

Forum:[Hack Forums](#)

Thread: [WHAT IS VIRUS, TROJEN HORSE AND WORM](#)

killerazeem - April 24, 2010, 9:42 pm

The most common blunder when the topic of a computer virus arises is that people will often refer to a Worm or Trojan Horse as a Virus. While the words Trojan, worm, and virus are used interchangeably, they are not the same. Viruses, worms, and Trojan Horses are all malicious programs that can cause damage to your computer, but there are differences between the three, and knowing those differences can help you to better protect your computer from their often damaging effects.

VIRUS:---

A computer Virus attaches itself to a program or file so it can spread from one computer to another, leaving infections as it travels. Some viruses 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 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. People continue the spread of a computer virus, mostly unknowingly, by sharing infecting files or sending e-mails with viruses as attachments in the e-mail.

WORM:---

A Worm is similar to a virus by its 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 ability to travel without any help from a person. A worm takes advantage of file or information transport features on your system, which allows it to travel unaided. The biggest danger with a worm is its ability 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 ability 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 more 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.

TROJAN:---

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. The Trojan horse itself would typically be a Windows executable program file, and thus must have an executable filename extension such as .exe, .com, .scr, .bat, or .pif. Since Windows is sometimes configured by default to hide filename extensions from a user, the Trojan horse is an extension that might be "masked" by giving it a name such as 'Readme.txt. exe'. With file extensions hidden, the user would only see 'Readme.txt' and could mistake it for a harmless text file. When the recipient double-clicks on the attachment, the Trojan horse might superficially do what the user expects it to do (open a text file, for example), so as to keep the victim unaware of its real,

concealed, objectives. Meanwhile, it might discreetly modify or delete files, change the configuration of the computer, or even use the computer as a base from which to attack local or other networks – possibly joining many other similarly infected computers as part of a distributed denial-of-service attack. 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.

MIXING:-----

Added into the mix, what is called a blended threat? A blended threat is a sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan horses and malicious code into one threat. Blended threats use server and Internet vulnerabilities to initiate, transmit and spread an attack. This combination of method and techniques means blended threats can spread quickly and cause widespread damage. Characteristics of blended threats include: causes harm, propagates by multiple methods, attacks from multiple points and exploits vulnerabilities.

To be considered a blended threat, 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 install a backdoor and damage a local system in one shot. Additionally, blended threats are designed to use multiple modes of transport. For example, a worm may travel through e-mail, but a single blended threat could use multiple routes such as e-mail, IRC and file-sharing sharing networks. The actual attack itself is also not limited to a specific act. For example, rather than a specific attack on predetermined .exe files, a blended threat could modify 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 require no human intervention to propagate.

Combating Viruses, Worms and Trojan Horses :

The first steps to protect your computer are to ensure your operating system (OS) is up-to-date. This is essential if you are running a Microsoft Windows OS. Secondly, you should have anti-virus software installed on your system and download updates frequently to ensure your software has the latest fixes for new viruses, worms, and Trojan Horses. Additionally you want to make sure your anti-virus program has the ability to scan e-mail and files as they are downloaded from the Internet. This will help prevent malicious programs from even reaching your computer. If this isn't enough protection, then you may want to consider installing a firewall as well.

A firewall is a system which prevents unauthorized use and access to your computer. A firewall can be either hardware or software. Hardware firewalls provide a strong degree of protection from most forms of attack coming from the outside world and can be purchased as a stand-alone product or in broadband routers. Unfortunately, when battling viruses, worms and Trojans, a hardware firewall may be less effective than a software firewall, as it could possibly ignore embedded worms in outgoing e-mails and see this as regular network traffic. For individual home users, the most popular firewall choice is a software firewall. A good software firewall will protect your computer from outside attempts to control or gain access your computer, and usually provides additional protection against the most common Trojan programs or e-mail worms. The downside to software firewalls is that they will only protect the computer they are installed on, not a network.

It is important to remember that on its own a firewall is unable to get rid of your computer virus problems, but when used in conjunction with regular operating system updates and a good anti-virus scanning software, it will add some extra security and protection for your computer or network.

this is not my own tut

UnknownEdition - April 24, 2010, 10:13 pm

Leeched tutorial!

<http://www.webopedia.com/didyouknow/internet/2004/virus.asp>

-=C0d3ak=- - April 24, 2010, 10:15 pm

Totally not ripped from else where, its the best explanations of viruses any one has ever did, ever.

killerazeem - April 24, 2010, 11:01 pm

thankx

i have already ask this is not my own..

..xX[ThunderStorm]Xx.. - April 25, 2010, 1:20 am

(Apr 24, 2010 10:13 PM)UnknownEdition Wrote: [\[CITE\]](#) Leeched tutorial!

<http://www.webopedia.com/didyouknow/internet/2004/virus.asp>

He has mentioned it that it's not his so what was the use of this?

Psilocybin Cubensis - April 25, 2010, 1:23 am

(Apr 24, 2010 10:13 PM)UnknownEdition Wrote: [\[CITE\]](#) Leeched tutorial!

<http://www.webopedia.com/didyouknow/internet/2004/virus.asp>

A little quick on the draw there, eh? Were you just looking for the "This tut is not mine" part to not be there so you could report it or something?

splatta - April 25, 2010, 2:13 am

you didn't explain what a "TROJEN" was...

--[(-S7N-)]-- - April 25, 2010, 3:43 am

This should be moved to the Computer Protection and Security section. Also, this is a good tutorial if you don't know the basics.

'Snorlax - April 25, 2010, 4:47 am

So what if he took it from someone else?

He's just trying to leech some rep.

I think he did it good.

Also, look at last line.

gaing - April 25, 2010, 5:31 am

Thanks for the tuto.

It is very good and helps.

whininguser - April 25, 2010, 5:32 am

Nice observation skills there... :D

--[(-S7N-)]-- - April 25, 2010, 6:00 am

He modified this post: 'This post was last modified: Today 01:00 PM' (My local time)
UnknownEdition posted 'Today, 12:13 PM' (My local time)

Therefore, I conclude that he just edited that part in after an hour of being caught for leeching.

killerazeem - April 25, 2010, 6:30 am

thankx all brothers for ur great replies..

(Apr 25, 2010 06:00 AM)--([-S7N-])-- Wrote: [\[CITE\]](#) He modified this post: 'This post was last modified: Today 01:00 PM' (My local time)

UnknownEdition posted 'Today, 12:13 PM' (My local time)

Therefore, I conclude that he just edited that part in after an hour of being caught for leeching.
brother u asked i edited this post i agree that i edit it..
but can u tell me wht i was edited...which part or line aur etc....
????????????????????????????????

--([-S7N-])-- - April 25, 2010, 7:05 am

Quote:this is not my own tut

Grammatical error not found in any other part of the tutorial, and you seem to post in bad grammar as well. That is how I can tell if you edited that part in or not. Besides, apart from that, everything in the tutorial matches, only minor edits maybe. By the way, I am not going to flame at you, just pointing out that you copy/pasted it. No hard feelings?

H3Gatm4h - May 2, 2010, 5:23 pm

good tut great info thx

Malitastic - May 2, 2010, 5:28 pm

Good share, might prove useful for some computer security beginners

Neon666 - June 28, 2010, 9:27 am

Leeching is sad, or give the author the credits..

N0va

Ted - June 28, 2010, 10:51 am

For gods sake! This is the most leeched piece of shit in the world! You even spelled trojan wrong in the title dumbfuck..

Far - June 28, 2010, 11:41 am

Amazing tutorial, really liked it. Well done!

Caos Blitz - June 28, 2010, 12:26 pm

Wow thanks now i know the difference :P

alfonzo1955 - June 28, 2010, 12:29 pm

Someone should reformat this and re-post it.

lucario555 - June 29, 2010, 12:00 pm

wow thanx so much i really needed a tut like that thx

killerazeem - January 4, 2011, 10:09 am

thank to all of u...and sorry for leaching...

Node - *January 4, 2011, 11:54 am*

this is good for basics. thanks for the effort though