CYBER SAFETY

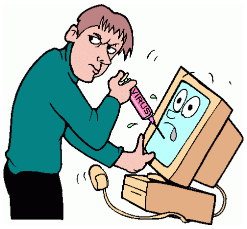
Table of Contents

One common mistake that people make when the topic of a computer virus arises is to refer to a worm or Trojan horse as a virus. While the words Trojan, worm and virus are often used interchangeably, they are not exactly the same thing. Viruses, worms and Trojan Horses are all malicious programs that can cause damage to your computer, but there are differences among the three, and knowing those differences can help you better protect your computer from damaging effects.

What Is a Computer Virus?

A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus can range in severity: some may cause only mildly annoying effects while others can damage your hardware, software or files. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program.

It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going. Because a virus is spread by human action people will unknowingly continue the spread of a computer virus by sharing infecting files or sending emails with viruses as attachments in the email.



Fast Facts: Attaches to an executable file, requires human action to spread.

What Is a Worm?

A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.

The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues on down the line.

Due to the copying nature of a worm and its capability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding. In recent worm attacks such as the much-talked-about Blaster Worm, the worm has been designed to tunnel into your system and allow malicious users to control your computer remotely.

Fast Facts: Can replicate itself on system, does not require human action to spread.

What Is a Trojan horse?

A Trojan Horse is full of as much trickery as the mythological Trojan Horse it was named after. The Trojan Horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer. Those on the receiving end of a Trojan Horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source.

When a Trojan is activated on your computer, the results can vary. Some Trojans are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

Fast Facts: Appears useful but damages system, requires human action to run, do not self-replicate.

What Is a Blended Threat?

Added into the mix, we also have what is called a blended threat. A blended threat is a more sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan horses and malicious code into one single threat. Blended threats can use server and Internet vulnerabilities to initiate, then transmit and also spread an attack. Characteristics of blended threats are that they cause harm to the infected system or network, they propagates using multiple methods, the attack can come from multiple points, and blended threats also exploit vulnerabilities.

To be considered a blended thread, the attack would normally serve to transport multiple attacks in one payload. For example it wouldn't just launch a DoS attack — it would also, for example, install a backdoor and maybe even damage a local system in one shot. Additionally, blended threats are designed to use multiple modes of transport. So, while a worm may travel and spread through e-mail, a single blended threat could use multiple routes including e-mail, IRC and file-sharing sharing networks.

Lastly, rather than a specific attack on predetermined .exe files, a blended thread could do multiple malicious acts, like modify your exe files, HTML files and registry keys at the same time — basically it can cause damage within several areas of your network at one time.

Blended threats are considered to be the worst risk to security since the inception of viruses, as most blended threats also require no human intervention to propagate.

Fast Facts: Sophisticated, bundles aspects of viruses, worms and Trojan horses, most require no human action.

Protect Myself from Cyber Attacks

The Department of Homeland Security plays an important role in countering threats to our cyber network. We aim to secure the federal civilian networks, cyberspace and critical infrasture that are essential to our lives and work.

DHS's National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 center responsible for the production of a common operating picture for cyber and communications across the federal, state, and local government, intelligence and law enforcement communities and the private sector.

Next Steps

The following preventative strategies are intended to help our public and private partners proactively look for emails attempting to deceive users into "clicking the link" or opening attachments to seemingly real websites:

- Never click on links in emails. If you do think the email is legitimate, whether from a third party retailer or primary retailer, go to the site and log on directly. Whatever notification or service offering was referenced in the email, if valid, will be available via regular log on.
- Never open the attachments. Typically, retailers will not send emails with attachments. If there is any doubt, contact the retailer directly and ask whether the email with the attachment was sent from them.
- Do not give out personal information over the phone or in an email unless completely sure. Social engineering is a process of deceiving individuals into providing personal information to seemingly trusted agents who turn out to be malicious actors. If contacted over the phone by someone claiming to be a retailer or collection agency, do not give out your personal information. Ask them to provide you their name and a call-back number. Just because they may have some of your information does not mean they are legitimate!

Other practical tips to protect yourself from cyberattacks:

- Set secure passwords and don't share them with anyone. Avoid using common words, phrases, or personal information and update regularly.
- Keep your operating system, browser, anti-virus and other critical software up to date. Security updates and patches are available for free from major companies.
- Verify the authenticity of requests from companies or individuals by contacting them directly. If you are asked to provide personal information via email, you can independently contact the company directly to verify this request.
- Pay close attention to website URLs. Pay attention to the URLs of websites you visit. Malicious websites sometimes use a variation in common spelling or a different domain (for example, .com instead of .net) to deceive unsuspecting computer users.
- For e-Mail, turn off the option to automatically download attachments.
- Be suspicious of unknown links or requests sent through email or text message. Do not click on unknown links or answer strange questions sent to your mobile device, regardless of who the sender appears to be.

Summary:

- common threats
    1) Virus
    2) Worm
    3) Trojan horse
    4) Blended Threat
- Protecting yourself
    1) Don’t click on links in emails
    2) Never open the attachments
    3) Don’t give away personal information
    4) Pick secure passwords

Bibliography

U.S. Departement of Homeland Security. (2016, January 20). *Protect Myself from Cyber Attacks*. Retrieved from http://www.dhs.gov/how-do-i/protect-myself-cyber-attacks

Vangie, B. (2016, January 20). *The Difference Between a Computer Virus, Worm and Trojan Horse*. Retrieved from http://www.webopedia.com/DidYouKnow/Internet/virus.asp