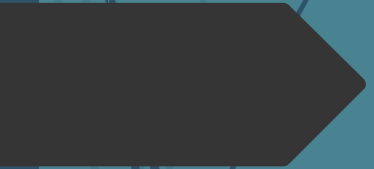


INTRODUCTION TO TROJANS





VIRUS & WORMS

Virus is a piece of code which is meant for the malicious purpose. It can replicate itself in the same system or also to the external hard drive. It may harm your system by deleting vital information from your hard drive or by corrupting the operating system files.

Worms are the malwares that replicate itself by resending itself as an e-mail attachment or as part of a network message. Worms do not alter files but reside in active memory and duplicate itself. Worms use parts of an operating system that are automatic and usually invisible to the user.

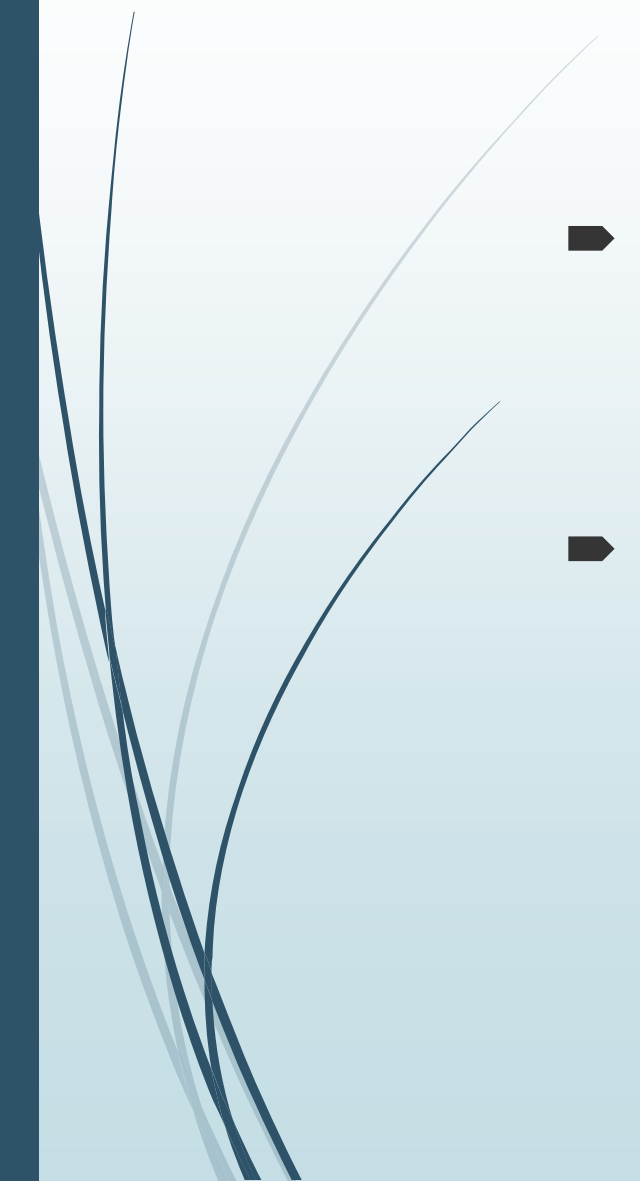


TROJANS

Trojans are piece of code which is meant for the remote administration purpose. It may or may not harm your computer but the hacker can administrate your computer remotely. A hacker may see the webcam, can get the logs of all the key strokes and can also delete any file & folders from your system. Trojans are one of the most dangerous and widely used by hackers to get into the systems



TYPES OF TROJANS

- Direct Connection Trojan
 - Reverse Connection Trojan
- 

DIRECT CONNECTION TROJAN

In the direct connection Trojan, Victim's IP Address plays essential role. Hacker sends Trojan to victim, victim unknowingly executes it. To get the remote connection of victim's computer, hacker needs to have IP Address of victim. Hacker uses different methods to get the IP address of victims such as,

- Email Tracing
- IP Grabbing
- Social Engineering



REVERSE CONNECTION TROJAN

Hacker creates the Trojan with his own IP address. In this case, when a victim executes the Trojan, hacker gets the connection. Hacker needs to open one port to get the connection.





RAT (REMOTE ADMINISTRATION TOOL)

RAT IS, Remote Admistration Tool used to create the Trojans. One can use their own coding to create the Trojans also but RAT may help you to create it easily.

- It is also used to control the victim's computer. After creating and sending the Trojan, hacker needs to open a port on his own system, for this a hacker can use RAT.
- RAT is created by the hackers to help the hackers,
- Also after getting the connection hacker can perform various tasks such as accessing the webcam, file & folder operations, edit the registry and even can edit the command prompt of the victim using RAT.



RAT (REMOTE ADMINISTRATION TOOL)

RATs are available for both the types of Trojans. There are numerous RATs available over the internet such as,

- Cyber Gate
- Dark Comet
- Pro Rat
- Poison Ivy
- Net Bus

Etc, etc, etc, ...



RATs can perform:

- Keystroke Logging
- Packet Capture
- Screen Capture
- Camera Capture
- File Access
- Code Execution
- Registry Management
- Password Sniffing

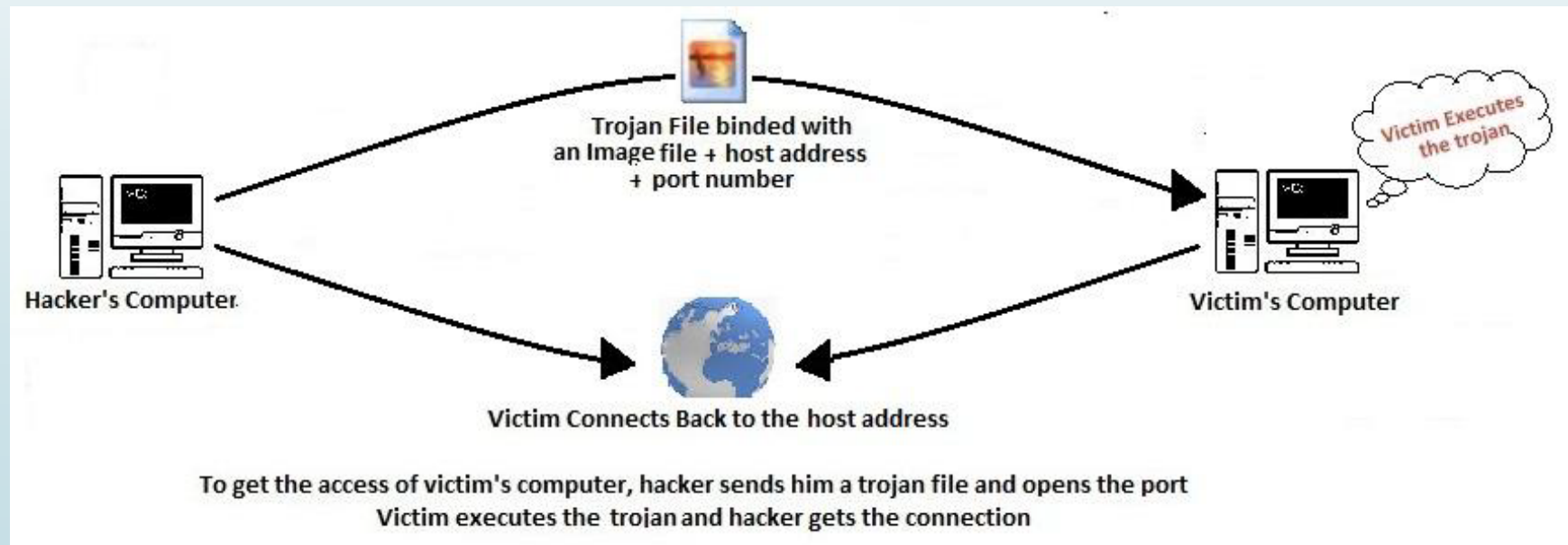


PROBLEMS & SOLUTIONS

- An Antivirus may detect the Trojan
- And also what if hacker's IP address is not static. After restarting he will lose his IP address and also the connection of the victim.

SOLUTION of STATIC IP

Website's IP are static but our IP address may not be static. So, a hacker can make the Trojan to connect to a particular host and then connect the system to the host to get the reverse connection.





SOLUTION of ANTI-VIRUSES

All the anti-virus applications detect any trojan or any virus from its signature. If we modify the signatures of the trojan or the viruses, we can prevent our trojan file from being detected by the anti-viruses

- To change the signatures of the trojan a hacker can use applications called **Crypters** or can also do it manually.
- There are lots of crypters available, and it's a very simple process to crypt file using Crypters.
- To check how many anti-virus detect it as a trojan, scan it online at <http://www.virustotal.com>



HOW TO SECURE YOURSELF??

- Check Opened ports
- Check the process of the system
- Run any unidentified file in Sandboxie
- Always install licensed anti-virus which updates it's virus signatures regularly



INTRODUCTION TO SOCIAL ENGINEERING

“Cause there’s no PATCH for HUMAN
STUPIDITY”



What is SOCIAL ENGINEERING??

In context of Information Security, it is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

HACKER?



TECHNIQUE

- Human Interaction
- Respectable & Known Person or Entity
- Assembling all gathered information together



TYPES OF SOCIAL ENGINEERING

- Quid Pro Quo – Something for something
- Phishing
- Baiting
- Pretexting
- Diversion Theft

Phishing Email



Dear Gmail User,

As part of our security measures, we regularly update all accounts on our database system. We are unable to update your email account and therefore we will be closing your email accounts to enable the web upgrade.

You have been sent this invitation because our records indicate you are currently a user whose account has not been activated. We are therefore you sending this email so you can inform us whether you still want to use this account. If you are still interested please confirm your account by updating your details immediately because out system requires an account verification for the update.

To prevent an interruption with your Gmail services, please take a few moments to update your account by filling out the verification and update form immediately.

[Click here to verify your account](#)

Warning! Any account owner that refuses to update their account after receiving this email will lose their account permanently.

We appreciate your cooperation in this matter.

Sincerely
Gmail Member Services Team



WEAKEST LINK??

No matter how strong your:

- Firewalls
 - IDS & IPS
 - Cryptography
 - Anti-Virus Software
-
- You are the weakest link in computer security. People are more vulnerable than computers.
 - “The weakest link in the security chain is the human element: - Kevin Mitnick



WAYS TO PREVENT SOCIAL ENGINEERING

- User Awareness
- Policies
- Third party Test
- Be Smart

Tips for avoiding a Social Engineering Attack

✓ **LIMIT PUBLIC INFORMATION:**

Limit the amount of personal information that you share online.

✓ **BE SKEPTICAL:**

Always question requests for sensitive information.

✓ **TRUST BUT VERIFY:**

Don't share information with people you don't know unless you can verify their identity.

✓ **CALL THEM BACK:**

Through the main switchboard if possible.

✓ **NO PASSWORDS OVER THE PHONE:**

Never share your password with anyone over the phone.





Students prone to Cyber Crime

REASONS:

- Prank
- Jealousy
- Revenge
- Ignorance
- Ex-relationships
- Curiosity
- Blackmailing
- Pornography

**WATCH THIS HACKER
BREAK INTO
MY CELL PHONE ACCOUNT
IN 2 MINUTES**

RANSOMWARE



Mobile Security



Indian Browser

Version 0.3 may request access to



Contacts

- find accounts on the device



Location

- access approximate location (network-based)
- access precise location (GPS)



Phone

- read phone status and identity



Storage

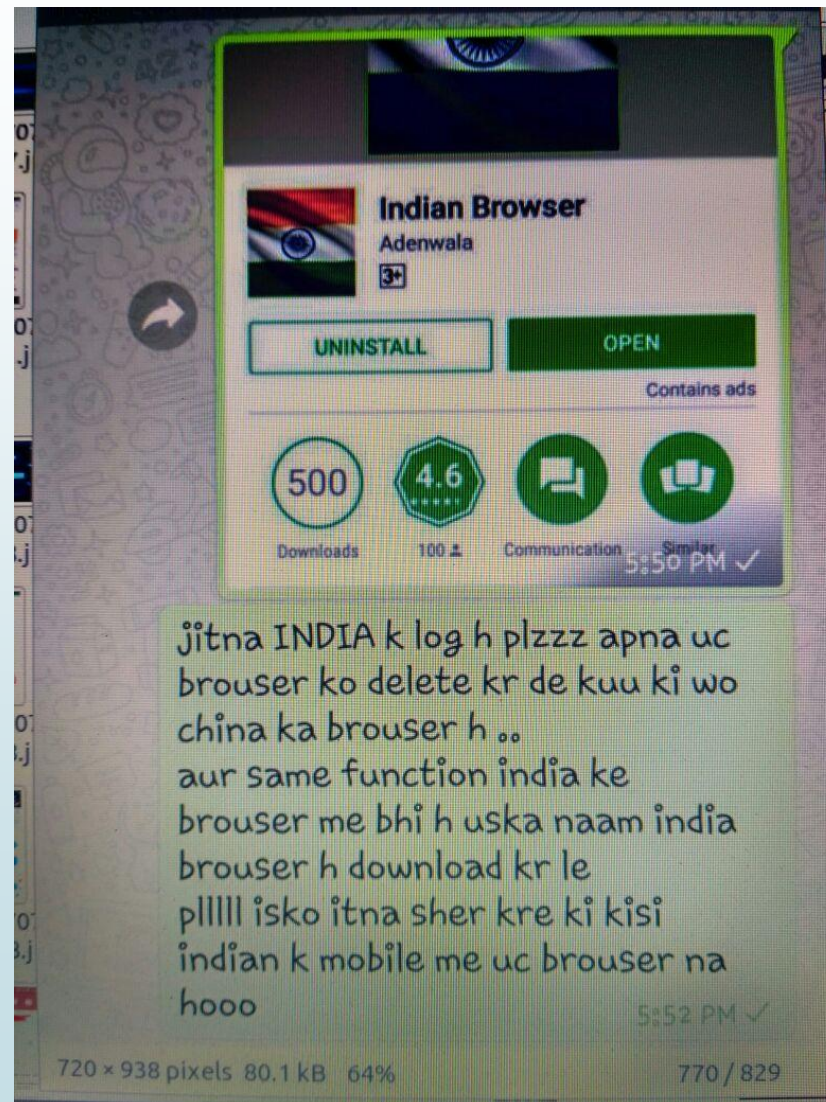
- write/delete internal storage
- read the contents of your internal storage



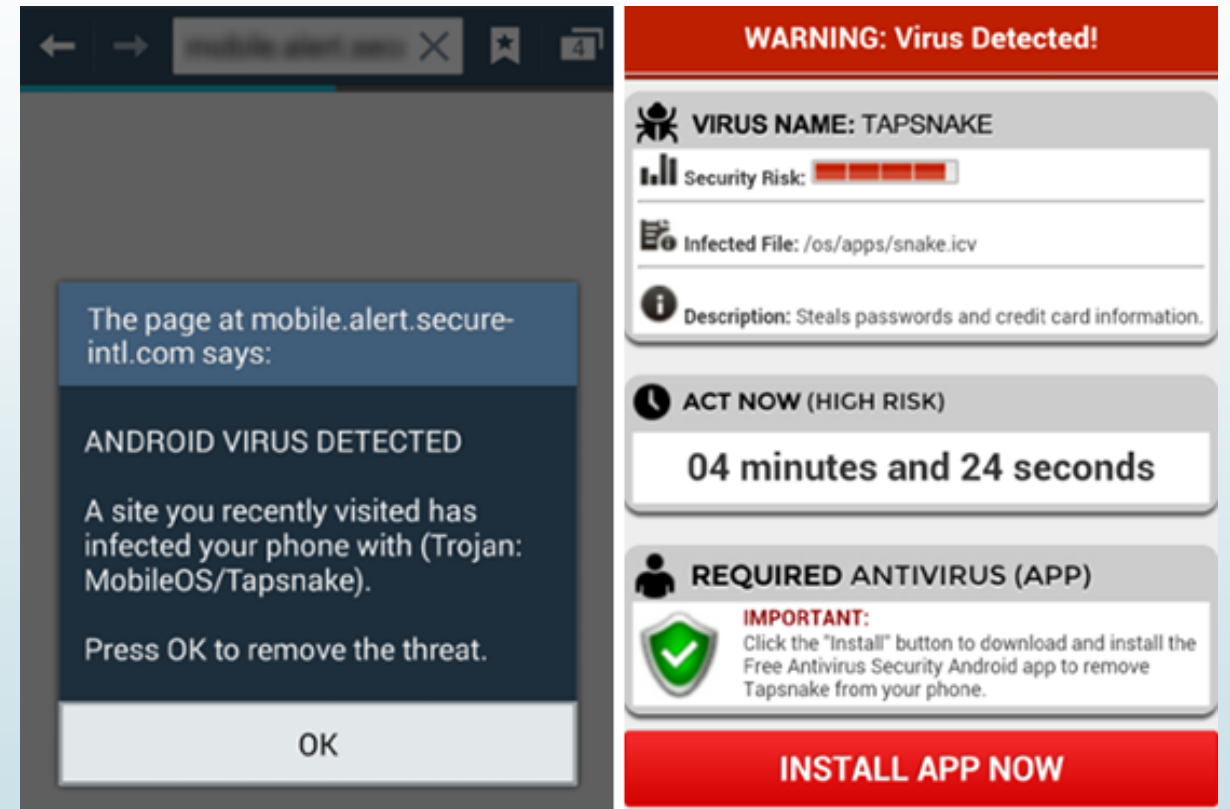
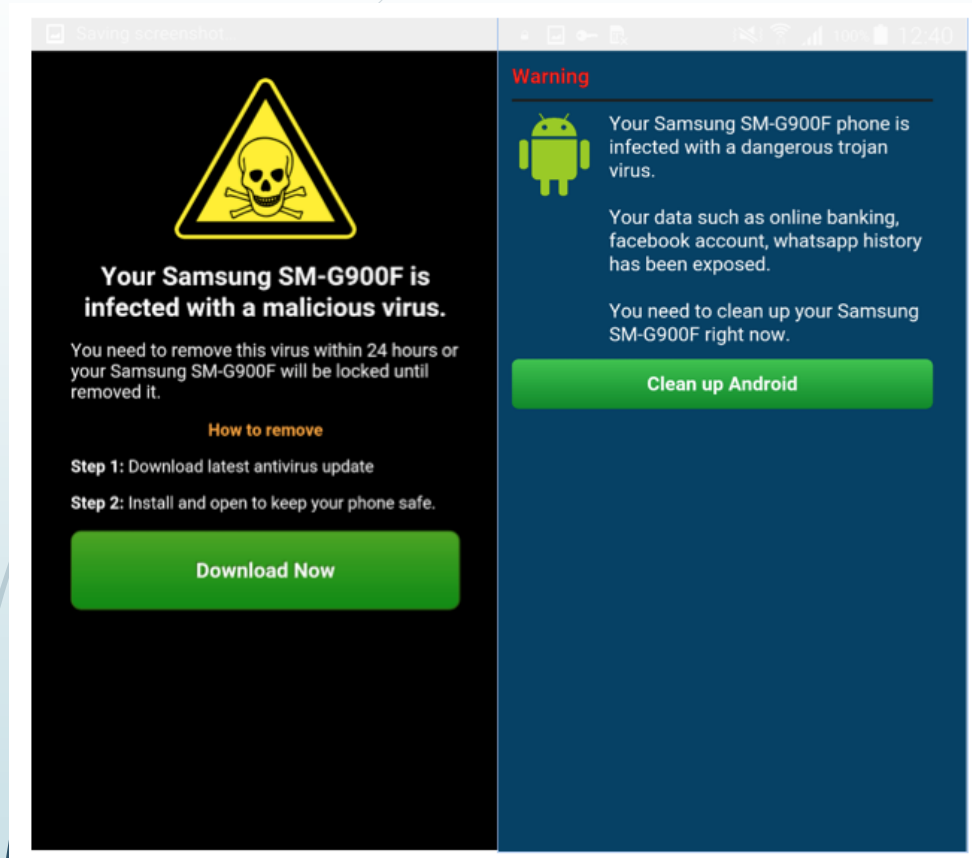
Other

- draw over other apps
- set wallpaper
- have full network access
- prevent phone from sleeping
- pair with Bluetooth devices
- run at startup
- install shortcuts
- receive data from Internet
- enable Bluetooth
- view network connections
- view Wi-Fi connections

You can disable access for these permissions in Settings. Updates to Indian Browser may automatically add additional capabilities within each group. [Learn more](#)



Scarewares









Security Awareness – Social Media

- Social Media (FB, twitter, etc) is now an integral part of our daily life
- Be sensitive in what you upload on your social networking account (status, pics, etc)
- Use security and privacy options provided by social media sites
- SMS based second factor authentication
- Access control (who can see what)
- Browser /machine mapping to your social media profile
- Block
- Keep your personal details, personal.
- Always use different passwords for different accounts



Security Awareness – Smart mobile devices

- DO NOT jail break or root your smart phones
- Connect to ONLY authorized wifi access
- Use auto lock features
- Download apps from authorized app stores ONLY
- Use Privacy options provided by various mobile Operating system
- Do NOT accept calls from weird numbers (VOIP)
- Don't react to Scarewares