CYBER SECURITY THREATS

INTRODUCTION TO THE MAIN CYBER SECURITY THREATS

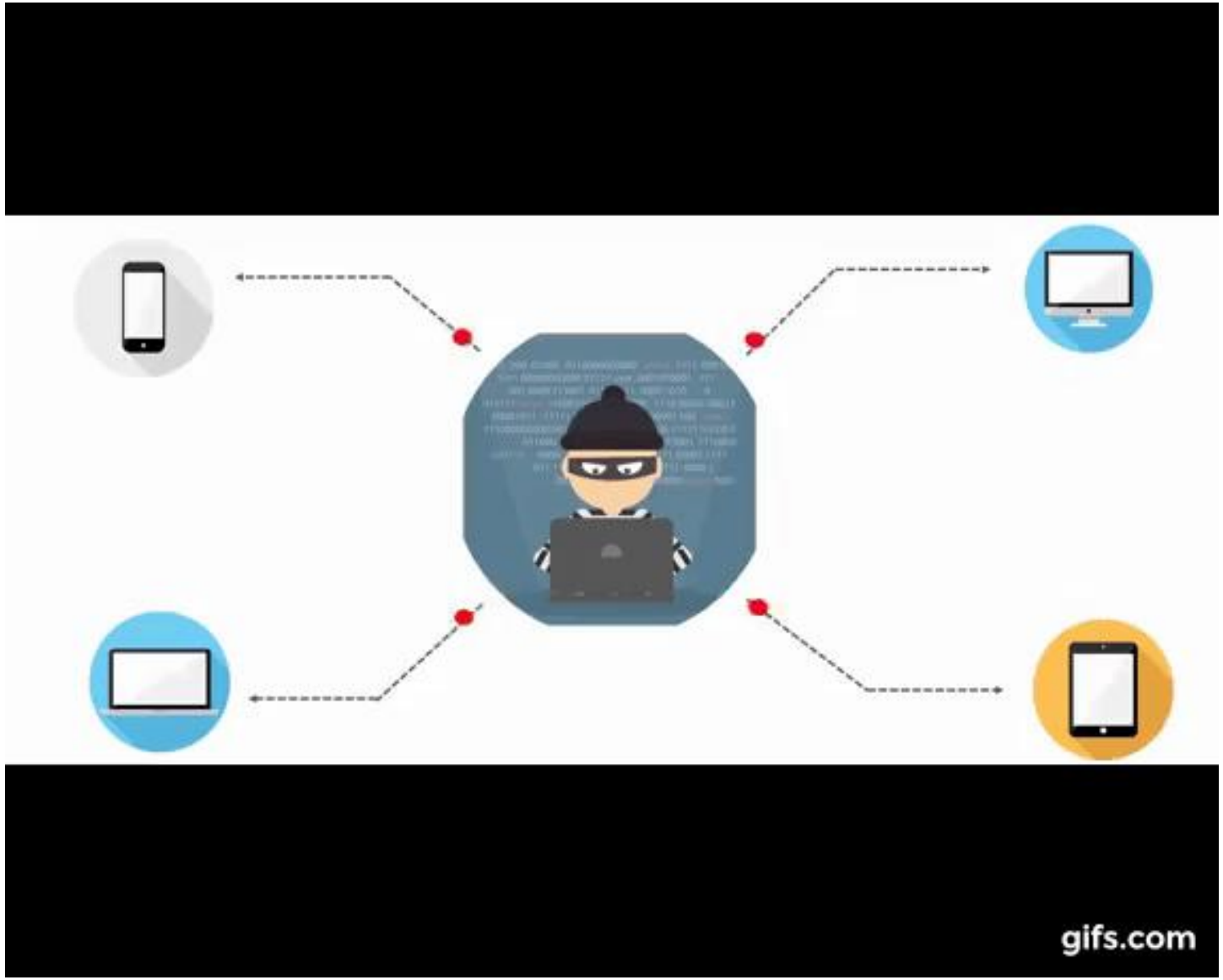
WHAT IS CYBER SECURITY?

DIGITAL ERA

- We are living in a digital era whether it be booking a hotel room ordering some dinner or even booking a cab
- We are constantly using the Internet and inherently constantly generating data
- This data is generally stored on the cloud which is basically a huge data server or data center that you can access online
- Also, we use an array of devices to access this data now for a hacker

GOLDEN AGE FOR DATA EXPLOITS

- It's a golden age with so many access points public IP addresses and constant traffic and tons of data to exploit
- Exploiting vulnerabilities and creating malicious software for the same above that cyber attacks are evolving by the day
- Hackers are becoming smarter and more creative with their malware and how they bypass virus scans and firewalls still baffle many people



TYPES OF ATTACKS

- some of the most common types of cyber attacks

What's a Bot?

- most sophisticated types of crime ware facing the Internet today.
- Bots oftentimes spread themselves across the Internet by searching for vulnerable, unprotected computers to infect.
- When they find an exposed computer, they quickly infect the machine and then report back to their master. Their goal is then to stay hidden until they are awoken by their master to perform a task.

Bot cont..

- Other ways in which a bot infects a machine include being downloaded by a Trojan, installed by a malicious Web site or being emailed directly to a person from an already infected machine.
- Bots do not work alone but are part of a network of infected machines called a botnet.ll Botnets are created by attackers repeatedly infecting victim computers using one or several of the techniques mentioned above

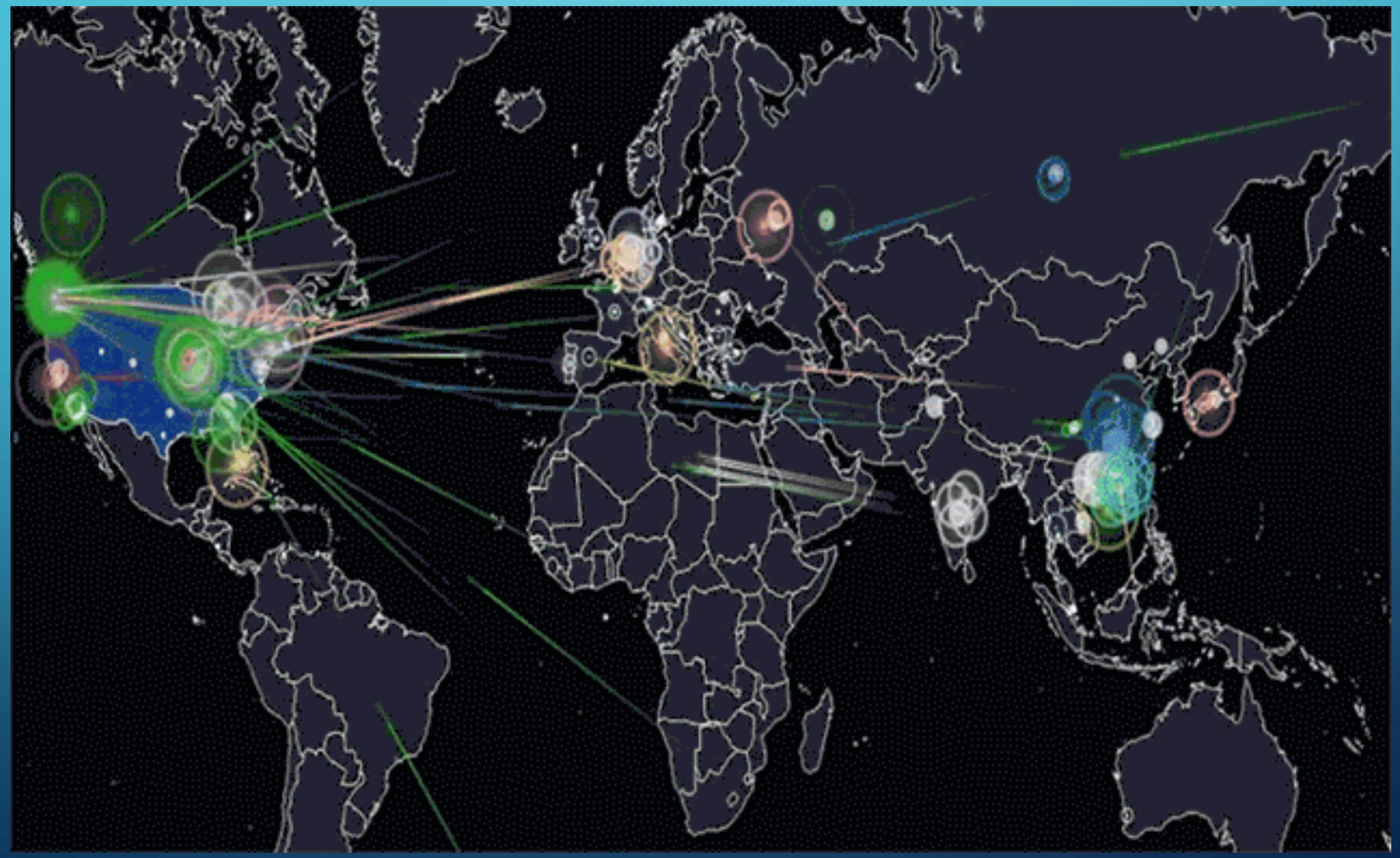
Bot cont..

- From spamming to hosting fraudulent Web sites, modern cybercrime at some point will make use of a botnet.
- Symantec reported nearly 9,000 different variations of the three most popular bots (Spybot, Gaobot, Randex) in the first half of 2005 alone.

Bot cont…

- Denial of Service
  - knock Web sites offline, making them unusable by their customers
- Extortion
  - warned in advance in what is known as a protection racket or extortion.
  - the criminal threatens to knock the company's Web site or online service off the Internet for a period of time if they are not paid.

DDOS ATTACK



https://threatmap.checkpoint.com/

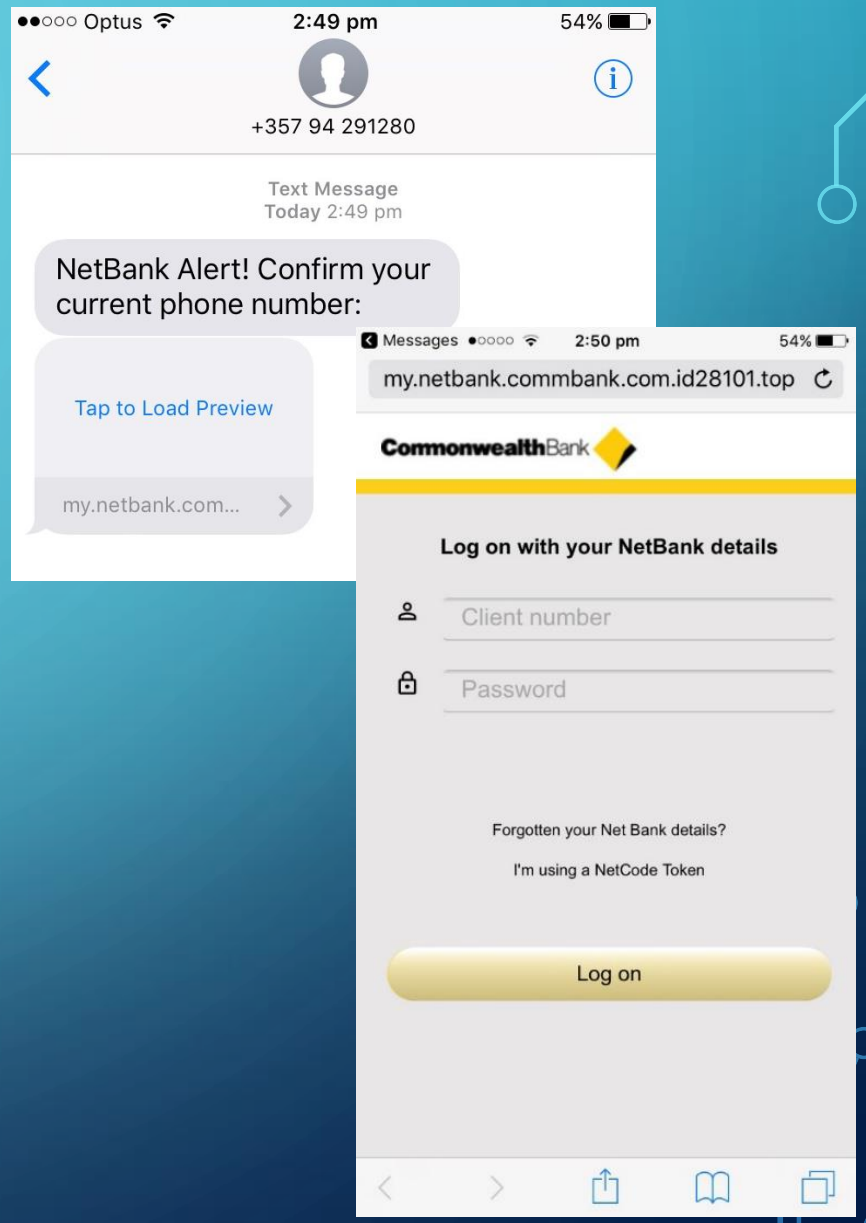
Bot cont…

- **Identity Theft**
  - sometimes they play the main and supporting role by not only infecting a computer, but also stealing personal information from the victim and sending it to the criminal.
- **Spam**
  - Botnets operate at the heart of today's spam industry bots both harvest email addresses for spammers and are also used to spam messages out. Sending spam through botnets is particularly common since it makes spammers more difficult to detect as they can send messages from many machines (all the infected machines in the botnet) rather than through a single machine.

Bot cont…

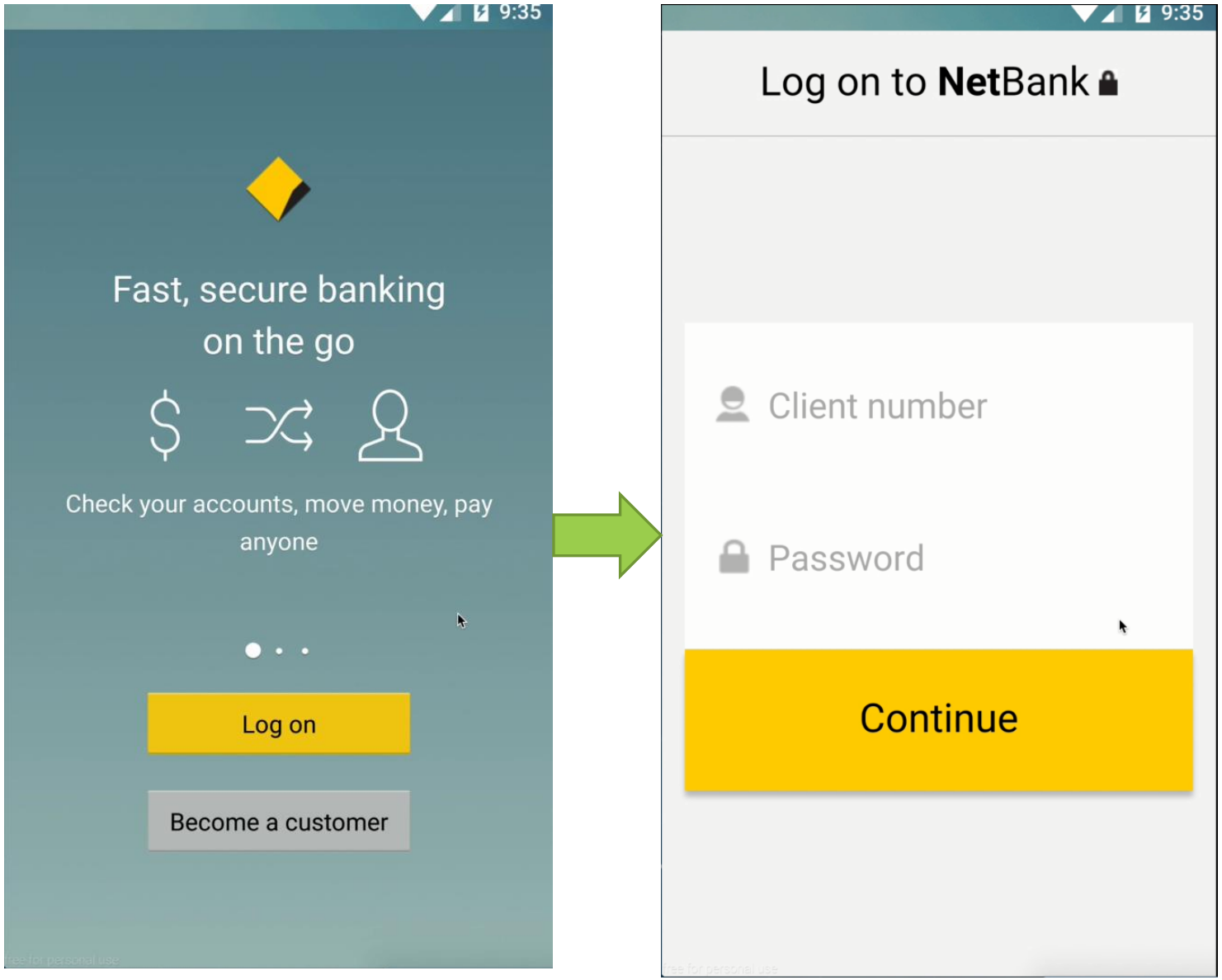
Phishing

- Much like spammers, phisher's use bots to identify potential victims and send fraudulent emails, which appear to come from a legitimate organization such as the user's bank.
- Bots are also used by phishers to host the phony Web sites, which are used to steal people's personal information and serve as collection points (dead dropll or egg dropll servers) for stolen data.



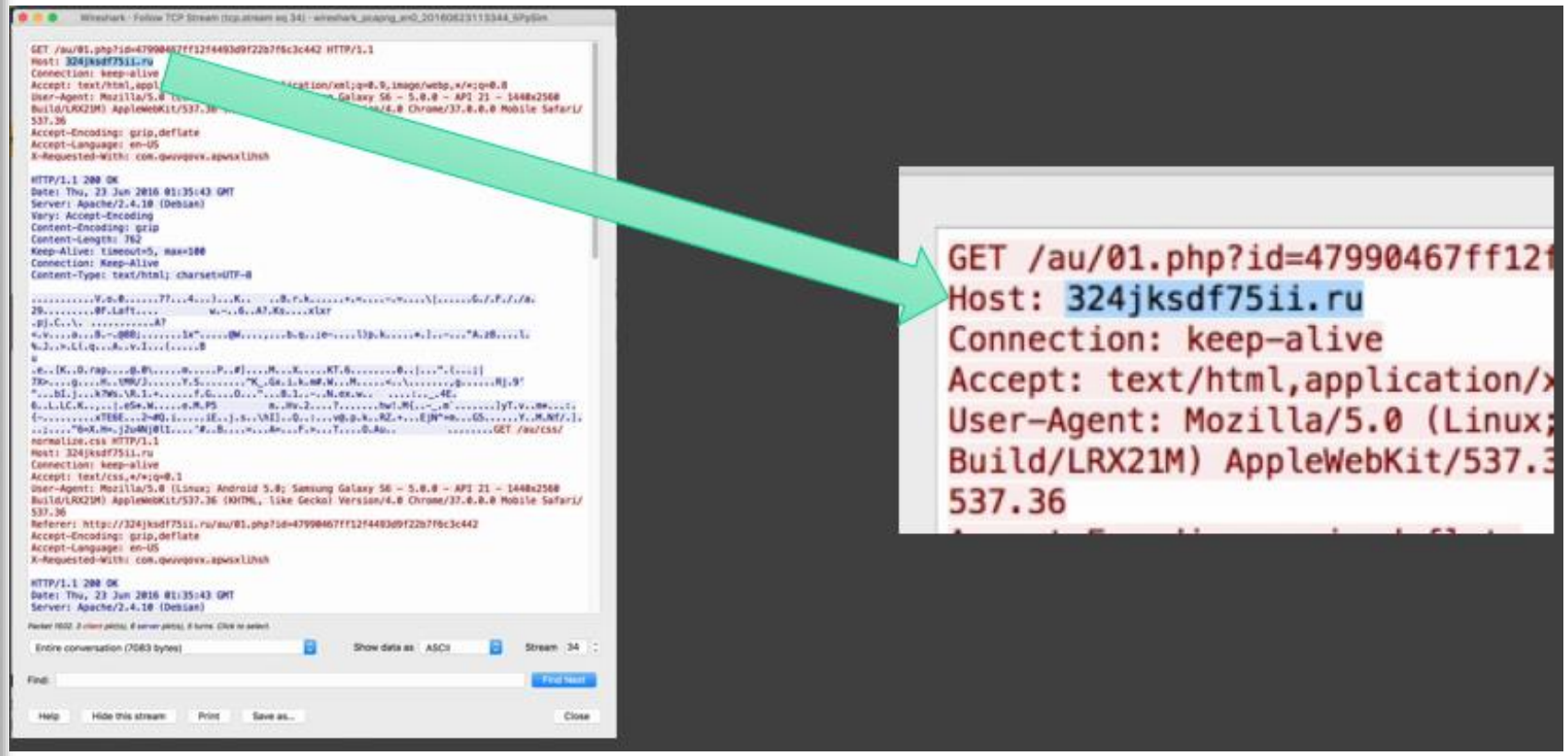
FAKE (MALICIOUS) APPS

- **Example: Android Malware (Marcher – GMBot – Maza)**



FAKE (MALICIOUS) APPS

- You can't *always* trust an application…



What is a Trojan horse?

- a Trojan horse program presents itself as a useful computer program, while it actually causes havoc and damage to your computer.
- Increasingly, Trojans are the first stage of an attack and their primary purpose is to stay hidden while downloading and installing a stronger threat such as a bot.
- Unlike viruses and worms, Trojan horses cannot spread by themselves.
- They are often delivered to a victim through an email message where it masquerades as an image or joke, or by a malicious website, which installs the Trojan horse on a computer through vulnerabilities in web browser software such as Microsoft Internet Explorer.

- After it is installed, the Trojan horse lurks silently on the infected machine, invisibly carrying out its misdeeds, such as downloading spyware, while the victim continues on with their normal activities.

What is Spyware?

- Spyware is a general term used for programs that covertly monitor your activity on your computer, gathering personal information, such as usernames, passwords, account numbers, files, and even driver's license or social security numbers.
- Some spyware focuses on monitoring a person's Internet behavior; this type of spyware often tracks the places you visit and things you do on the web, the emails you write and receive, as well as your Instant Messaging (IM) conversations.
- After gathering this information, the spyware then transmits that information to another computer, usually for advertising purposes.

- Spyware is similar to a Trojan horse in that users unknowingly install the product when they install something else. However, while this software is almost always unwelcome, it can be used in some instances for monitoring in conjunction with an investigation and in accordance with organizational policy.

Spyware is installed in many ways…

- Most often spyware is installed unknowingly with some other software that you intentionally install. For example, if you install a "free" music or file sharing service or download a screensaver, it may also install spyware. Some Web pages will attempt to install spyware when you visit their page.

Trojans, Spyware & Crime

- Trojans and spyware are developed by professionals. Trojans and spyware are often created by professional crimeware authors who sell their software on the black market for use in online fraud and other illegal activities.

Hacker Attacks

Spoofing…

- IP spoofing –
- In the context of computer security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.
- An attacker may fake their IP address so the receiver thinks it is sent from a location that it is not actually from. There are various forms and results to this attack.
  - The attack may be directed to a specific computer addressed as though it is from that same computer. This may make the computer think that it is talking to itself. This may cause some operating systems such as Windows to crash or lock up.

Man in the middle attack

- ◦ *Session hijacking* - An attacker may watch a session open on a network. Once authentication is complete, they may attack the client computer to disable it, and use IP spoofing to claim to be the client who was just authenticated and steal the session. This attack can be prevented if the two legitimate systems share a secret which is checked periodically during the session.

DNS Poisoning

- This is an attack where DNS information is falsified. This attack can succeed under the right conditions, but may not be real practical as an attack form. The attacker will send incorrect DNS information which can cause traffic to be diverted.
- The DNS information can be falsified since name servers do not verify the source of a DNS reply. When a DNS request is sent, an attacker can send a false DNS reply with additional bogus information which the requesting DNS server may cache.
- This attack can be used to divert users from a correct webserver such as a bank and capture information from customers when they attempt to logon.
- Password cracking - Used to get the password of a user or administrator on a network and gain unauthorized access.

DNS Cache Poisoning

- DNS provides distributed host information used for mapping domain names and IP addresses. To improve productivity, the DNS server caches the most recent data for quick retrieval.
- This cache can be attacked and the information spoofed to redirect a network connection or block access to the Web sites),a devious tactic called DNS cache poisoning.
- The best defense against problems such as DNS cache poisoning is to run the latest version of the DNS software for the operating system in use. New versions track pending and serialize them to help prevents spoofing.

Denial Of Service attacks

- Unlike other exploits, denial of service attacks are not used to gain unauthorized access or control of a system.
- They are instead designed to render it unusable.
- Attackers can deny service to individual victims, such as by deliberately entering a wrong password 3 consecutive times and thus causing the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once.

DoS:

- In a Denial of Service (DoS) attack, the attacker sends a stream of requests to a service on the server machine in the hope of exhausting all resources like "memory" or consuming all processor capacity.
- DoS Attacks Involve:
  - Jamming Networks
  - Flooding Service Ports
  - Misconfiguring Routers
  - Flooding Mail Servers

Distributed Denial of Service attack

- attacks are common, where a large number of compromised hosts (commonly referred to as "zombie computers", used as part of a botnet with, for example; a worm, trojan horse, or backdoor exploit to control them) are used to flood a target system with network requests, thus attempting to render it unusable through resource exhaustion.
- There are also commonly vulnerabilities in applications that cannot be used to take control over a computer, but merely make the target application malfunction or crash. This is known as a denial-of-service exploit.

MAKE YOURSELF A HARDER TARGET

- Only download mobile apps from official online app stores (iOS App Store, Windows Phone Store or Google Play Store)
  - ✓Trust your operating system to make this decision for you. On Android 4.0 and above, go to Settings and ensure the “unknown sources” feature is not selected. Your device will now be unable to download apps from anywhere but the Google Play store.
- Don’t ‘root’ or ‘jailbreak’ your device.

BASIC HYGIENE

Basic (user) hygiene

- Always change default credentials.
- Passphrases beat passwords (for length and complexity).
- Choose a password manager/wallet that stores your credentials in encrypted format.
- Be wary of attachments on emails (especially on emails you weren't expecting).
- Hover over links appearing in emails to check the web address ('tap and hold' on mobile).

Remember:
Your bank will never send you an email or SMS that asks you to confirm, update or disclose personal or banking information.

SECURING YOUR NETWORK

Create the Path of "most" resistance

While networks make it easy to share information within the office and with others, an improperly configured network risks allowing outsiders to disrupt your business activities or steal data.

Here are some essential steps for protecting your business network:

- Review your default settings
- Choose a secure form of encryption like Wireless Protected Access II (WPA2)
- Got guests? Create a visitor mode
- Turn off features you don't use like universal plug and play (UPnP)
- Keep an inventory of approved devices

THANK YOU