Cyber Security EDUCATION AND TRAINING SEMINAR

TOPIC :
VIRUS INTERPRETATION AND MANAGEMENT

B. Geeplay Williams

DIP,"A A", B.Sc., M.Sc. in Computing-IS/cyber forensics Security

INTRODUCTION

The hour plus awareness training is to provide general knowledge on the issue of cyber security with focus on virus interpretation and Management. Virus is a malware generally, malware is a malicious software that damage or disable computer system and give limited or full control of the system to the malware creator for the purpose of theft or fraud

Virus is one of the malwares used by hacker to enter system and organizations. Phasing and spoofing are Some of the social engineering techniques used. A successful defense is having good policies and their diligent implementation. This training will increase the knowledge of defense skills on virus prevention and mitigation in the context of cyber security. Presenter will be more practical speaking and participatory.

OBJECTIVES

The session seeks to Provide the following:

- ❑ Introduction to Malware and malware Propagation Techniques
- ❑ Understanding the Malware analysis Process
- ❑ Understanding different Techniques to Detect Malware
- ❑ Introduction to Virus, type of viruses what and how they infect systems
- ❑ How Spoofing and Phishing as social engineering Malware tools use to attack devices/system
- ❑ Malware/ Virus Countermeasure
- ❑ Anti-Virus Tools

WHAT IS MALWARE

Malware is a malicious software that damage or disables computer system and gives limited or full control of the systems to the system to the malware creator for the purpose of theft or fraud

- *Advertising*
- *Trojan Horse*
- *Backdoor*
- *Rootkit*
- *Ransomware*
- ***Virus***
- *Worm*
- *Spyware*
- *Botnet*
- *Adware*
- *Crypter*

Different Ways a Malware can Get Into a system

- Instant Messenger application
- IRC9 (Internet Relay Chat)
- Removable devices
- Attachments, Browser and email software bugs
- NetBIOS (File sharing)
- Fafe Prog
- Untrusted sites and Freeware software rams)
- Downloading filing, games and screensaver from internet sites etc

COMMON TECHNIQUES ATTACHERS USE TO DISTRIBUTE MALWARE ON THE WEB

- ❑ Black chat search

Ranking malware pages highly in search Results

- ❑ Advertising

embedding malware in ad- network that display across hundreds of legitimate, high traffic sites

- ❑ Social Engineered click-jacking

Tricking users into clicking on innocent looking webpages

- ❑ Spear phishing sites

Mimicking legitimate institution to steal in an attempt to steal login credential

INTRODUCTION TO VIRUS

- A virus is a self-replication program that produce its own copy by attaching itself to another program, computer boot sector or document
- Viruses are generally transmitted through the file download, infected disk/flash drives and as email attachments

WHAT IS COMPUTER VIRUS

- A virus is a self-replication program that produces its own copy by attaching itself to another program, computer boot sector or document

- Viruses are generally transmitted through file download, infected dis/flash drives and as email attachment

  - ***VIRUS CHARACTERISTICS***
    - *Infects other program*
    - *Alter data*
    - *Transforms itself*
    - *Corrupts files and Program*
    - *Self- replication*
    - *Encrypts itself*

INDICATION OF VIRUS ATTACK

- Processes take more resources and time
- Computer slows down when program start
- Computer beeps with no display
- Unable to load operating system
- Files and folders are missing
- Browser window freezes
- Computer freezes or encounter error

Abnormal Activities

If the system acts in an unprecedented manner, you can suspect a virus attached

False Positives

However, not all glitches can be attributed to virus attacks

HOW DOES A COMPUTER GET INFECTED BY VIRUSES

- When a user accept files and downloads without checking
- Operating infected e-mail attachments
- Installing pirated software
- Not upgrading and not installing new versions of plug-ins

THE TYPE OF VIRUSES

What Do they infect?

- System or Boot Sector
- Files Viruses
- Multipartite
- Macro Virus
- Cluster Viruses

How Do they infect?

- Tunneling Virus
- Sparse infector virus
- Add-on virus
- Polymorphic Virus
- Intrusive Virus

EXAMPLE ON WHAT DO THEY INFECT

– System or boot sector viruses- this virus move MBR to another location on the hard drive and copies itself to the original location of MBR

How it work

Before infection

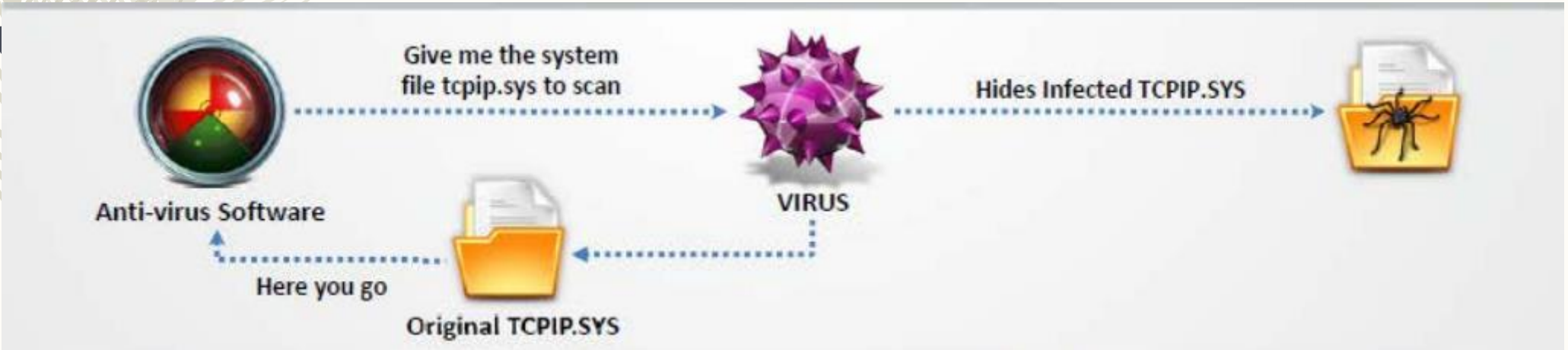
After infection

EXAMPLE ON WHAT DO THEY INFECT

- File and Multipartite Viruses- This virus infect files which are executed or interpreted in the system such as COM, EXE SYS, OVL, OBJ, PRG, MNU AND RAT FILES, This virus can either be direct action (non-resident) or memory resident

EXANPLE –ON HOW DO THEY INFECT

- **Tunneling Viruses** – These viruses evade the anti-virus software by intercepting its requests to the operating system
- A virus can hide itself by intercepting the anti-virus software request to read the file and passing the request to the virus, instead of the OS
- The virus can then return an unaffected version of the file to the anti virus software, so



WHAT IS RANSOMEWARE

- Ransomware is a type of a malware which restricts access to the computer system files and folders and demanding an online ransom payment to malware creator(s) in order to remove the restrictions

PHISHING

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

What is it?

Cybercriminals pretend to be a trustworthy source in order to acquire sensitive personal information such as usernames, passwords, social security numbers, and credit card details.

What does it look like?

An email, phone call or text message from a seemingly legitimate email address or number instructs you to click on a link to take action (e.g., “validate your account,” “confirm your identity,” “access your tax refund”). The link brings you to a website requiring you to enter your personal information.

PHISHING- CONT…

How does it happen?

Because the cybercriminal masquerades as a legitimate source (e.g., financial institution employee, client, realtor, banker), you believe the request is from a trusted source and you unwittingly oblige when they ask you for your personal information.

What's the impact?

Victims of phishing may have malware installed on their computer systems or have their identity stolen.

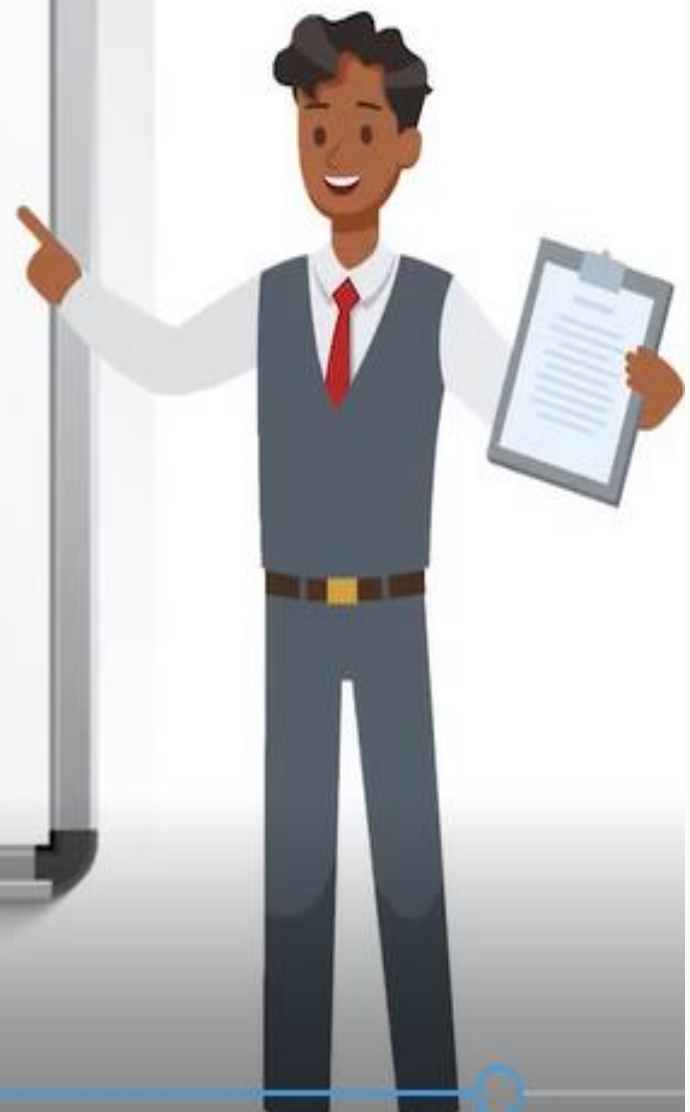
How can you defend against it?

- Hover over questionable links to reveal the true destination before clicking.
- Beware of cloned websites that may appear to be legitimate. Note that secure websites start with **https**, not http.

Case Study on Phishing

- **Dear UL Email Users;**
- Beginning next week, we will be deleting all inactive email account in order to create space for more user. You have required to send the following information to continue using your email account. if we do not receive this information from you by the end of this week, you email account will be closed:
- **Name(First and Last):**
- **Email login**
- **Password**
- **Date of birth**
- **Alternative email**
- Please contact the IT manager on this email. harrison@gmail.com
- Thanks for your immediate attention

- This email is a classic example of ***"phishing"*** – trying to trick you into ***"biting".*** The justification is the generalised way of addressing the receiver which is used in mass spam mails.
- Above that a corporate company will never ask personal details on mail
- They want your information. Don't respond to email, instant messages (IM), texts, phone calls, etc., asking you for your password or other private information.
- You should never disclose your password to anyone, even if they say they work for UCSC, ITS, or other campus organizations.



WHAT IS SPOOFING?

Spoofing is a cyberattack that occurs when a scammer is disguised as a trusted source to gain access to important data or information. Spoofing can happen through websites, emails, phone calls, texts, IP addresses and servers

What is it?

Masking the source of a communication (phone or email) to look like a reputable source (e.g. government, call within a company, etc.).

What does it look like?

We receive an email from a cybercriminal who impersonates one of our clients and confirms a fraudulent wire transfer request.

WHAT IS SPOOFING?

How does it happen?

There are easy tools available to cybercriminals that help to mask the source/sender. For example, the cybercriminal can create an email address nearly identical to our client's email address (i.e., off by a character), so that, at-a-glance, the email address appears legitimate.

The cybercriminal is relying on our lack of attention to detail in order to commit the fraud.

What's the impact?

Similar to the other cyberattacks we've discussed, our client's money is stolen, and they become the victim of fraud and/or identity theft.

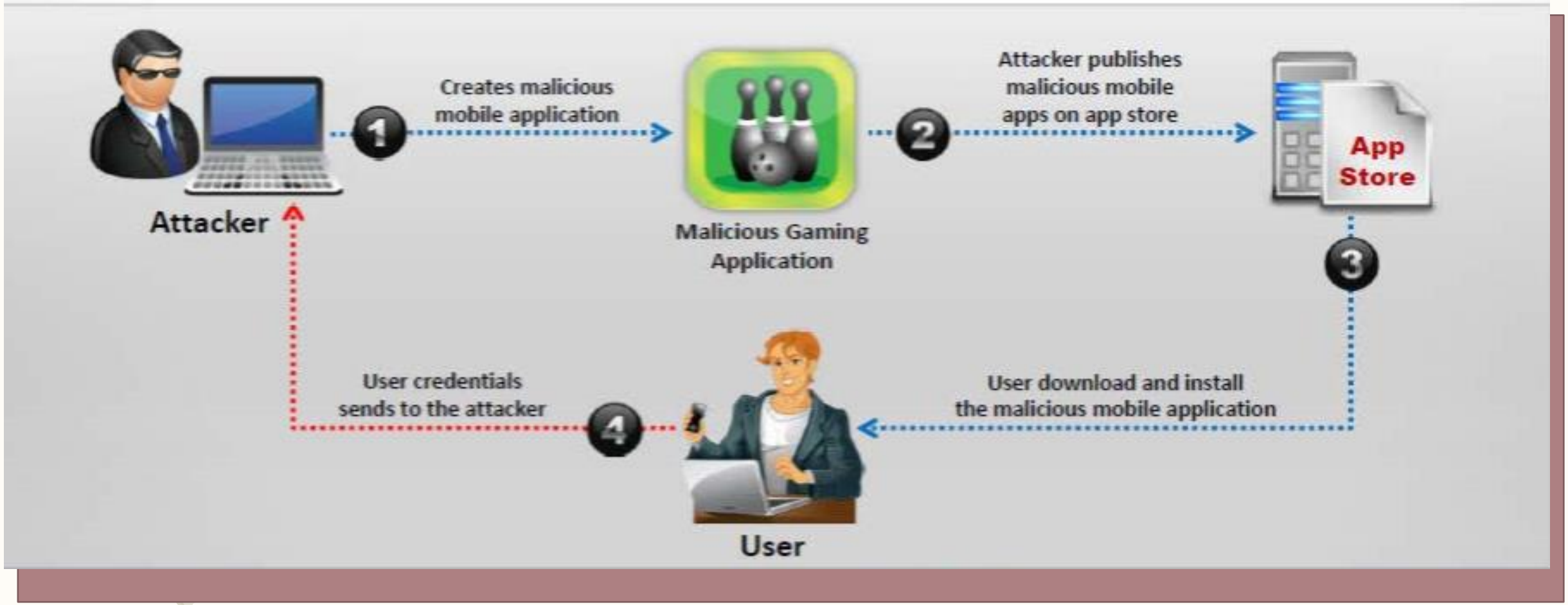
How can you defend against it?

- Carefully check the incoming emails for the proper email address and the accuracy of the spelling of the sender's name. Hover over the sender's name to see the underlying email address matches what you have on file for our client.

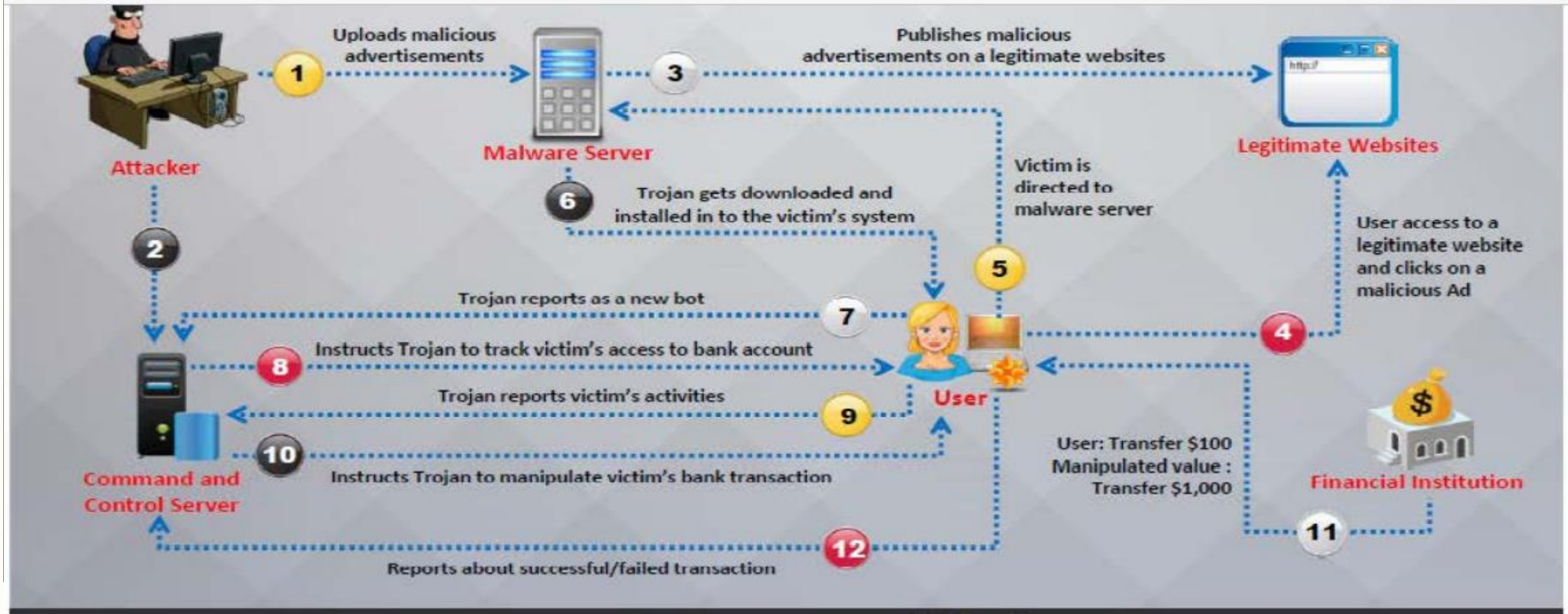
- If an email or phone call are questionable, contact the sender directly, using the email address or phone number you have on file for that individual.

- Delete the email. Better yet, use the web client (e.g. gmail, yahoo mail, etc.) and report it as spam or phishing, then delete it.
- Any unsolicited email or phone call asking you to enter your account information, disclose your password, financial account information, social security number, or other personal or private information is suspicious – even if it appears to be from a company you are familiar with. Always contact the sender using a method you know is legitimate to verify that the message is from them.

Mobile-based Social Engineering Publishing Malicious Apps



USING MALWARE TO STEAL FROM E-BANKING PLATFORM



The Cash-Out and Jackpot Attack on ATM Machines

- One of the most common types of cybercrime hacks on ATM machines is known as a cash-out or jackpot attack.
- Hackers install malware in the ATM machine through the server it is networked to, which then enables them to direct the ATM machine to dispense its entire stock of cash.
- Just as ATM machines have progressed in terms of technology and quality, so has ATM machine malware.
- ATM machine malware has become more sophisticated, making it even more difficult for the average person using the ATM machine to detect it.
- The hacker using a few key skills proceeds to empty the ATM machine and delete the malware to erase any evidence linking the theft to them.

ATM Scams

- Your ATM card is one of the quickest ways a thief can commit identity theft - and wipe out your bank account! Here are some of the most common types of ATM scams:
- 1. **Skimmer**- This scam involves a device that is installed into an ATM that can read your account information including your account number, PIN and balance. Usually these skimmers can hold up to 200 accounts worth of information at a time.
- 2. **Shoulder Surfing**- This low-tech scam involves observation techniques or some crafty tactics. Some thieves install a fake keypad on top of a real one to record account information and pin numbers.
- 3. **Cash Trapping**- A crook installs something to block the cash from dispensing out of an ATM machine. A customer will then go inside the bank for help and will return to find the cash stolen by a thief.
- 4. **"Lebanese Loop"**This type of financial identity theft is one of the simplest and becoming increasingly common. An identity thief installs a metal or plastic strip into the ATM card slot.

VIRUS DETECTION METHODS

- Scanning
  - Once a virus has been detected, its is possible to write scanning program that look for signature string characteristics of the virus
- Integrity Checking
  - Integrity checking products work by reading the entire disk and recording integrity data acts as a signature for the files and system sectors
- Interception
  - The interceptor monitors the operating system requests that are written to the disk

VIRUS- COUNTERMEASURES

1. Install anti- virus software that detects and removes infections as they appear
2. Generate an anti-virus policy for staff c computing and distribute it to the staff
3. Pay attention to the instructions while downloading files or any program from the internet
4. Update the anti-virus software regularly
5. Avoid operating the attachment received from unknown sender as virus spread via e-mail attachments
6. Do not accept disk or programs without checking them first a correct version of an anti virus program
7. Schedule regular scans for al drives after the installation of anti-virus software
8. Ensure the executable code sent to the organization is approved
9. Donot boot the machine with infected bootable system disk
10. Turn on the firewall and run anti-spyware or adware once in a week

ANTI-VIRUS TOOLS

- AVG Antivirus
- BitDefender
- Trend Micro Titanium
- Total defense internet
- F-secure Anti-Virus


Thank You

References

- Visit www.identitytheft.gov to report identity theft and to get a recovery plan
- Go to FTC.gov for additional consumer resources and to report identity theft
- http://www.ic3.gov/default.aspx is another website where you can file cybercrime complaints
- **Visit Schwab's Cybersecurity Resource Center**
- **www.CEH.org**
- **www. Obafemi awolowo university cyber security lab**

References

- Go to StaySafeOnline.org and review the STOP. THINK. CONNECT.™ cybersecurity educational campaign
- Visit OnGuardOnline.gov, also a part of the STOP.THINK. CONNECT.™ campaign, that focuses on online security for kids and includes a blog on current cyber trends
- Visit https://www.fbi.gov/scams-safety/fraud to learn more about common fraud schemes