BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

innovate achieve lead

BITS Pilani
Pilani Campus

SSZG681: Cyber Offenses
Lecture No: 10

How Criminals Plan the Attacks

Agenda

- Overview of cyber attacks
- Cyber attack life cycle
- Tools to gather target information
- Overview of social engineering
- Role of cyber cafe in cybercrime
- Understand cyber stalking
- Learn about botnet

Cyber Crime Overview - Recap

Terminology

- **Hacker:** A person with strong interest in computers who enjoys learning and experimenting with them
  - Hackers are usually very talented, smart people who understand computers better than the others.
- **Brute Force Hacking: A** technique used to find passwords or encryption keys. It involves trying every possible combination of letters, numbers, etc., until the code is broken.
- **Cracker:** A person who breaks into computers. He is a computer criminal.
  - Acts include vandalism, theft and snooping in unauthorized areas.

Terminology…

- **Cracking:** An act of breaking into computers.
  - Cracking is a popular, growing subject on the internet.
  - Many sites are devoted to supplying crackers with tools that allow them to crack computers (like guessing passwords)
- **Cracker Tools:** Programs that break into computers i.e. password crackers, trojans, viruses, war dialers, worms etc.
- **Phreaking:** Art of breaking into phone or other communication systems.
- **War Dialer:** Program that automatically dials phone numbers looking for computers on the other end. It catalogs numbers so that the hackers can call back and try break in.

Vulnerabilities Exploited by Hackers

- Inadequate border protection
- Remote Access Servers (RASs) with weak access controls.
- Applications with known exploits
- Mis-configured or default configured systems

Commonly exploited vulnerabilities:

- Minimally protected phone systems
- Weak email credentials and phishing
- Poorly protected customer info
- Source code
- Website vulnerabilities
- OSINT gathering
- Distributed Denial of Service
- Software vulnerabilities
- Out of date patching

Hacker Types…

- **White Hat:** White hats are ethical hackers.
  - They use their knowledge and skill to thwart the black hats and secure the integrity of computer systems or networks.
  - They use hacking to identify vulnerabilities and inform the owners of systems so that the vulnerabilities can be plugged-in.
  - If a black hat decides to target you, it’s a great thing to have a white hat around.

- **Black Hat:** These are the bad guys. A black hat is a cracker and usage hacking with malicious intent
  - Black hats may also share information about the “break in” with other black hat crackers so they can exploit the same vulnerabilities before the victim becomes aware and takes appropriate measures.

Hacker Types…

- **Gray Hat –** A gray hat is a bit of both a white hat and a black hat.
  - Their main objective is not to do damage to a system or network, but to expose flaws in system security.
  - The black hat part of the mix is that they may very well use illegal means to gain access to the targeted system or network, but not for the purpose of damaging or destroying data:
  - They want to expose the security weaknesses of a particular system and then notify the “victim” of their success.
  - Often this is done with the intent of then selling their services to help correct the security failure so black hats can not gain entry and/or access for more devious and harmful purposes.

Categories of Cyber Crime

- Based on target of the crime
  - Crimes targeted at individuals
  - Crimes targeted at property
  - Crimes targeted at organizations
- Based on whether the crime occurs as a single event or as a series of events
  - **Single event cybercrime:** hacking or fraud
  - **Series of events:** cyber stalking

Cyber Attacks Types

- **Active attack**
  - Used to alter system
  - Affects the availability, integrity and authenticity of data
- **Passive attack**
  - Attempts to gain information about the target
  - Leads to breaches of confidentiality
- **Inside attack**
  - Attack originating and/or attempted within the security perimeter of an organization
  - Gains access to more resources than expected.
- **Outside attack**
  - Is attempted by a source outside the security perimeter,
  - May be an insider or an outsider, who is indirectly associated with the organization
  - Attempted through internet or remote access connection

Cyber Crime Life Cycle

Cyber Crime Planning

Cyber crime has 8 major phases:

- **Reconnaissance**: Get to know the target
- **Weaponization:** Things that need to get into the network
- **Delivery:** Attack starts
- **Exploitation:** Exploit the network and get better idea of network
- **Installation:** Ensure continued access to network
- **Command & control:** Take commanding position on the network
- **Action on Objective:** Achieve objectives
- **Close and Cover the Tracks:** Remove foot prints

Reconnaissance

- Identify a vulnerable target and explore the best ways to exploit it. The initial target can be anyone in an organization. The attacker requires a single point of entrance to get started.
- The questions that attacker needs answering at this stage are:
  - Who are the important people in the company? This can be answered by looking at the company web site or LinkedIn.
  - Who do they do business with? For this they may be able to use social engineering, by make a few “sales calls” to the company. The other way is good old-fashioned dumpster diving.
  - What public data is available about the company? Hackers collect IP address information and run scans to determine what hardware and software they are using. They check the ICAAN web registry database.
- An attacker attempts to gather information in two manners: Passive & Active

Passive Information Gathering

- Involves gathering information about the target without his/her knowledge
- **Google or Yahoo search:** to locate information about employees
- **Surfing online community group:** Facebook to gain information about an individual
- **Organization website:** for personnel directory or information about key employees; used in social engineering attack to reach the target
- Blogs, newsgroups, press releases, job postings etc.
- **Network sniffing:** information on Internet Protocol address ranges, hidden servers or networks or services on the system

Passive Information Gathering Tools

- Google Earth
- Internet Archive
- Linkedin, Facebook
- People Search
- Domain Name Confirmation
- WHOIS
- Nslookup
- Dnsstuff
- Traceroute
- VisualRoute Trace
- eMailTrackerPro
- HTTrack

```
nslookup
> ndtv.com
Non-authoritative answer:
Name: ndtv.com
Address: 72.247.54.47
```

WHOIS

Hostname: 72-247-54-47. deploy.static.akamaitechnologies.com
Address type IPv4 ASNAS9498
BHARTI Airtel Ltd. Organization Akamai Technologies, Inc. (akamai.com)
Route72.247.54.0/23

Active Information Gathering

- Involves probing the network to discover individual hosts to confirm the information gathered in the passive attack phase
- Can provide confirmation to an attacker about security measures in place

- **Arphound:** Listens network traffic and reports IP/MAC mismatches & IP conflicts
- **Arping:** Discovers and probes computers on a network
- **Bugtraq:** Mailing list about security related issues
- **Dig:** Queries domain name service database
- **DNStacer:** Where does a DNS servers gets it information from and follows the chain of servers
- **Dsniff:** Password sniffing and network analysis tool
- **Filesnarf:** sniffs files from NFS file system
- **FindSMB:** information about machine and subnets

- **Hmap:** finger printing of web servers
- **Hping:** TCP/IP packet analyzer
- **Hunt:** Exploit vulnerabilities in TCP/IP
- **Netcat:** reads and writes network connections using TCP & UDP
- **Nmap:** network explorer – security and port scanner
- **TCPdump:** command line packet analyzer
- **TCPreplay:** edits and replays previously captured packets

How Reconnaissance Works?

- **WHOIS Lookups:** Used for gathering domain names, IP addresses, and web system information.
- **NMAP Port Scanning:** A network discovery tool that can be used to identify open ports and vulnerabilities to exploit in your network.
- **Web Page Analysis & Email Address Search:** Using search engines and queries, attackers can gather information available about your organization and its email communications online.
- **Social Media Research:** Learning about your organization and its employees through Facebook, Linkedin, Twitter, and more can prove valuable for attackers looking to craft targeted phishing attacks.

Weaponization

- Coupling a remote access Trojan with a computer operating system or software application exploit into a deliverable payload. Increasingly, data files such as Microsoft Office documents or Adobe PDF files have been used as a weapon platform
- Three step process:
  - Step 1: Create believable Spear Phishing e-mails. These would look like e-mails that they could potentially receive from a known vendor or other business contact.
  - Step 2: Create Watering Holes, or fake web pages. These web pages will look identical to a vendor’s web page or even a bank’s web page. But the sole purpose is to capture your user name and password, or to offer you a free download of a document or something else of interest.
  - Step 3: Collect the tools that attacker plans to use once he gains access to the network so that he can successfully exploit any vulnerabilities found.

Delivery

- Implant of malware by remote or physical access to a targeted computer.
- Transmission of the payload to the target. The three commonly used delivery vectors for weaponized payloads:
  - Email messages with attachments containing malware
  - Websites containing malware that attack from a remote location
  - USB and other removable media containing malware
- Phishing e-mails are sent, Watering Hole web pages are posted to the Internet.
- If the Phishing e-mail contains a weaponized attachment, then the attacker waits for someone to open the attachment and for the malware to call home
- Attacker waits for all the data they need to start rolling in.

Exploitation

- Triggering of the attacker's code. The payload exploits an application or operating system vulnerability.
- It can exploit the user by persuading him to open an executable attachment, or leverage a feature of the operating system that auto-executes code
- If a user name and password arrive, the attacker tries it against web-based e-mail systems or VPN connections of the company network.
- If malware-loaded attachments were sent, then the attacker remotely accesses the infected computers.
- The attacker explores the network and gains a better idea of the traffic flow on the network, what systems are connected to the network and how they can be exploited.

Exploitation…

- Examples:
  - The attacker's malware seeks and locates a known or previously unknown software application or operating system vulnerability on a targeted network
  - An attacker persuades a user to open a malware executable attachment
  - The interception of computer wireless transmissions to monitor, modify, interrupt, or deny normal system or user operations or functions

Installation

- Creation of access point on a victimized computer that allows the attacker unauthorized entry and exit on a victimized computer and network.
- Attacker will install a persistent backdoor, create Admin accounts on the network, disable firewall rules and perhaps even activate remote desktop access on servers and other systems on the network.
- Example
  - Installing a remote access Trojan or backdoor on the victimized system and network, allowing the attackers to affect all users of the system
  - The physical emplacement of internal or external hardware devices that allow an attacker unauthorized access to a computer system or network
  - An attacker leverages a feature of a computer operating system that auto-executes malicious functions

Command & Control

- Now attacker has access to the network, administrator accounts, and all the needed tools are in place.
- This is unfettered access to the entire network.
- Attacker can look at anything, impersonate any user on the network, and even send e-mails from the CEO to all employees.
- Attacker is in control and can even lock you out of your network
- Examples:
  - An outbound beacon from the infected computer to the attacker, which is sort of a “phone home” function, that initiates a command and control dialogue between the attacker and the targeted computer
  - A connection that provides an attacker with “hands-on-the-keyboard” access to a targeted computer
  - The initiation of applications on a targeted computer that are not a normal user command or operating systems function

Action on Objectives

- Now attacker has the control and will work to achieve attack objectives.
  - Stealing information on employees, customers, product designs, etc.
  - Disrupt the operations of the company
  - If you take online orders, attacker can shut down your order-taking system or delete orders from the system.
  - Create orders and have them shipped to your customers.
- Common Actions
  - Data exfiltration—copying and removing files from computers or servers
  - Data corruption—altering or erasing data from computers or servers
  - Attacks to destroy—launching harmful applications or queries
  - Redirecting browser queries
- Cover the track – delete access logs, temporary files so that there is no trail attack.

Ways to Launch Attack Vectors

- Attack by email attachments
- Attack by Deception: Social Engineering/Hoaxes
- Hackers
- Heedless Guests (attack by webpage)
- Attack of the Worms
- Malicious Macros
- Foist ware/ Sneak ware
- Viruses

Zero-Day Attack

- A **zero-day** (or **zero**-hour or **day zero**) **attack** or threat is an **attack** that exploits a previously unknown vulnerability in a computer application or operating system, one that developers have not had time to address and patch.
- Software vulnerabilities may be discovered by hackers, by security companies or researchers, by the software vendors themselves, or by users.
- If discovered by hackers, an exploit will be kept secret for as long as possible and will circulate only through the ranks of hackers, until software or security companies become aware of it or of the attacks targeting it.

Scan for Information

- Scanning and scrutinizing gathered information is a key step to examine and identify vulnerabilities
- The objectives are:
  - Port scanning
  - Network scanning
  - Vulnerability scanning

Port Scan

- A port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.
- The result of a scan on a port is usually generalized into one of the following categories:
  - Open or accepted
  - Closed or not listening
  - Filtered or blocked.

Types of Port Scans

- **Vanilla**: the scanner attempts to connect to all 65,535 ports
- **Strobe:** a more focused scan looking only for known services to exploit
- **Fragmented packets:** the scanner sends packet fragments that get through simple packet filters in a firewall
- **UDP**: the scanner looks for open UDP ports
- **Sweep**: the scanner connects to the same port on more than one machine
- **FTP bounce**: the scanner goes through an FTP server in order to disguise the source of the scan
- **Stealth scan**: the scanner blocks the scanned computer from recording the port scan activities.

Scrutinize Phase

- Called as “enumeration” in the hacking world
- Objective is to identify:
  - Valid user accounts or groups
  - Network resources and/or shared resources
  - OS and different applications that are running on the machine.

Social Engineering

Social Engineering

- It is an art of exploiting the trust of people (“Con Game”)
- Influence and persuade a person to share his confidential information or perform some action.
- A social engineer usually uses telecommunications or internet to get them to do something that is against the security practices and policies of the organization.
- Involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.
- Social engineering is a non-technical method of intrusion that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.

Social Engineering: Human Based

- Requires interaction with humans (person-to-person contact) to retrieve desired information. Popular human based social engineering techniques are:
  - Impersonating an employee or user
  - Posing as an important user
  - Being a third person
  - Being a technical support Person
  - Shoulder surfing
  - Dumpster diving

Social Engineering: Computer Based

- Computer-based social engineering uses computer software that attempts to retrieve the desired information:
  - Fake E-mails
  - Baiting
  - E-mail attachments
  - Pop-up windows

Impersonation: An Employee or User

- Hacker pretends to be an employee or valid user on the system.
- Hacker may gain physical access by pretending to be a janitor, employee, or contractor.
- Valid credentials are a coveted assets for attackers.
- An attacker who has obtained valid user credentials through social engineering techniques has the ability to roam the network with impunity searching for valuable data.
- In log data, the attacker’s activities are easily hidden due to the inability to see the subtle differences in behaviors and access characteristics.
- This phase of attack chain often represents the lengthiest portion of the attack.

Impersonation: An Important User

- Hacker pretends to be a VIP or high-level manager who has the authority to use computer systems or files.
- Most of the time, low-level employees don’t ask any questions of someone who appears in this position.

Impersonation: A Third Party Person

- Hacker pretends to have permission from an authorized person to use the computer system.
- It works when the authorized person is unavailable for some time.

Impersonation: A Technical Support Person

- Calling tech support for assistance is a classic social-engineering technique.
- Help desk and technical support personnel are trained to help users, which makes them good prey for social engineering attacks.

Shoulder Surfing

- **Shoulder surfing:** Shoulder surfing is the technique of gathering passwords by watching over a person’s shoulder while they log in to the system.
- A hacker can watch a valid user log in and then use that password to gain access to the system.

Dumpster Diving

- Dumpster diving involves looking in the trash for information written on pieces of paper or computer printouts.
- Hacker can often find passwords, filenames, or other pieces of confidential information like SSN, PAN, Credit card ID numbers etc
- Also called dumpstering, binning, trashing, garbage gleaning, scavenging etc.

Fake E-mails

- Phishing involves false emails, chats, or websites designed to impersonate real systems with the goal of capturing sensitive data.
- A message might come from a bank or other well-known institution with the need to "verify" your login information.
- It will usually be a mocked-up login page with all the right logos to look legitimate.
- The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords without the knowledge of AOL users.
- They replaced "f" by "ph"

Baiting

- Baiting involves dangling something you want to entice you to take an action the criminal desires.
- It can be in the form of a music or movie download on a peer-to-peer site or it can be a USB flash drive with a company logo labeled “Executive Salary Summary Q1 2013” left out in the open for you to find.
- Once the device is used or downloaded, the person or company’s computer is infected with malicious software allowing the criminal to advance into your system.

E-Mail Attachments

- Emails sent by scammers may have attachments that include malicious code inside the attachment.
- Those attachments can include key loggers to capture users' passwords, viruses, Trojans, or worms.

Pop-up Windows

- Pop-up windows can be used in social engineering attacks.
- Pop-up windows that advertise special offers may tempt users to unintentionally install malicious software.

Don’t Be a Victim

- **Slow down:** Spammers want you to act first and think later. If the message conveys a sense of urgency, or uses high-pressure sales tactics be skeptical
- **Research the facts:** Be suspicious of any unsolicited messages. If the email looks like it is from a company you use, do your own research. Use a search engine to go to the real company’s site, or a phone directory to find their phone number.
- **Delete any request for financial information or passwords:** If you get asked to reply to a message with personal information, it’s a scam.
- **Reject requests for help or offers of help:** Legitimate companies and organizations do not contact to provide help. If you did not specifically request assistance from the sender, consider any offer to help i.e. restore credit scores, refinance a home, answer your question etc., a scam.
- **Don’t use an in-line link to access websites:** Find the websites using a search engine to be sure you land where you intend to land. Hovering over links in email will show the actual URL at the bottom, but a good fake can still steer you wrong.

Don’t Be a Victim…

- **Email hijacking is rampant:** Hackers taking over control of people’s email accounts (and other communication accounts) is rampant. Even when sender is known but you aren’t expecting an email with a link or attachment, check with your friend before opening links or downloading attachment.
- **Beware of any download:** If you don’t know the sender personally and got an attachment from them, avoid downloading it.
- **Foreign offers are fake:** Emails from a foreign lottery, money offer from an unknown relative or requests to transfer funds from a foreign country for a share of the money, are scam.
- **Set your spam filters to high:** Use email spam filter, set these filters to high and check your spam folder periodically to see if legitimate email has been categorized as spam.
- **Secure your computing devices:** Install anti-virus software, firewalls, email filters and keep these up-to-date. Set your operating system to automatically update, and if your smart phone doesn’t automatically update, manually update it whenever you receive a notice to do so.
- **Avoid phishing:** Use an anti-phishing tool offered by your web browser or third party to alert you to risks.

Cyber Stalking

Cyber Stalking

- **Cyber stalking** is the use of the Internet or other electronic means to stalk or harass an individual, a group, or an organization.
- May include false accusations, defamation, slander and libel.
- May include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass.
- Also referred to as Internet stalking, e-stalking or online stalking.

Cyber Stalking…

- Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging or messages posted to a web site or a discussion group.
- A cyber stalker relies upon the anonymity afforded by the internet to allow them to stalk their victim without being detected.
- Cyber stalking messages differ from ordinary spam in that a cyber stalker targets a specific victim with often threatening messages, while the spammer targets a multitude of recipients with simply annoying messages.

Types of Stalkers

- Online and Offline stalkers
- Stalking is a criminal offense
- Stalker is motivated by a desire to control, intimidate or influence a victim
- Stalker may be an online stranger or a person whom the target knows
- Stalker may be anonymous and solicit involvement of other people online who do not even know the target

How Stalking Works?

- Personal information gathering about the victim
- Establish a contact with the victim through telephone/cell phone and start threatening or harassing
- Establish a contact with the victim through email
- Keep sending repeated emails asking for various kinds of favors or threaten the victim
- Post victim’s personal information on any website related to illicit services
- Whosoever comes across the information, start calling the victim on the given contact details, asking for illicit services
- Some stalkers may subscribe/ register email account of the victim to innumerable pornographic and sex sites, because of which victim starts receiving such unsolicited emails

Cyber Cafe and Cyber Crimes

- An **Internet café** or **cybercafé** is a place which provides Internet access to the public, usually for a fee.
- According to Nielsen Survey on the profile of cyber cafes users in India:
  - 37% of the total population use cyber cafes
  - 90% of this were males in age group 15-35 years
  - 52% graduates and post-graduates
  - > 50% were students
- Its extremely important to understand the IT security and governance practiced in the cyber cafes.

Cyber Café: Usage Risks

- Can be used for either real or false terrorist communication
- For stealing bank passwords, fraudulent withdrawal of money
  - Key loggers or spywares
  - Shoulder surfing
- For sending obscene mails to harass people.
- Not considered as network service providers according to ITA2000
- They are responsible for “due diligence”

Cyber Café: Illegal Activities

- Pirated software: OS, Browser, Office
- Antivirus software not in use or not updated
- Cybercafes should have “deep freeze” software
  - Clears details of all activities carried out, when one clicks “restart” button
- Annual Maintenance Contract(AMC): normally not in place
  - Its a risk as cybercriminal can install malicious code for criminal activities
- Pornographic websites and similar websites are not blocked
- Owners have low awareness about IT Security and IT Governance.
- IT Governance guidelines are not provided by cyber cell wing
- No periodic audit visits by cyber cell wing (state police) or cyber cafe association

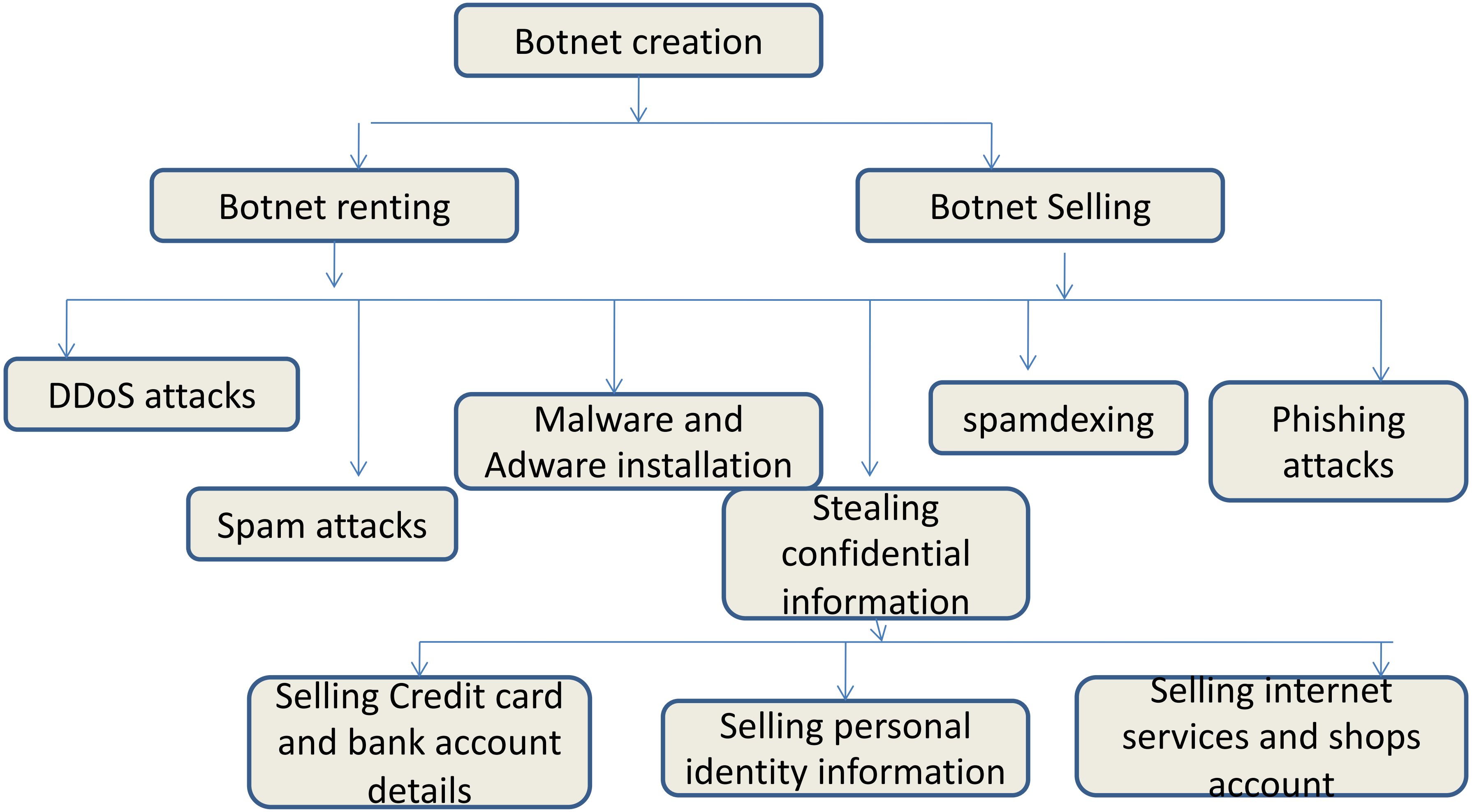
Cyber Café: Safety and Security Measures

- Always Logout: do not save login information through automatic login information
- Stay with the computer
- Clear history and temporary files before and after use
- Be alert: don’t be a victim of shoulder surfing
- Avoid Online Financial Transaction
- Don’t change passwords
- Use virtual Keyboards
- Look for security warnings

Botnets: The Fuel for Cybercrime

- **Bot:** An automated program for doing a particular task, often over a network
- **Botnet (zombie army):** A number of internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the internet
- **Zombie:** A computer "robot" or "bot" that serves the wishes of a master spam or virus originator
- Most computers compromised in this way are home-based.
- As per Russia based Kaspersky Labs, botnets - not spam, viruses, or worms - pose the biggest threat to the internet

Use of Botnets


Botnet creation

Botnet renting

Botnet Selling

DDoS attacks

Spam attacks

Malware and Adware installation

Stealing confidential information

spamdexing

Phishing attacks

Selling Credit card and bank account details

Selling personal identity information

Selling internet services and shops account

Measures to Secure the System

- Use antivirus and anti-spyware
- Install updates
- Use firewall
- Disconnect internet when not in use
- Don’t trust free downloads
- Check regularly inbox and sent items
- Take immediate action if system is infected

Prominent Cyber Attack Examples

- **Iran Nuclear Program**
  - Earliest instance of a nation waging cyberwar was the Stuxnet worm, which was used to attack Iran's nuclear program in 2010. The malware targeted SCADA (supervisory control and data acquisition) systems and was spread with infected USB devices. United States and Israel have both been linked to the development of Stuxnet, neither nation has formally acknowledged its role.
- **Ukraine DDOS Attack**
  - In March 2014, the Russian government allegedly perpetrated a DDOS attack that disrupted the internet in Ukraine, enabling pro-Russian rebels to take control of Crimea.
  - In May 2014, three days before Ukraine's presidential election, a Russian hacking group took down Ukraine's election commission's system, including the backup system. Ukrainian computer experts were able to get the system up and running before the election. The attack was launched to wreak havoc and damage the nationalist candidate while helping the pro-Russian candidate, who ultimately lost the election.
- **Sony Picture Attack**
  - Hackers associated with the government of North Korea were blamed for the 2014 cyber attack on Sony Pictures after Sony released the film 'The Interview', which portrayed the North Korean leader Kim Jong-un in a negative light. During its investigation into the hack, the FBI noted that the code, encryption algorithms, data deletion methods and compromised networks were similar to malware previously used by North Korean hackers. In addition, the hackers used several IP addresses associated with North Korea.
- **German Parliament Infection**
  - A 2015 attack on the German parliament, suspected to have been carried out by Russian secret services, caused massive disruption when the attack infected 20,000 computers used by German politicians, support staff members and civil servants. Sensitive data was stolen, and the attackers demanded several million euros to clean up the damage. Although a group of Russian nationalists who wanted the government of Berlin to stop supporting Ukraine claimed responsibility, members of the Russian intelligence were also reported to be involved.

Prominent Cyber Attack Examples…

- Malware Analysis Report (MAR) issued by the Department of Homeland Security (DHS) and the FBI identified two malware codes, HOPLIGHT and ELECTRICFISH, released by North Korea.
- In 2015, cybercriminals backed by the Chinese state were accused of breaching the website of U.S. Office of Personnel Management to steal data on approximately 22 million current and former employees of the U.S. government. Chinese cybercriminals have been implicated in the theft of U.S. military aircraft designs, an incident that caused then-president Barack Obama to call for a treaty on cyber arms control.
- In December 2016, more than 230,000 customers in Ukraine experienced a blackout, the result of remote intrusions at three regional electric power distribution companies. The attack was suspected to originate from Russia. The perpetrators flooded phone lines with a DoS attack and also used malware to attack and destroy data on hard drives at the affected companies. While the power was restored within hours, it took months for the companies to restore full functionality to the control centers that had been attacked.
- In 2016, 2017 and 2018, variations of malware known as Shamoon struck businesses in the Middle East and Europe. McAfee’s Advanced Threat Research concluded that the Iranian hacker group APT33, or a group masquerading as APT33, is likely responsible for these attacks.
- On August 2, 2017, President Trump signed into law the Countering America’s Adversaries Through Sanctions Act (Public Law 115-44) (CAATSA), imposing new sanctions on Iran, Russia, and North Korea.

Thank You