copy themselves using flaws in the computer / network security and are more complex; email viruses use email / attachments to spread viruses. For those who want to go more into detail, there are many sub types of viruses – e.g. Network viruses that degrade the performance of a network, Stealth virus (e.g. Frodo, number of the beast etc) which hide themselves in the system memory every time a scanner is run; Multipartite virus (e.g. Ghostball, Emperor, Tequila etc) which can infect both program files and boot sectors; Companion viruses, Polymorphic viruses, Macro viruses etc.

History of worms and types

Self replicating code (this is how worms work) was first created by Ken Thompson in 1984 and this can be thought of as the precursor to the worms that abound today and first made their presence in the early days of the Unix operating system. Some examples include Chernobyl and Michelangelo. The earliest self propagating worm was the Morris worm causing buffer overflows, debugging routines in mail components, password sniffing etc.

Worms are similar to viruses yet very distinct as well – it does not require a host file in order to propagate and can instead work on system vulnerabilities such as open ports, Examples of worms include the Nimda worm, Slapper worm, Sober X worm, MyDoom worm and more recently the Valentin E and the Nuwar OL worm.

Prevention, tools and software

Other than the tools and software for detection, there are some basic work practices to avoid viruses and worms which should be enforced through the organization's IT policy – e.g. avoid opening emails/email attachments from unknown senders – especially with themes relating to holidays, money or dating; never click on links in an email message even if it from a reliable source; beware of unknown sites you visit (you can use a rating tool to check out the site); change passwords regularly.

Over and above anti virus software, a personal firewall is a good start point on PCs and laptops – most ISPs provide good service bundles which are especially useful for individual, home or small business users. Good software bundles are available from Norton, Symantec, Microsoft, Mc Afee, Kaspersky Labs, Trend Micro, Eset, Frisk Software, Quick Heal Pro, Network Associates, Sophos etc. From an operating system perspective, Linux is still a safe bet since most of the viruses and worms have targeted Microsoft O/S.

How the tools work

As per an article on MacTech, anti virus products can be divided into Class 1 (Infection prevention products), Class 2 (Infection detection products) and Class 3 (Infection identification products). There are 3 approaches used by these softwares – the first is viral signature matching requires information about the virus; the second is code enumeration involves examining known programs periodically to check for unknown fragments of code; the third is the checksum method to check file sizes.

Virus, Worms and networks

Viruses and worms can also impact networks on a large scale – this requires lot more sophisticated intrusion detection that is ensured by a combination of techniques involving hardware and software – today there are several devices available that come built with firmware or software that can protect a complete network effectively – companies such as Cisco, Juniper, Sonic Wall, Nokia etc have such products – net appliances also come bundled with security and monitoring / detection tools. As one can see, virus and worms are just too vast a subject to completely understand – what works is a combination of policy, process and tools and a constant audit of the system – exactly similar to that health check you always skip ! -