Torjan Horse

A Trojan horse is anything that looks innocent but, once accepted, has power to harm or destroy—for example, a computer program that seems helpful but ends up corrupting or demolishing the computer's software.

They are useful for invading privacy by saving and leaking passwords of the legitimate user.

Trojan Infection Methods

user lai suruma target garne via fishing or social engineering ani aafu useful jsot pretend garne tarw tyo site haru chai kunai pani euta reknown or authorized organization ko hudenw bt exactly same hunxa ani user lai trick garerw user le donwload garxa ani system ma install vyo torjan horse files haru delete grne harm garne gardenw khasae bt passwords ani important info save garne ani leak garne garxa

Here are common ways trojans can infect computers in your corporate network:

- A user is targeted by phishing or other types of social engineering, opens an infected email attachment or clicks a link to a malicious website
- A user visits a malicious website and experiences a drive-by download pretending to be useful software, or is prompted to download a codec to play a video or audio stream
- A user visits a legitimate website infected with malicious code (for example, malvertising or cross-site scripting)
- A user downloads a program whose publisher is unknown or unauthorized by organizational security policies
- Attackers install a trojan by exploiting a software vulnerability, or through unauthorized access

“Daserf” Trojan created by the cyber-espionage group REDBALDKNIGHT is often installed through the use of decoy documents attached in emails.

Types of Trojans

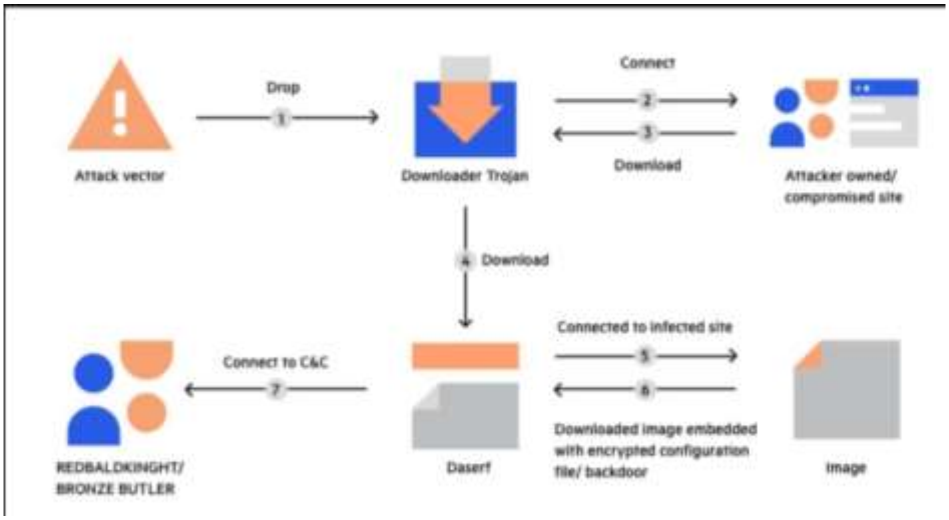
The first trojan was seen in the wild was ANIMAL, released in 1975. Since then, many millions of trojan variants have emerged, which may be classified into many types. Here are some of the most common types.

Downloader Trojan

A downloader trojan downloads and deploy other malicious code, such as rootkits, ransomware or keyloggers. Many types of ransomware distribute themselves via a “dropper”, a downloader trojan that installs on a user’s computer and deploys other malware components.

Downloader Torjan is a type of torjan horse which waits for internet connection to get connected with the site and when they are connected then they installs files (usually malicious files).
Downoader Torjan horse seems like actual downloader.

suruma euta attack vector naam ko file aako xa ani downloader torjan suruma connect download huna pryo aafu ani balla tyo drop vako file download garxa usle ani tespxi systema enter garihlyo ani kaam garxa


Attack vector
Drop
1
Downloader Trojan
Connect
2
3
Download
Attacker owned/ compromised site
4
Download
Connected to infected site
5
6
Downloaded image embedded with encrypted configuration file/ backdoor
Image
Daserf
Connect to C&C
7
REDBALDKNIGHT/ BRONZE BUTLER

bujnew vne wordfile herne

A dropper is often the first stage in a multi-phase trojan attack, followed by the installation of another type of trojan that provides attackers with a persistent foothold in an internal system. For example, a dropper can be used to inject a backdoor trojan into a sensitive server.

Backdoor Trojan

A backdoor trojan opens up a secret communication tunnel, allowing the local malware deployment to communicate with an attacker's Command & Control center. It may allow hackers to control the device, monitor or steal data, and deploy other software.

Spyware

Spyware is software that observes user activities, collecting sensitive data like account credentials or banking details. They send this data back to the attacker. Spyware is typically disguised as useful software, so it is generally considered as a type of trojan.

Rootkit Trojans

kasari kasari trick gaererw rootlevel access nae acquire garne raexa

Rootkit trojans acquire root-level or administrative access to a machine, and boots together with the operating system, or even before the operating system. This makes them very difficult to detect and remove.

DDoS Attack Trojan (Botnet)

dherae euta machine harvest garne raexa ani tyo machine haru bata fake traffic pathayerw server lai overaload garauna sakine vyo distributed denial of service hunxa

A DDoS trojan turns the victim's device into a zombie participating in a larger botnet. The attacker's objective is to harvest as many machines as possible and use them for malicious purposes without the knowledge of the device owners—typically to flood servers with fake traffic as part of a Distributed Denial of Service (DoS) attack.

Trojan Horse Malware Examples (naam matra padne)

Following are some of the fastest-spreading and most dangerous trojan families.

Zeus

Zeus/Zbot is a malware package operating in a client/server model, with deployed instances calling back home to the Zeus Command & Control (C&C) center. It is estimated to have infected over 3.6 million computers in the USA, including machines owned by NASA, Bank of America and the US Department of Transportation.

Zeus infects Windows computers, and sends confidential data from the victim's computer to the Zeus server. It is particularly effective at stealing credentials, banking details and other financial information and transmit them to the attackers.

The weak point of the Zeus system is the single C&C server, which was a primary target for law enforcement agencies. Later versions of Zeus added a domain generation algorithm (GDA), which lets Zbots connect to a list of alternative domain names if the Zeus server is not available.

Zeus has many variants, including:

- **Zeus Gameover**—a peer-to-peer version of the Zeus botnet without a centralized C&C.
- **SpyEye**—designed to steal money from online bank accounts.
- **Ice IX**—financial malware that can control content in a browser during a financial transaction, and extract credentials and private data from forms.
- **Citadel**—an open-source variant of Zeus that has been worked on and improved by a community of cybercriminals, and was succeeded by Atmos.
- **Carberp**—one of the most widely spread financial malware in Russia. Can exploit operating system vulnerabilities to gain root access to target systems.
- **Shylock**—uses a domain generation algorithm (DGA), used to receive commands from a large number of malicious servers.

ILOVEYOU

ILOVEYOU (commonly referred to as the "ILOVEYOU virus") was a trojan released in 2000, which was used in the world's most damaging cyberattack, which caused $8.7 billion in global losses.

The trojan was distributed as a phishing email, with the text "Kindly check the attached love letter coming from me", with an attachment named "ILOVEYOU" that appeared to be a text file. Recipients who were curious enough to open the attachment became infected, the trojan would overwrite files on the machine and then send itself to their entire contact list. This simple but effective propagation method caused the virus to spread to millions of computers.

Cryptolocker

Cryptolocker is a common form of ransomware. It distributes itself using infected email attachments; a common message contains an infected password-protected ZIP file, with the password contained in the message. When the user opens the ZIP using the password and clicks the attached PDF, the trojan is activated. It searches for files to encrypt on local drives and mapped network drives, and encrypts the files using asymmetric encryption with 1024 or 2048-bit keys. The attackers then demand a ransom to release the files.

Stuxnet

Stuxnet was a specialized Windows Trojan designed to attack Industrial Control Systems (ICS). It was allegedly used to attack Iran’s nuclear facilities. The virus caused operator monitors to show business as usual, while it changed the speed of Iranian centrifuges, causing them to spin too long and too quickly, and destroying the equipment.