Trojans and Backdoors

By Gaurav Dalvi
3rd Year CSE
Reg no:-2011BCS501

Malware Family.

- Trojans.
- Viruses.
- Worms.
- Rootkits.

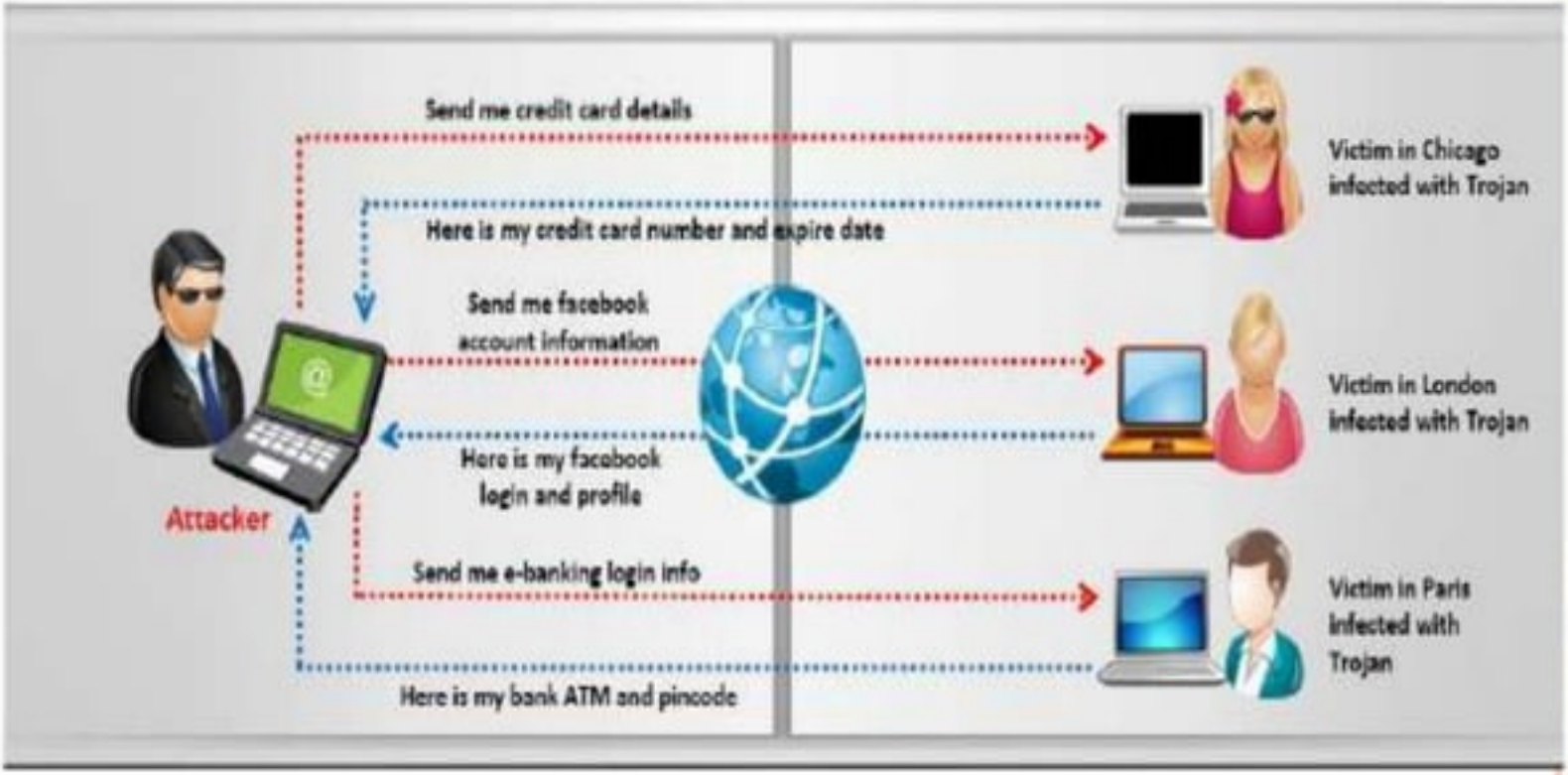
Birth of Trojan

- the story of old Greek.(Greek vs. Troy).

- The Application works same as the story and is the most powerful application used for attacking computers.
- A new game, an electronic mail or a free software from unknown person can implant Trojan or a backdoor.
- The first Trojan computer infection is believed to have appeared in 1986 as a shareware program called “PC-Write”.

WHAT IS TROJAN?

- malicious payload inside a legitimate program.



Types of Trojans

- Destructive Trojan.
- Denial Of Service Trojan.
- Remote Access Trojan.
- Data sending Trojan.
- Proxy Trojan.
- FTP Trojan.
- Security Software Disabler Trojan.

How Systems get infected by Trojan?

- Visiting untrusted websites.
- Email Attachments.
- Pirated Software.

How to Infect Systems Using a Trojan?

III Create a wrapper using tools to install Trojan on the victim's computer

IV Propagate the Trojan

V Execute the dropper

VI Execute the damage routine

Evading Anti-Virus Techniques

Break the Trojan file into multiple pieces and zip them as single file

Never use Trojans downloaded from the web (anti-virus can detect these easily)

ALWAYS write your own Trojan and embed it into an application

Change the content of the Trojan using hex editor and also change the checksum and encrypt the file

Change Trojan's syntax:

- Convert an EXE to VB script
- Convert an EXE to a DOC file
- Convert an EXE to a PPT file
- Convert an EXE to a PDF file

Trojan Detection

Manual

- Run key of regedit

Computer\HKey_local_machine\Software\Microsoft\Windows\Currentversion\Run put in it to run malicious software .

- May appear as Malicious drivers

C:\windows\System32\Drivers*.sys

With the help of tools

- process explorer
- Icesword(port monitoring) .
- Driverview.
- Srvman.
- Sigverif.
- TrojanHunter.

Overt and Covert Channels

Overt Channel

A legitimate communication path within a computer system, or network, for transfer of data

Example of overt channel includes games or any legitimate programs

Poker.exe
(Legitimate Application)

Covert Channel

A channel that transfers information within a computer system, or network, in a way that violates the security policy

The simplest form of covert channel is a Trojan

Trojan.exe
(Keylogger Steals Passwords)

Backdoor Concept

- A Backdoor allows a malicious attacker to maintain privileged access to a compromised host
- Unix back doors are typically installed via a Worm ,Root Kit or manually after a system has been initially compromised.
- Windows back doors are typically installed via a Virus, Worm or Trojan Horse.

Backdoor Installation.

- Through Trojan.
- Through ActiveX (embedded in website).
- Protection offered by Microsoft.

Hiding Mechanisms.

- Cryptography.
- Rootkits.
- Use different protocols and port numbers.
- Reverse control.
- Backdoor timing.

ROOTKITS

- Classical rootkits

1. Usually attacker replace the /bin/login file with the another version.
2. He can also save the password of other users.
3. Sometimes Classical Rootkit hide many things.

- Kernel rootkits

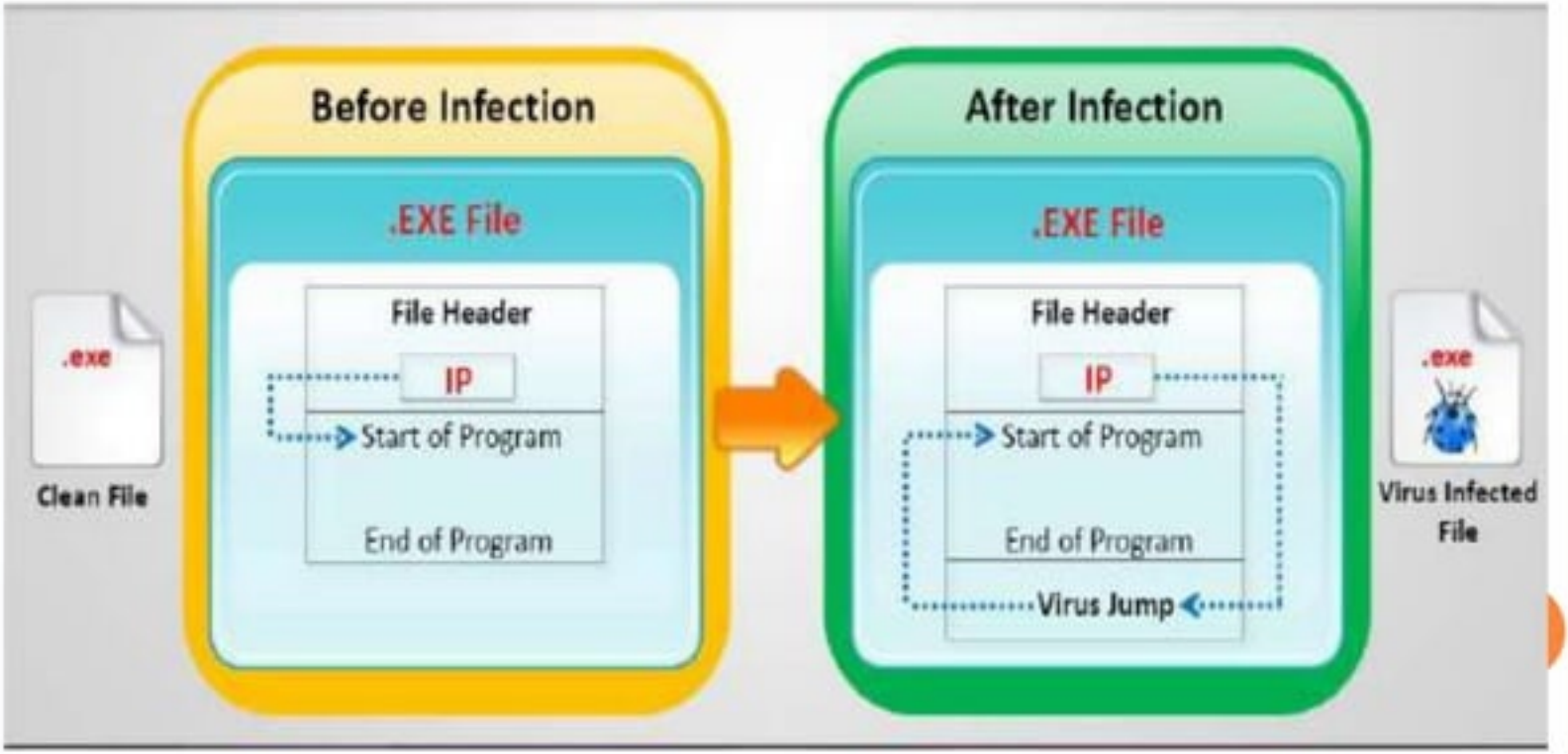
1. Most powerful rootkit.
2. It replaces the kernel of OS.
3. It can also off monitoring, antivirus.
4. It is very hard to detect.

VIRUSES

- A virus is a self-replicating program that produces its own code by attaching copies of itself into other executable codes
- Some viruses affect computers as soon as their code is executed; other viruses lie dormant until a pre-determined logical circumstance is met

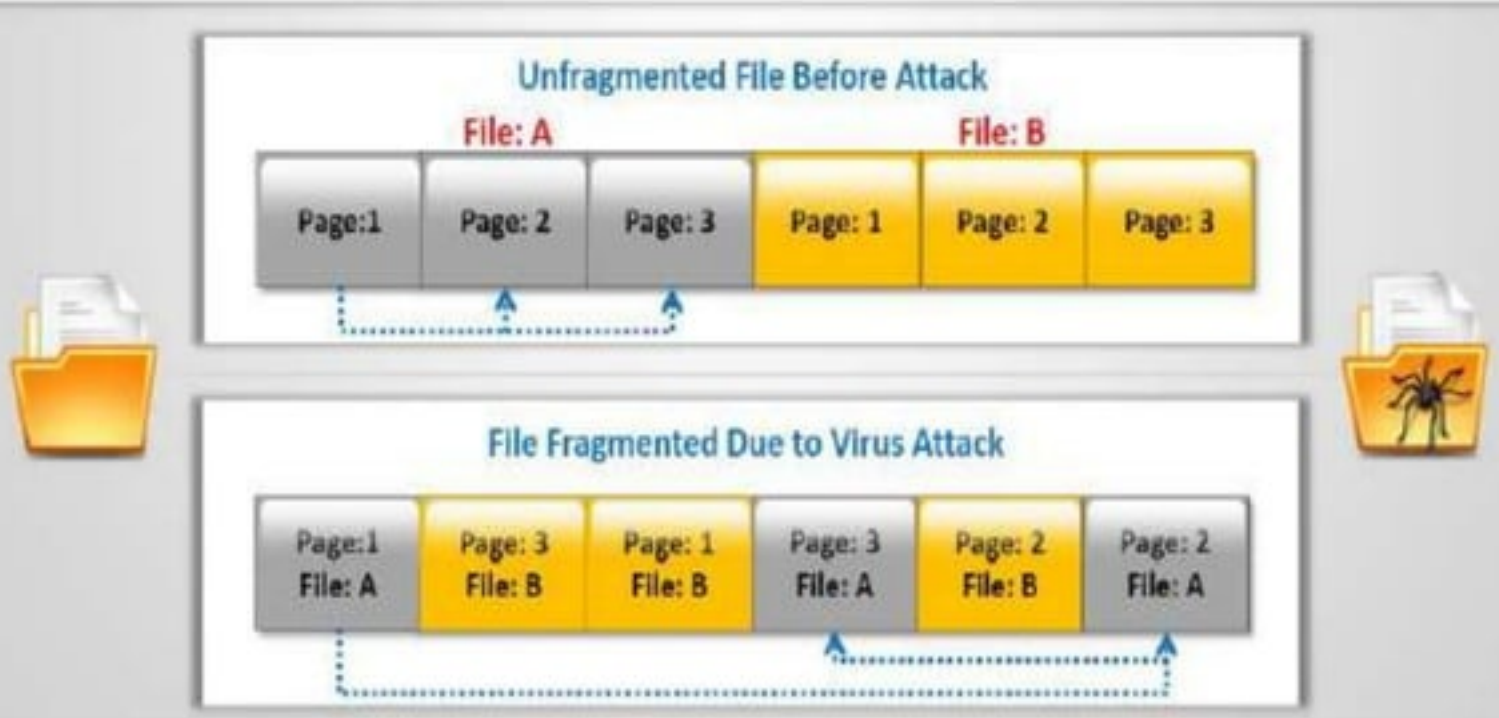
Working of Viruses: Infection Phase

- In the infection phase, the virus replicates itself and attaches to an .exe file in the system
- Some viruses infect each time they are run and executed completely and others infect only when users' trigger them, which can include a day, time, or a particular event



Working of Viruses: Attack Phase

- Some viruses have trigger events to activate and corrupt systems
- Some viruses have bugs that replicate and perform activities such as file deletion and increase the session's time
- They corrupt the targets only after spreading completely as intended by their developers



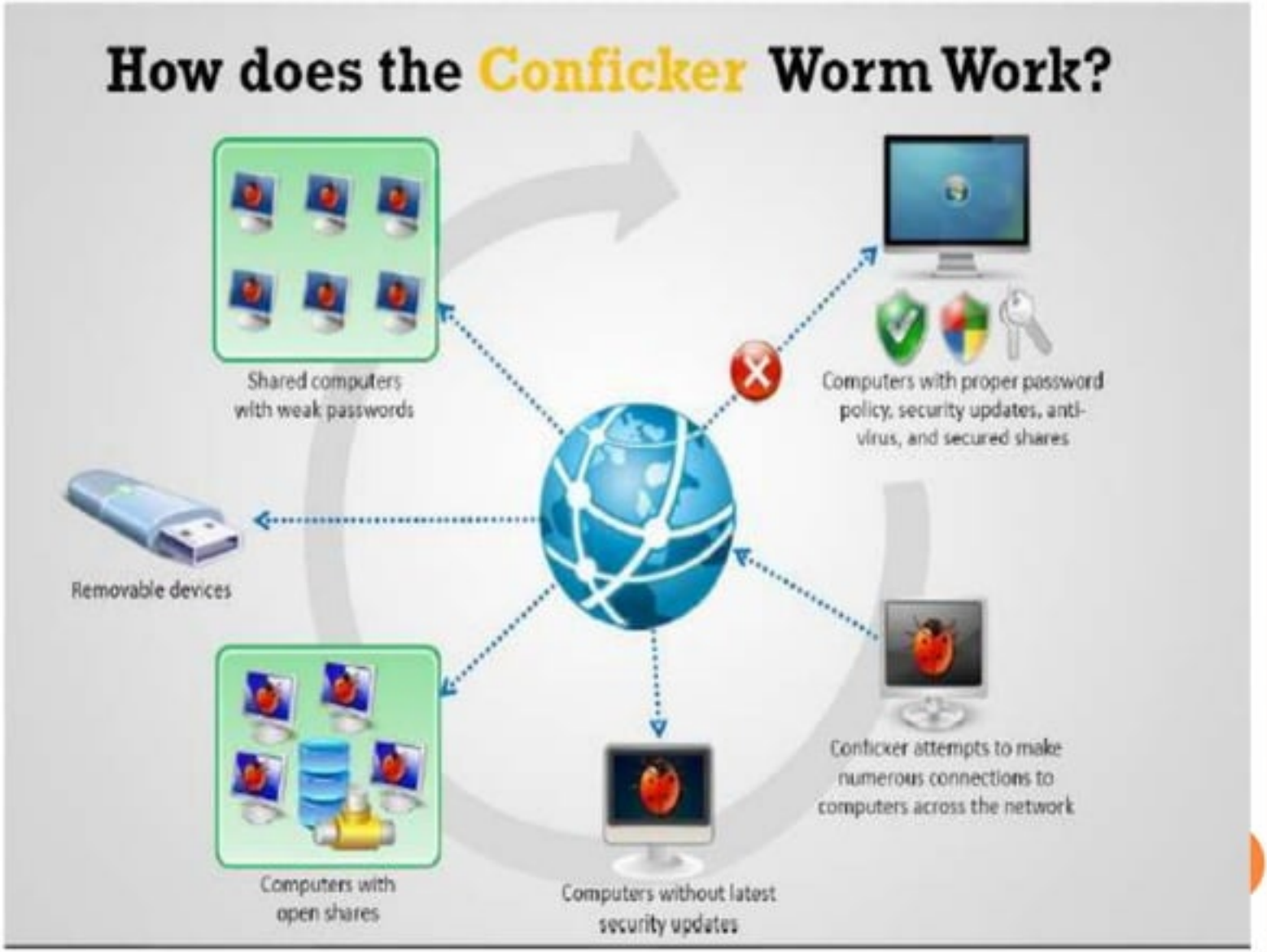
WORMS

Computer Worms

Computer worms are malicious programs that **replicate**, **execute**, and **spread** across the network connections independently without human interaction

Most of the worms are created only to replicate and spread across a network, consuming available **computing resources**; however, some worms carry a payload to damage the host system

Attackers use worm payload to install backdoors in infected computers, which turns them into zombies and **creates botnet**; these botnets can be used to carry further cyber attacks


How does the Conficker Worm Work?
Shared computers with weak passwords
Computers with proper password policy, security updates, anti-virus, and secured shares
Removable devices
Conficker attempts to make numerous connections to computers across the network
Computers with open shares
Computers without latest security updates

How is a Worm Different from a Virus?

A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs

A worm takes advantage of file or information transport features on computer systems and spreads through the infected network automatically but a virus does not

SPREADING MALWARE .

- Fake programs (pop up/rogue security).
- Internet downloads .
- Internet Messenger.
- Email attachments, Links.
- Browser + email software Bugs.
- May contain frame which contain malicious code.
- Physical Access through keyloggers ,spywares.

Protection from malware

- New Updates.
- Personal Firewall.
- Use non-admin account.
- Use User Access Control.

CASE STUDY.

- Back Orifice 2000.(Bo2k)
- Oldest and most powerful backdoor used for training issues in windows machine.
- It is Open source and is free available on Sorce forge website.

Back Orifice 2000

- It was written by Deldog one of the member of the 'Cult of the dead cow' group.
- It was introduce in the DefCon Conference in 1999.
- It was made for good use for monitoring activity but many people make the malicious use of it.

Abilities of BO2K

- BO2K is very small but very complete in abilities.
- Its client code is just 100KB can be easily implanted on the victims computer.
- It can use different kinds of Hiding technique.
- In recent version it has the reverse client connection.
- As it is open source you can customize according to your need.

Making a Trojan use BO2K

- You can use binder application to bind the B02K client code with other program.
- Elite wrap , Saran Wrap, Silk Rope which are mostly use to wrap BO2K.

References

- www.securitytube.net
- CEHv7 courseware.
- www.hackernews.com
- www.insecure.com
- www.securityforge.com
- Defcon Conference.

Quotes

"I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive. We've created life in our own image."

- **Stephen Hawking,**
Theoretical Physicist
and Cosmologist