**HiLCoE**

School of Computer Science and Technology

Computer Systems Security (CS486)

Trojan Horse Attack

Group Members: ID NO:

1. Natnael Geremew OC0865
2. Solomon Tegabu AL1862
3. Yohannes Ketema JM8919

Submitted To: Mohammed Abdella

Submission Date: May 22, 2020

**Abstract**

A Trojan, or Trojan horse, is a type of malware that conceals its true content to fool a user into thinking it's a harmless file. Like the wooden horse used to sack Troy, the "payload" carried by a Trojan is unknown to the user, but it can act as a delivery vehicle for a variety of threats. A Trojan is sometimes called a Trojan virus or a Trojan horse virus, but that’s a misnomer. Viruses can execute and replicate themselves. A Trojan cannot. A user has to execute Trojans. Even so, Trojan malware and Trojan virus are often used interchangeably. One should thoroughly scrutinize apps or different files before installing in a computer, always download apps or files from trusted sources and use anti-malwares or anti-viruses because we can never be too safe.

1. **Introduction**

**Computer security**, also known as **cybersecurity** or **IT security**, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. In this paper we will be discussing more about the theft of information, disruption or misdirection of services due to a security breach and the famous Trojan horse attack that leads to the security breach.

This report is prepared to create awareness on disguised malicious attack or Trojan horse attack and to emphasis on the damage that such a breach may cause in this information era, also we have stated some methods that can be used as a prevention.

* 1. **Background**

The Trojan Horse is a story from the Trojan war about the subterfuge that the Greeks used to enter the independent city of Troy and win the war. In the canonical version, after a fruitless 10-year siege, the Greeks constructed a huge wooden horse and hid a select force of men Inside including Odysseus. The Greeks pretended to sail away, and the Trojans pulled the horse into their city as a victory trophy. That night the Greek force crept out of the horse and opened the gates for the rest of the Greek army, which had sailed back under cover of night. The Greeks entered and destroyed the city of Troy, ending the war.

A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system.

* 1. **Problem statement**

Trojan horses are big problems in today’s connected world, with all the data and information sharing in our recent era, computers are more susceptible to such an attack **In a Trojan horse attack, a criminal simply disguises malware as a legitimate piece of software (like a program or app) or even a harmless document (like a spreadsheet) to trick users into willingly installing it on their computer. Although there are different anti-malwares which are effective and available, most people are still victims to a well disguised malware**

* 1. **Methodology**

We have used the qualitative approach in order to prepare this paper, this method was used **to understand** concepts, thoughts or experiences, it enabled us to gather **in-depth insights** on topics that are not well understood and the thorough review of different researches conducted on the aspect.

1. Main text

2.1. What is a Trojan horse attack ?

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.

A Trojan is sometimes called a Trojan virus or a Trojan horse virus, but that’s a misnomer. Viruses can execute and replicate themselves. A Trojan cannot. A user has to execute Trojans. Even so, Trojan malware and Trojan virus are often used interchangeably.

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

**2.2. How Do Trojans Work & Spread?**

Hacking requires a lot of technical skill and know-how, in many cases. Cybercriminals will often scour software and operating systems for security [exploits](https://www.safetydetectives.com/blog/what-is-a-computer-exploit-tips-to-keep-you-safe/) or create complicated [worms](https://www.safetydetectives.com/blog/what-is-a-computer-worm-tips-to-protect-your-computer-in/) that replicate themselves and spread across networks. Eventually, someone realized it might be easier to just manipulate people into installing malware directly onto their own computer.

That’s the goal of a Trojan, which refers specifically to the way a malware payload is delivered and is not a form of malware or a virus by itself.

**Trojans can infect your computer and spread in a few different ways.**

## Email Attachments and Spam Messages

These seemingly harmless email attachments are often Trojan horse attacks; meaning, if you download the document and open it, you’ll trigger the installation of dangerous malware on your device.

## Freeware or Cracked Software

## Another common way cybercriminals trick users into installing malware is by disguising it as a real piece of software. Freeware from untreputable Internet marketplaces can sometimes turn out to be malware, and so can “cracked” software or free versions of software that normally cost money.

1. **Drive-By Downloads**

A drive-by download refers to a download onto your computer that you didn’t purposefully initiate.

This is a common form of malware distribution often seen on shady adult websites, software or media pirating sites, and the like. Just by visiting the site, your browser could trigger a download of malware with you even clicking anything.

1. **File Sharing**

Downloading files like movies or music over a torrenting service is risky business. There’s no way of verifying the file on the other end, so one easy way for hackers to spread malware is to disguise it as a popular movie available for people to download for free.

## 2.3 TYPES OF TROJAN HORSE

A Trojan horse isn't just a single type of virus. It also varies to its purpose. The cyber criminal can target a specific person or disseminate the [Trojan horse](https://enterprise.comodo.com/what-is-a-trojan-virus.php?af=7639) of his choice everywhere. This list will make you understand the different types of Trojan horses and what do they do:

**Backdoor**  
It gives malicious users [remote access](https://remoteaccess.itarian.com/?key5sk1=d9f5df09758f02c47d657c42f75d59ab28224e92&af=7639) over the infected computer. They can do whatever they want such as sending, receiving, launching and deleting files, displaying data and rebooting the endpoint.

**Exploit**  
It contains data or code that abuses a vulnerability within application software that’s operating on your endpoint.

**Rootkit**  
These are designed to hide certain objects or activities in your system. This can effectively prevent malicious programs being detected.

**Trojan-Banker**  
Its purpose is to steal your account data for online banking systems, e-payment systems and credit or debit cards.

**Trojan-DdoS**  
This Trojan can start up the Denial of Service (DoS) attacks. Not only it can affect endpoints, but also websites. By sending multiple requests – from your computer and several other infected computers – the attack can overload the target address which leads to a denial of service.

**Trojan-Downloader**  
Trojan-Downloaders can download and install new versions of malicious programs onto your computer – including Trojans and adware.

**Trojan-Dropper**  
Trojan-FakeAV programs copies the activity of [antivirus software](https://antivirus.comodo.com/?af=7639). They are created to extort money from you. In return, they'll remove the detection and threat removal. Even though, the threats that they report are don't actually exist.

**Trojan-GameThief**  
If you're into gaming, you know that online gaming can also garner loads of cash. Cyber criminals also crafted this Trojan virus which steals user account information from online gamers.

**Trojan-Ransom**  
This Trojan can change data on your endpoint. This can lead to endpoint malfunction. The cyber criminal will demand a ransom. They'll only replace your computer’s performance or unblock your data, after you have paid them.

**Trojan-SMS**  
This Trojan can change data on your endpoint. This can lead to endpoint malfunction. The cyber criminal will demand a ransom. They'll only replace your computer’s performance or unblock your data, after you have paid them.

**Trojan-Spy**  
Trojan-Spy programs can spy on how you’re using your computer – for example, by tracking the data you enter via your keyboard, taking screen shots or getting a list of running applications.

**Trojan-Mailfinder**  
This robs email addresses from your endpoint.

### 2.3 HOW TO SECURE YOURSELF FROM TROJAN HORSE:

We'll always preach the basic of security online. Though, that's all up to you if you'll practice safety. We're still here to guide you on further steps on how to fully stay safe from Trojan viruses. Just follow the tips in here:

**Antivirus**  
An effective antivirus can alert you when there's a suspicious file on your endpoint. You can start using free branded antivirus offered in the Internet. A Trojan can also take a form of an antivirus, so trusting a branded antivirus can also keep you away from the danger.

**Up-to-date Security Software**  
What's the use of antivirus when it's outdated? Update them when the updates are ready. It'll upgrade the software for better virus mitigation.

**Avoid Malicious Websites**  
These spread the danger among the community of Internet users. Malicious websites mostly have pop-up messages that can trick you. Better stay out of trouble.

**Ignore Unknown Emails**  
When you receive an email from an unknown sender, you can just ignore them and delete them. Trojans also take the form of an email attachments.

**Difficult Passwords**  
Confuse your enemies. Your difficult, creative passwords can save you from a big mess.

**Firewalls**  
A firewall monitors and controls incoming and outgoing network traffic on a standardized security rules. This another protection for your own good.

**In a Nutshell**  
Trojan horse viruses can act various preset tasks by a cyber criminal. It's better to know which Trojan horse virus you might encounter to prepare a security plan. Never cyber criminals take advantage of the things you worked hard for.

In Comodo, we offer Advanced Endpoint protection to many businesses to improve their endpoint security even more. Comodo [Advanced Endpoint Protection](https://enterprise.comodo.com/blog/what-is-endpoint-security/?af=7639) provides a lightweight, scalable Default Deny Platform with a unique endpoint security approach, which results in complete protection and enterprise visibility. The app based platform eliminates complexity and solution overlap. Provisioned in minutes, Advanced Endpoint Protection also includes unified IT and security management console, that through an app enabled platform reduces the effort of managing your Android, iOS, OSX, Linux, and Windows devices, on every segment of your physical and virtual networks.

## 2.4. Trojan horse examples

The first Trojan was probably a computer program called ANIMAL, which was written in 1974 for Univac computers by John Walker. ANIMAL was a "20 questions" program that tried to guess the user's favorite animal, using some clever machine learning to improve its questions as it went along. As [Walker explains it](http://www.fourmilab.ch/documents/univac/animal.html), enough Univac users requested copies that it was starting to occupy a lot of his time in the days before easy computer networking. So he created a subroutine called PERVADE that would, while the user was answering the questions, save copies of ANIMAL to any user-accessible directories it could find. Many of these directories were actually on reel-to-reel tapes that were shared between offices, so the Trojan spread via that vector as well. Walker insists that ANIMAL was a "very good citizen" and did no damage, merely copying itself so he could tell interested parties that the program was probably already on their machine. He also notes that the widespread story that another program, HUNTER, was written to track down and erase ANIMAL copies is an urban legend.

Modern Trojans are more malicious, of course. We've already met Emotet and Petya, two of the most wide-ranging and destructive Trojans.

Other prominent examples include:

 **Emotet banking Trojan.** After a long hiatus, Emotet’s activity increased in the last few months of 2017, according to the Symantec 2018 Internet Security Threat Report. Detections increased by 2,000 percent in that period. Emotet steals financial information, among other things.

 **Rakhni Trojan**.This malware has been around since 2013. More recently, it can deliver ransomware or a cryptojacker (allowing criminals to use your device to mine for cryptocurrency) to infected computers. “The growth in coin mining in the final months of 2017 was immense,” the 2018 Internet Security Threat Report notes. “Overall coin-mining activity increased by 34,000 percent over the course of the year.”

 **ZeuS/Zbot**.This banking Trojan is another oldie but baddie. ZeuS/Zbot source code was first released in 2011. It uses keystroke logging — recording your keystrokes as you log into your bank account, for instance — to steal your credentials and perhaps your account balance as well

**3. Conclusion**

In this paper we have researched what Trojan horse attack is and how many types of Trojan horse attacks there are, we have also conducted a detailed experiment which we will share during our presentation. During our experiment we have observed how a disguised picture can make a computer prone to a hack. In all conclusion the trojan horse attack can be very dangerous because in such an attack one may not be aware about the backdoor they have opened to hackers. So we should always download any file from a trusted source and use different kinds of security system whether it is using anti-malware software or firewall.

**Bibliography**

* [wikipedia.org/wiki/Trojan\_Horse](https://en.wikipedia.org/wiki/Trojan_Horse)
* [webroot.com/us/en/resources/tips-articles/what-is-trojan-virus](https://www.webroot.com/us/en/resources/tips-articles/what-is-trojan-virus)
* [owasp.org/www-community/attacks/Trojan\_Horse](https://owasp.org/www-community/attacks/Trojan_Horse)
* [malwarebytes.com/trojan/](https://www.malwarebytes.com/trojan/)
* 36. Whalley, I. 1998 Talking Trojan. Virus Bulletin
* Gordon, S. & Chess, D. 1998. Where There's Smoke, There's Mirrors: The Truth About Trojan Horses on the Internet. From the Proceedings of The Eighth International Virus Bulletin Conference. Munich Germany