Worm, Virus & Trojan Horse: Ethical Hacking Tutorial

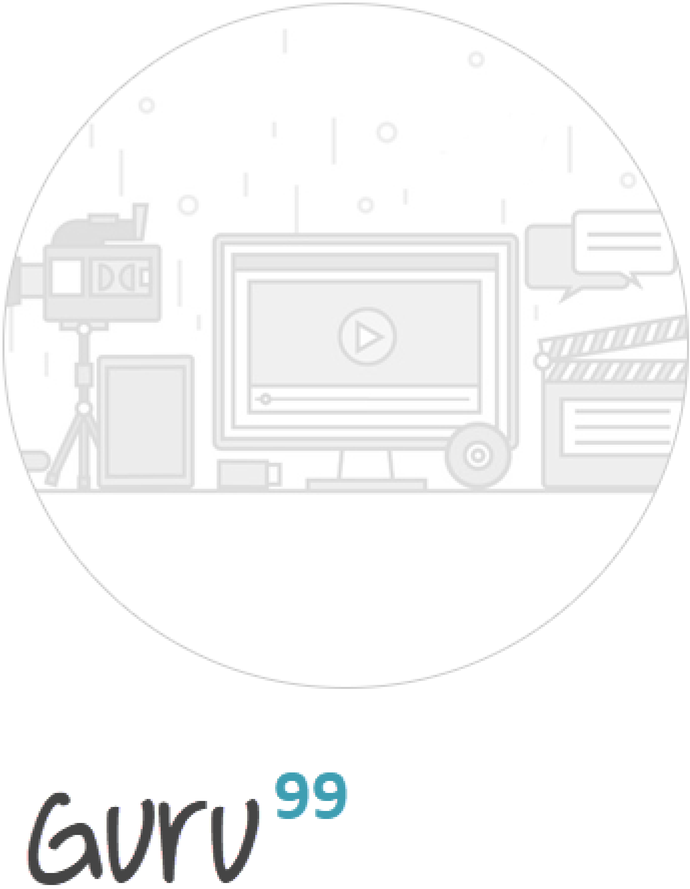
Some of the skills that hackers have are programming and computer networking skills. They often use these skills to gain access to systems. The objective of targeting an organization would be to steal sensitive data, disrupt business operations or physically damage computer controlled equipment. **Trojans, viruses, and worms can be used to achieve the above-stated objectives**.

In this article, we will introduce you to some of the ways that hackers can use Trojans, viruses, and worms to compromise a computer system. We will also look at the countermeasures that can be used to protect against such activities.

Topics covered in this tutorial

What is a Trojan horse?

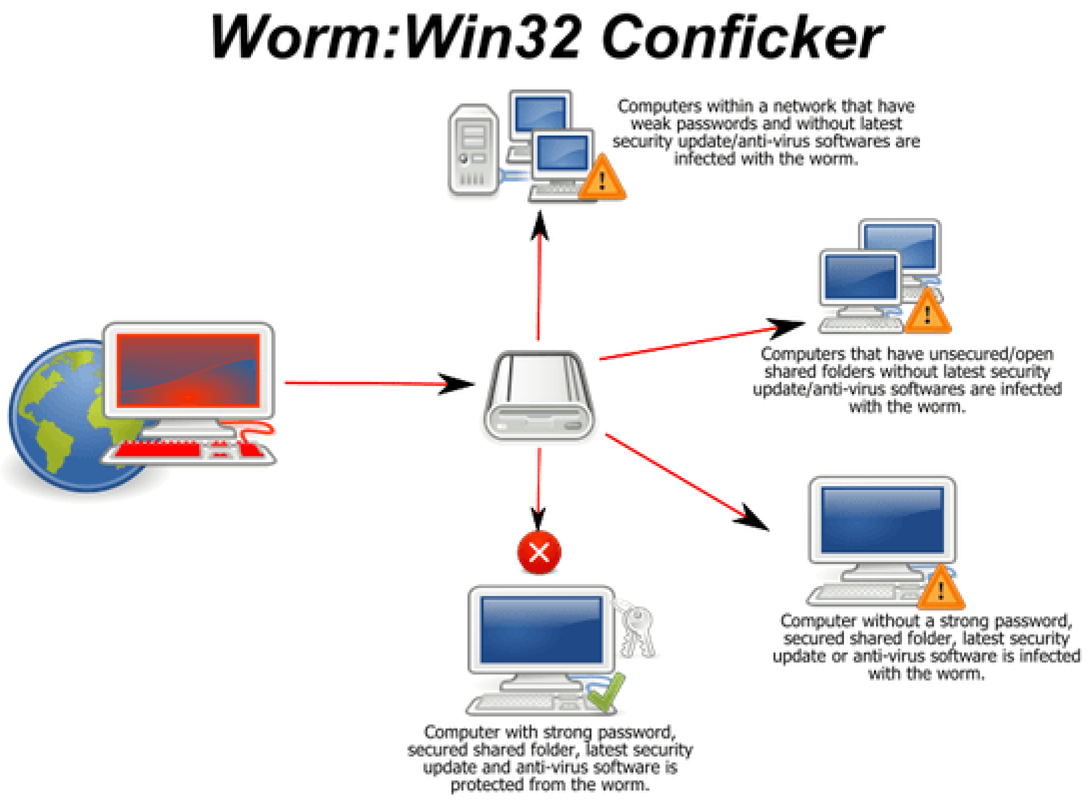
A Trojan horse is a program that allows the attack to control the user's computer from a remote location. The program is usually disguised as something that is useful to the user. Once the user has installed the program, it has the ability to install malicious payloads, create backdoors, install other unwanted applications that can be used to compromise the user's computer, etc.



The list below shows some of the activities that the attacker can perform using a Trojan horse.

- Use the user’s computer as part of the Botnet when performing distributed denial of service attacks.
- Damage the user’s computer (crashing, blue screen of death, etc.)
- **Stealing sensitive data** such as stored passwords, credit card information, etc.
- **Modifying files** on the user’s computer
- **Electronic money theft** by performing unauthorized money transfer transactions
- **Log all the keys** that a user presses on the keyboard and sending the data to the attacker. This method is used to harvest user ids, passwords, and other sensitive data.
- Viewing the users’ **screenshot**
- Downloading **browsing history data**

What is a worm?


Worm:Win32 Conficker
Computers within a network that have weak passwords and without latest security update/anti-virus softwares are infected with the worm.
Computers that have unsecured/open shared folders without latest security update/anti-virus softwares are infected with the worm.
Computer without a strong password, secured shared folder, latest security update or anti-virus software is infected with the worm.
Computer with strong password, secured shared folder, latest security update and anti-virus software is protected from the worm.

A worm is a malicious computer program that replicates itself usually over a computer network. An attacker may use a worm to accomplish the following tasks;

- **Install backdoors on the victim's computers**. The created backdoor may be used to create zombie computers that are used to send spam emails, perform distributed denial of service attacks, etc. the backdoors can also be exploited by other malware.
- Worms may also **slowdown the network by consuming the bandwidth** as they replicate.
- Install **harmful payload code** carried within the worm.

What is a Virus?

- A virus is a **computer program that attaches itself to legitimate programs and files without the user's consent**. Viruses can consume computer resources such as memory and CPU time. The attacked programs and files are said to be "infected". A computer virus may be used to;
    - Access private data such as user id and passwords
    - Display annoying messages to the user
    - Corrupt data in your computer
    - Log the user's keystrokes

Computer viruses have been known to employ **social engineering techniques**. These techniques involve deceiving the users to open the files which appear to be normal files such as Word or Excel documents. Once the file is opened, the virus code is executed and does what it's intended to do.

Trojans, Viruses, and Worms counter measures

- To protect against such attacks, an organization can use the following methods.
- A policy that prohibits users from downloading unnecessary files from the Internet such as spam email attachments, games, programs that claim to speed up downloads, etc.
- Anti-virus software must be installed on all user computers. The anti-virus software should be updated frequently, and scans must be performed at specified time intervals.
- Scan external storage devices on an isolated machine especially those that originate from outside the organization.
- Regular backups of critical data must be made and stored on preferably read-only media such as CDs and DVDs.
- Worms exploit vulnerabilities in the operating systems. Downloading operating system updates can help reduce the infection and replication of worms.
- Worms can also be avoided by scanning, all email attachments before downloading them.

Trojan, Virus, and Worm Differential Table

	Trojan	Virus	Worm
Definition	Malicious program used to control a victim's computer from a remote location.	Self replicating program that attaches itself to other programs and files	Illegitimate programs that replicate themselves usually over the network
Purpose	Steal sensitive data, spy on the victim's computer, etc.	Disrupt normal computer usage, corrupt user data, etc.	Install backdoors on victim's computer, slow down the user's network, etc.
Counter Measures	Use of anti-virus software, update patches for operating systems, security policy on usage of the internet and external storage media, etc.		

For SQL injection

https://www.youtube.com/watch?v=3Axp3VDnf0I