The computer worm virus computer science essay

Technology, Computer

The computer worms are programs that reproduce, duplicate independently and travel to spread across networks, it does not rely on the host file or boot sector and the transfer of files between computers to spread and this is the main key difference between the computer virus and the worm virus. Computer Worms are skilled to damage entire series of data as destroying crucial and important files, slowing it down or even stop the computer from working at all.

It keeps on spreading unless no more computers are left to be infected on the same network, such viruses are dangerous in businesses that use large number of networks.

The Most Well-Known examples of computer worm

These are examples of most famous computer worm and their specific features:

Internet worm or Morris worm: The Morris worm or Internet worm was the first worm that was spread and launched through the Internet and the first to achieve important attention in the media.

It was launched on internet accidently by Robert Tappan Morris in 1988. It was created originally to figure the size of the internet and not to cause damage. However, as a result of the code an unexpected outcome caused it to be more destroying and harmful.

A computer network can be harmed multiple times with each added process causing to slow down the computer. After all, it will make the computer unusable.

Sobig worm: It is a worm that appeared in 2003 for the first time. Since then, it has infected millions of Microsoft Windows computers connected to the Internet.

As a worm, it can duplicate itself. It also has some similar features to a Trojan virus because it spreads as an electronic email by itself.

It has six types but the most well-known, widespread and famous is its Sobig. F variant.

Mydoom: It is an affecting Microsoft Windows computer worm . It is also named as , Novarg, Mimail. R and Shimgapi .

In January 2004 it was considered as the fastest email worm sreading, beating the set Sobig worm record. On January 26, 2004 it was first appeared.

The email messages containing these sentences are the way mydoom worm spreads through like " Andy; I'm just doing my job, nothing personal, sorry". It was said to launch this worm the creator was paid to do so. However the real creator is unknown.

It shares some similarities to a Trojan virus that a user's computer gets as soon the infected attachment in an email is opened.

Blaster Worm: It spreads through networks running windows XP and Windows 200 operating system on the computer. This worm is also called Lovesan or Lovsan. It was first developed in August 2003.

There are two messages that this worm acts as a virus in. The first message contains " I just want to say Love You San" thus giving the name Lovesan worm. The second message was specified for Bill Gates, the worm target. The message says " Billy Gates why do you make this possible? Stop making money and fix your software".

How to avoid getting computer worm virus?

Email is the most common way of getting infected: To open an email or link safely u must know the source and never ever click unless you are positive about it. Here are two common ways that it is usually done by:

A good way to avoid this is to use Mozilla Firefox, since it is known to be more secure. An email that you receive from any source that you know or you don't but it contains a link for you to open and you click on it and here it goes the virus is allowed to your computer. It appears to be an email from some one you may know, don't fall for it! It was actually malicious code executed in your browser that allowed it to look like it is coming from an actual source.

You may receive an email from a friend you know but the email is not really sent by her it may be her infected computer and the worm that generated the email sent, it usually carries a message that would encourage you to open it but it is not a personal message from your friend as it is the virus that formed it like" Hey, check out this important site of yoursaˆ¦." etc and here you go your computer is infected.

Don't click on pop-up windows that announce a sudden disaster in your city: A cracker(hackers that aim to confuse important information to make users angry, not to hack personal data or steel properties) used your Internet protocol address to determine the location you are in, and then sends you an email that makes you open it like " you would like to know the causes of earthquake or anything similar" you click and here the device is infected.

Be careful about using MS Outlook: It is the most acceptable application to the worms more than other e-mail programs. To avoid its spreading you can better use anti-virus or also try Outlook anti-spam addons freely available on Microsoft's Web site.

Do not use disks that other people gave you, even from work: you can use anti-virus programs to scan a disk or CD that maybe infected with the worm virus even if you have got this disk from work or important sources, but at times the AV programs are not 100% effective. The drive can be wiped using a bootable CD like DBAN then it will be safe.

Do not download applications from un-trusted websites: Downloading from trusted websites with the license is safer than old websites, however, the threat isn't only in the applications but also words documents that have more than one extensions listed above

Set up your Windows Update to automatically download patches and upgrades: This will help you to get the latest updates done automatically and safely by your device instead of you doing such updates from un-trustable

sites. This automatic updates also fix security holes in both pieces of software.

Use a software firewall: Read about the latest virus threats so you are aware of the potential danger that may affect your devices.

Avoid file sharing: Peer-to-peer file sharing is another source of viruses. Like some of the viruses above, these are viruses that you invite into your computer. If you use peer-to-peer file sharing to download music, videos, games, or other information you put yourself at legal risk for piracy, and you put your computer at serious risk to computer worm to infect your computer.

Keep Your Computers Patched: Worms most often rely on unpatched computers to spread. They use vulnerable network services to infect and gain access to the computer's resources. Patches fix the vulnerabilities.

Read more: http://www. brighthub. com/computing/smb-security/articles/42130. aspx#ixzz1J4DKiqKA

Harmful effects of computer worms
Its hard to ignore the psychological damages an owner system may have as a result of the computer worm. Some of the worms are designed and un leached to replicate it self on a system to stock it and then send back the information on that system to the user. It can also be used to create " hordes" of " zombie" computers, that is controlled by a remote user that can destroy a service or website using these computers.

Sources:

http://www. wikihow. com/Avoid-Getting-a-Computer-Virus-or-Worm-on-Your-Windows-PC

Computer Worms

Worm Virus