CSC429 – Computer Security

LECTURE 6
MALICIOUS PROGRAMS

Mohammed H. Almeshekah, PhD
meshekah@ksu.edu.sa

Quiz 1

- Marking a Stack to be non-executable prevent the attacker from running code in the Stack where:
  1. Attacker can no longer execute an arbitrary sequence of instruction.
  2. Attacker can intelligently craft a sequence of function calls to achieve his goals.
  3. Attacker can only call one function in libc library.
  4. Attacker cannot inject code at all in the Stack as it is non-executable.

- Mark the statement above with **T**rue or **F**alse.

Malicious Programs

- **Malware**: software designed to infiltrate or damage a computer system without the owner's informed consent

- **Spyware:** software designed to intercept or take partial control over the user's interaction with the computer, without the user's informed consent
  - secretly monitors the user's behavior
  - collect various types of personal information

Trapdoor/Back-Door

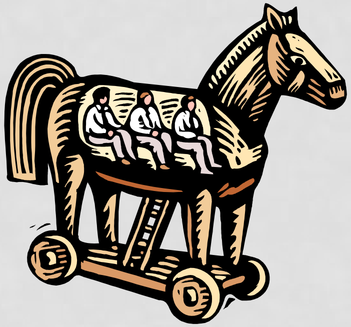
- Secret entry point into a system
  - Specific user identifier or password that circumvents normal security procedures.
- Presents a security risk
- Could be used for
  - Troubleshooting
  - Maintenance
  - Malicious intent

Logic Bomb

- Embedded in legitimate programs.
- Activated when specified conditions met
  - E.g., presence/absence of some file; Particular date/time or particular user
- When triggered, typically damages system
  - Modify/delete files/disks
- E.g. Shamoon Virus

Trojan Horse

- Program with an overt (expected) and covert (unexpected) effect
  - Appears normal/expected
  - Covert effect violates security policy



- User tricked into executing Trojan horse
  - Expects (and sees) overt behavior
  - Covert effect performed with user's authorization

- E.g. Pirated software

Virus

- Self-replicating code
  - Like replicating Trojan horse
  - Alters normal code with "infected" version

- No *overt* action
  - Generally tries to remain undetected

- Operates when infected code executed

```
If spread condition then
    For target files
        if not infected then alter to include virus
```

  - Perform malicious action

Virus Types

- Boot Sector
  - Problem: How to ensure virus “carrier” executed?
  - Solution: Place in boot sector of disk
    - Run on any boot
  - Propagate by altering boot disk creation
  - *Similar concepts now being used for thumb drive*
- Executable
  - Malicious code placed at beginning of legitimate program
  - Runs when application run
  - Application then runs normally

Virus Types/Properties

- Terminate and Stay Resident
    - Stays active in memory after application complete
- Stealth
    - Encrypt virus
        - Prevents "signature" to detect virus
    - Polymorphism
        - Change virus code to prevent signature

Macro Virus

- Infected “executable” isn’t machine code
    - Relies on something “executed” inside application data
    - Common example: Macros
- Otherwise similar properties to other viruses
    - Architecture-independent
    - But, Application-dependent

Worm

- Runs independently
  - Does not require a host program
- Propagates a fully working version of itself to other machines
- Carrie a payload performing hidden tasks
  - Backdoors, spam relays, DDoS agents; …
- Phases
  - Probing ➔ Exploitation ➔ Replication ➔ Payload

Cost of Worm Attacks

- Morris worm, 1988
  - Infected approximately 6,000 machines
    - 10% of computers connected to the Internet
  - cost ~ $10 million in downtime and cleanup

- Code Red worm, July 16 2001
  - Direct descendant of Morris' worm.
  - Infected more than 500,000 servers.
  - Caused ~ $2.6 Billion in damages.

- Love Bug worm:
  - May 3, 2000, $8.75 billion

- WannaCry:
  - June 2017, $10 billion

Morris Worm

- What happened to Morris?
  - Robert T. Morris was convicted of violating the computer Fraud and Abuse Act (Title 18), and sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision.
- Where is now Morris?
  - Professor at MIT
- Who was the first to analyze the Morris worm?
  - Prof. Spafford at Purdue
    - “The Internet Worm Program: An Analysis”.

Computer Emergency Response Team (CERT)

- As a result of Morris worm incident, DARPA created CERT, a development center at Carnegie Mellon University in Pittsburgh, Pennsylvania.

- Coordinates communication among experts during security emergencies and to help prevent future incidents.

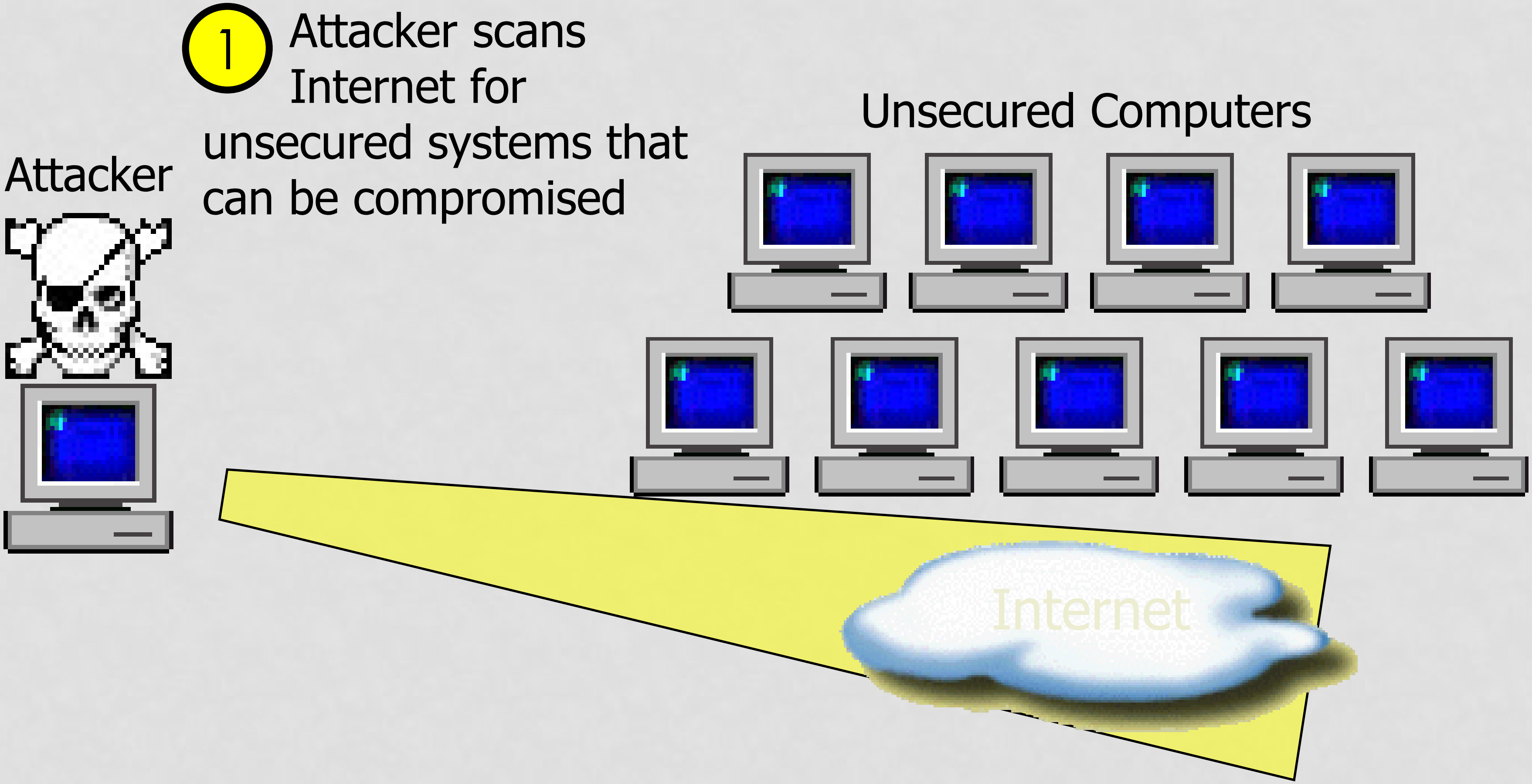
Zombie & Botnet

- Secretly takes over another networked computer by exploiting software flows

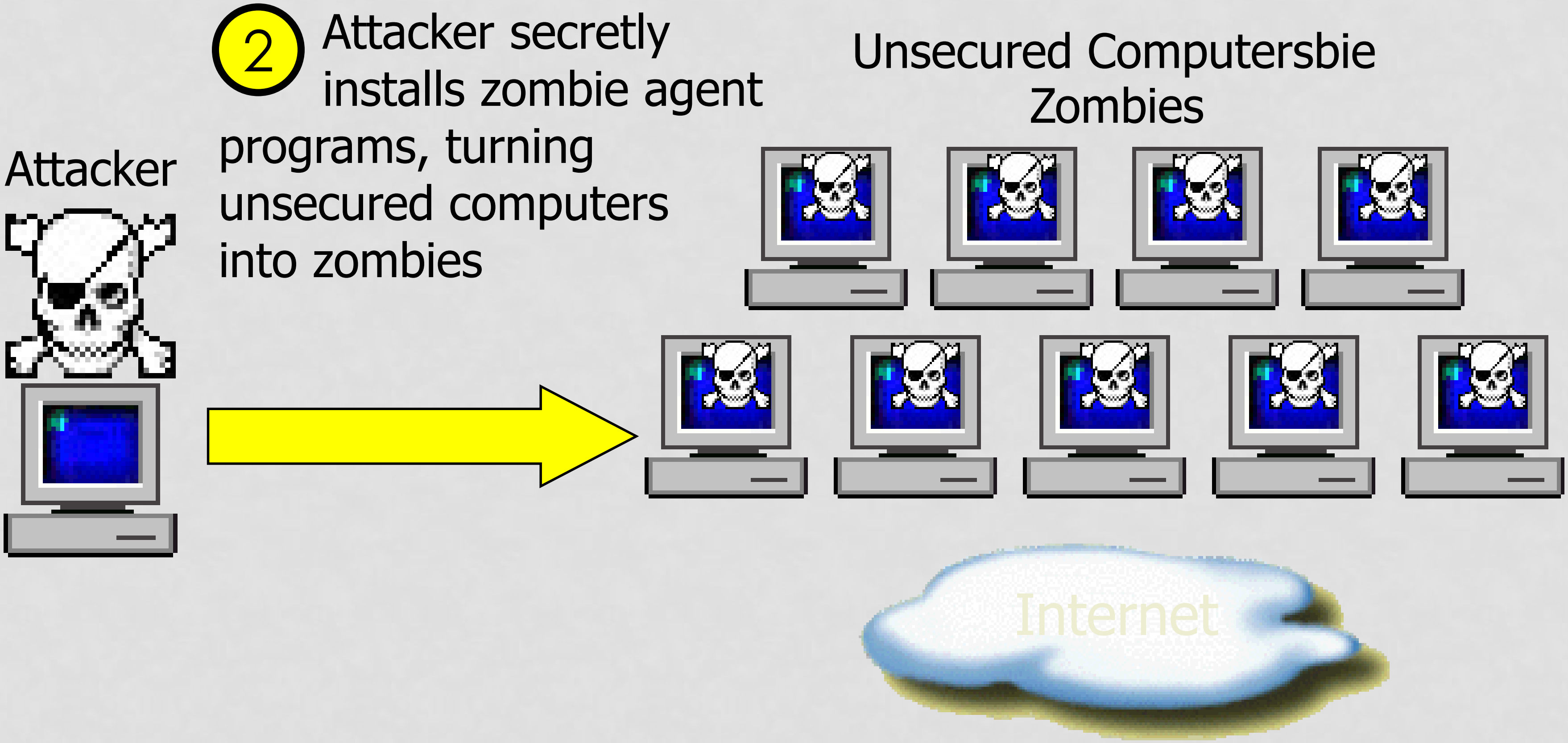
- Builds the compromised computers into a zombie network or botnet
  - a collection of compromised machines running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure.

- Uses it to indirectly launch attacks
  - E.g., DDoS, phishing, spamming, cracking

Botnets and DDoS – Step 1


1
Attacker scans Internet for unsecured systems that can be compromised
Unsecured Computers
Attacker
Internet

Botnets and DDoS – Step 2

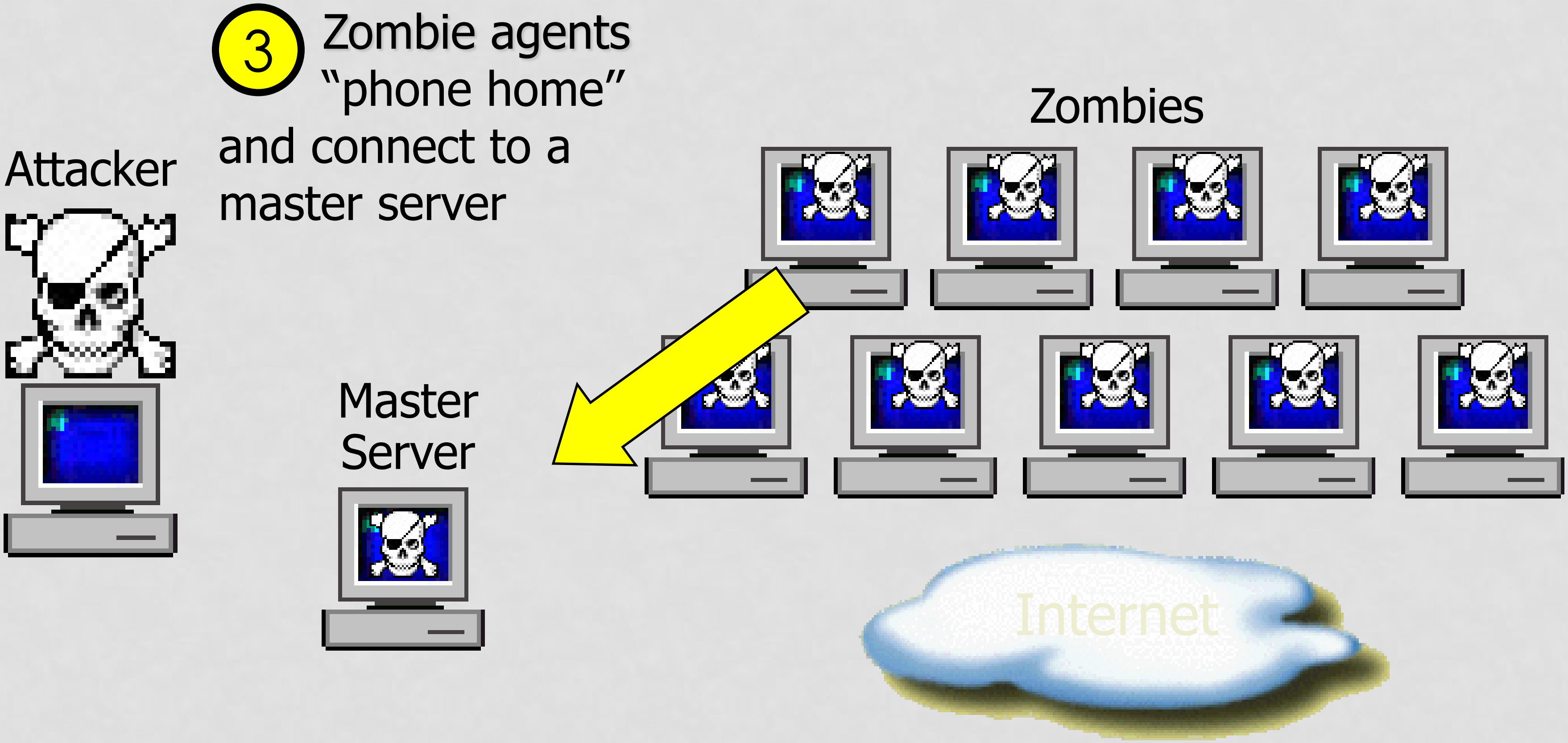


2 Attacker secretly installs zombie agent programs, turning unsecured computers into zombies

Unsecured Computersbie Zombies

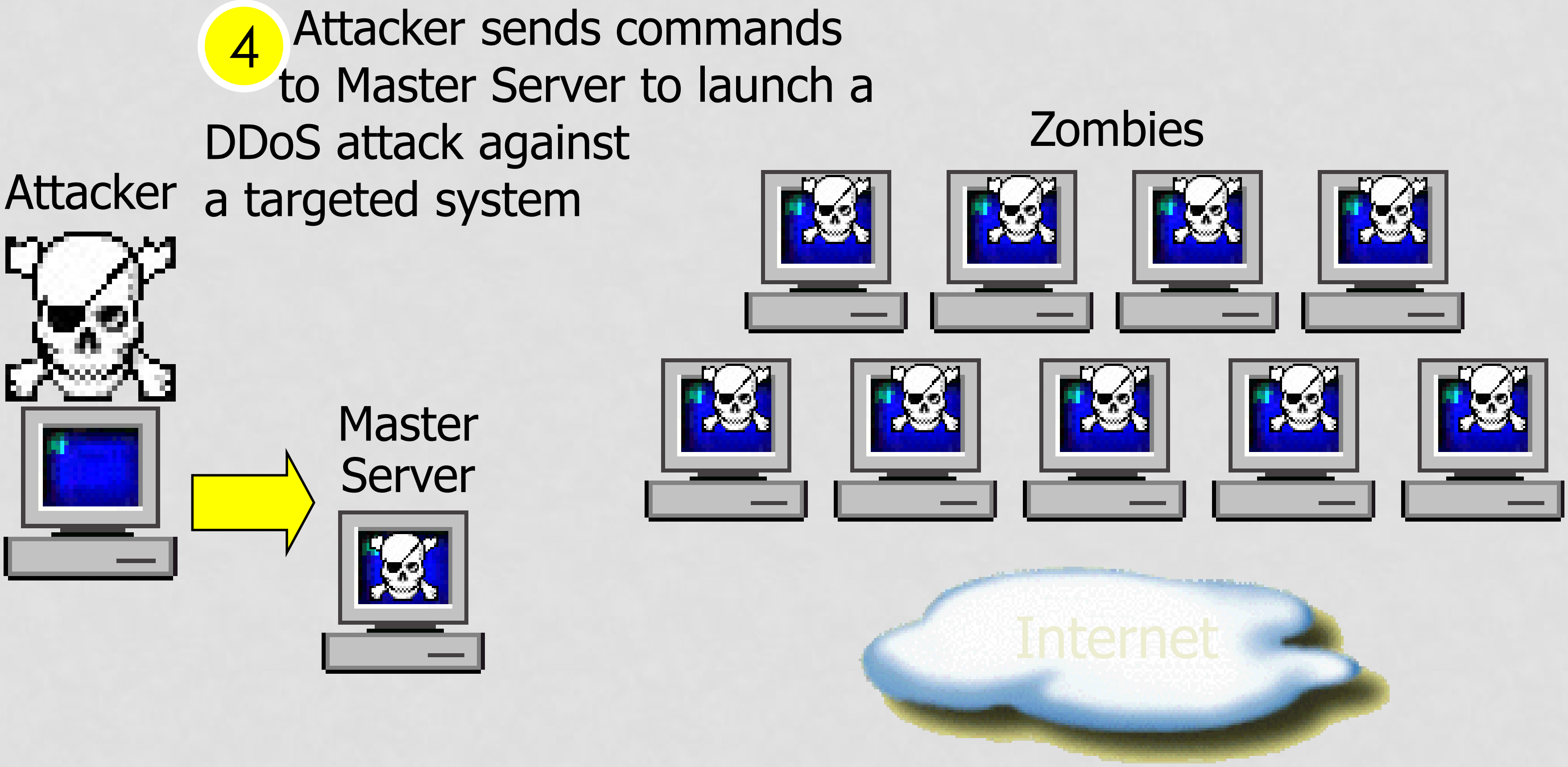
Attacker

Botnets and DDoS – Step 3



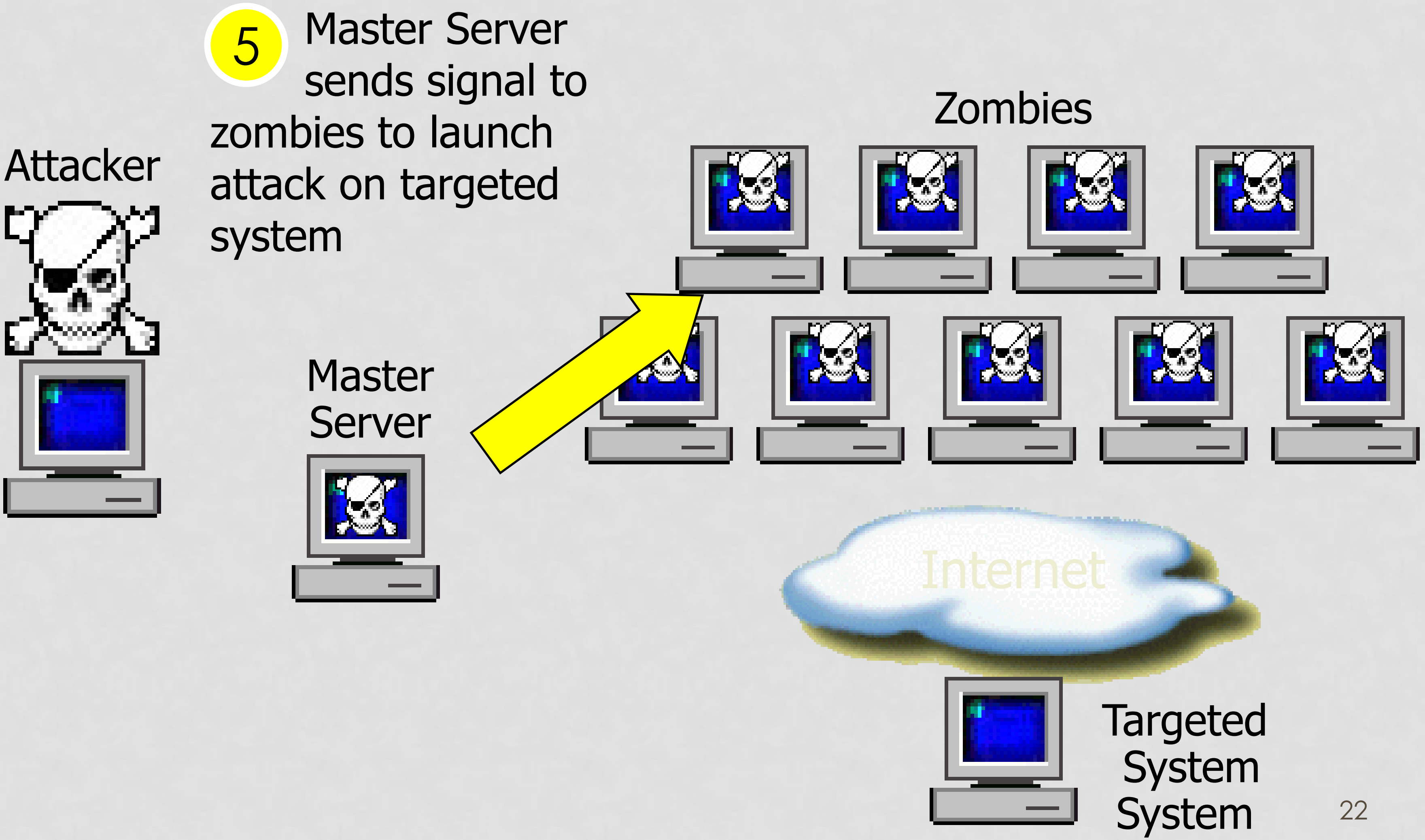
3 Zombie agents "phone home" and connect to a master server

Botnets and DDoS – Step 4



4 Attacker sends commands to Master Server to launch a DDoS attack against a targeted system

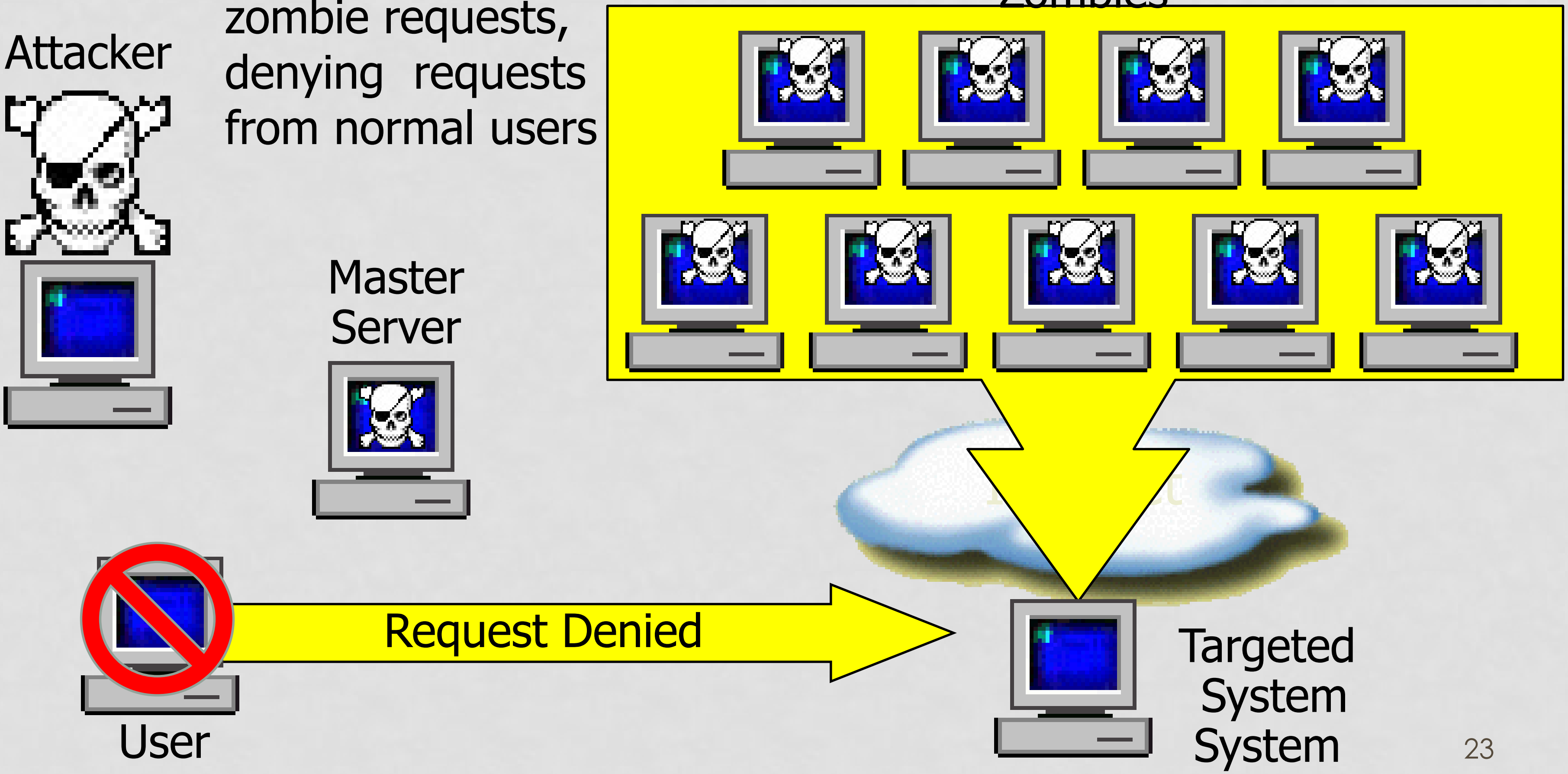
Botnets and DDoS – Step 5



Master Server sends signal to zombies to launch attack on targeted system

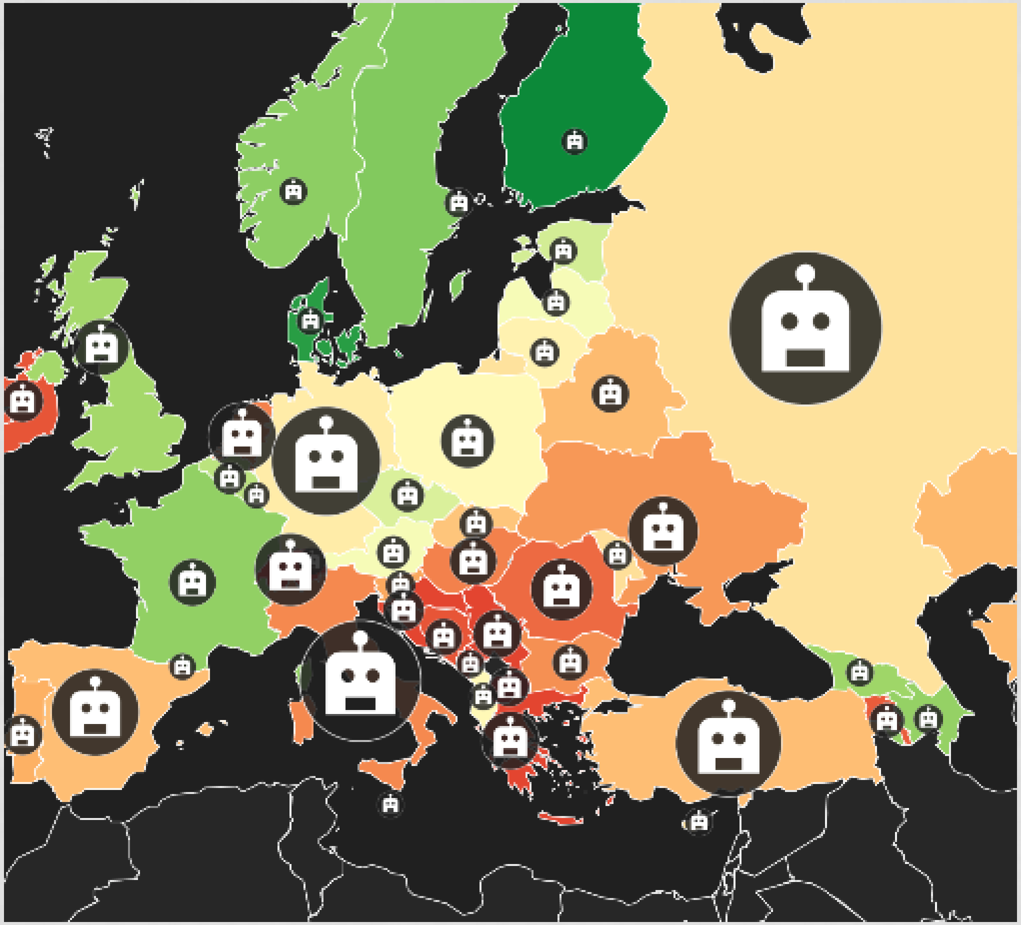
Botnets and DDoS – Step 6

6 Targeted system is overwhelmed by zombie requests, denying requests from normal users



Bots are everywhere!

https://uk.norton.com/tools/bots/index.html



Rootkits

- Software used after system compromise to:
  - Hide the attacker's presence
  - Provide backdoors for easy reentry
- Simple rootkits:
  - Modify user programs (ls, ps)
  - Detectable by tools like Tripwire
- Sophisticated rootkits:
  - Modify the kernel itself.
  - May also change the boot record.
  - Harder to detect.

Spyware

- **Spyware:** software designed to intercept or take partial control over the user's interaction with the computer, without the user's informed consent
  - secretly monitors the user's behavior
  - collect various types of personal information

- Techniques:
  - Log keystrokes
  - Collect web history
  - Scan documents on hard disk.

- **Adware**: software that display marketing information.

Drive-By-Download

- **Drive-by download** means two things, each concerning the unintended download of computer software from the Internet:
  - Downloads which a person authorized but without understanding the consequences (e.g. ActiveX component, or Java applet).
  - Download that happens without the user's knowledge.

Scareware

- Software
  - with malicious payloads
  - Sold by social engineering to cause shock, anxiety, or the perception of a threat
- Rapidly increasing

Ransomware

- Holds a computer system, or the data it contains, hostage against its user by demanding a ransom.
  - Disable an essential system service or lock the display at system startup
  - Encrypt some of the user's personal files.

- Victim user has to
  - Enter a code obtainable only after wiring payment to the attacker or sending an SMS message.
  - Buy a decryption or removal tool.

Malicious Programs

Detection and Prevention

Malicious Programs Detection

- How to detect a malicious program:
  - Change in executables
    - Length
    - Content
    - Date/time in the directory listing.
  - Unaccounted use of resources (esp. memory)
  - Unusual hardware behavior

- There is always the issue with false positives/negatives.

Anti-Viruses

- Types of anti-virus packages:
  1. Activity monitors
     - Look for virus-like activity (e.g., write to executable, …)
  2. Scanners
     - Look for known viruses
     - Include virus-removers
  3. Authentication or change-detection
     - Compute/store hashes.
     - Later, compute and compare with stored.
     - Can catch unknown viruses, also disinfect.

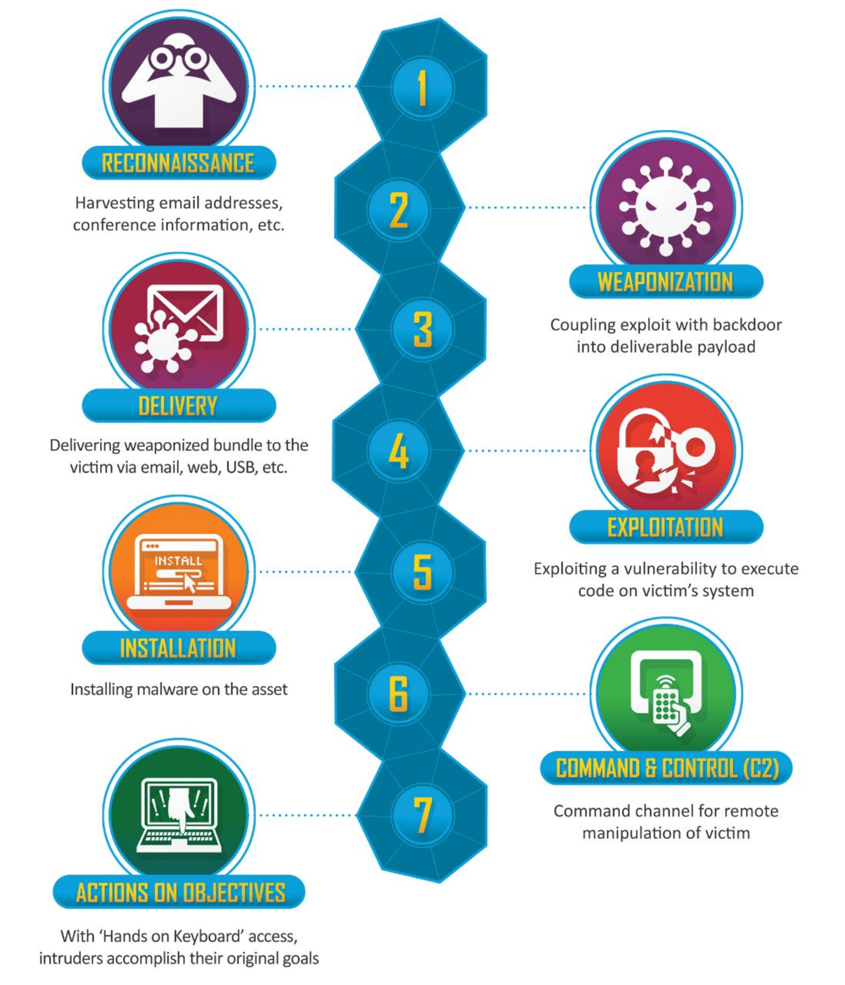
Virus Checking Gateways

- Virus-checking gateways
  - Scan incoming and outgoing
    - E-mail attachments
    - Transferred files
- Challenges!
  - Unusual formats, encrypted file, etc.

Prevention

- Keep your software up to date
  - Promptly (patch distribution problem).
  - Tools like “Secunia” can help.
- Use only clean software
- If you have to take risks:
  - Do so with least privilege (limits damage)
- File protections
  - Network access rights can protect.

Cyber Kill Chain



1 RECONNAISSANCE

Harvesting email addresses, conference information, etc.

2 WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

3 DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION

Installing malware on the asset

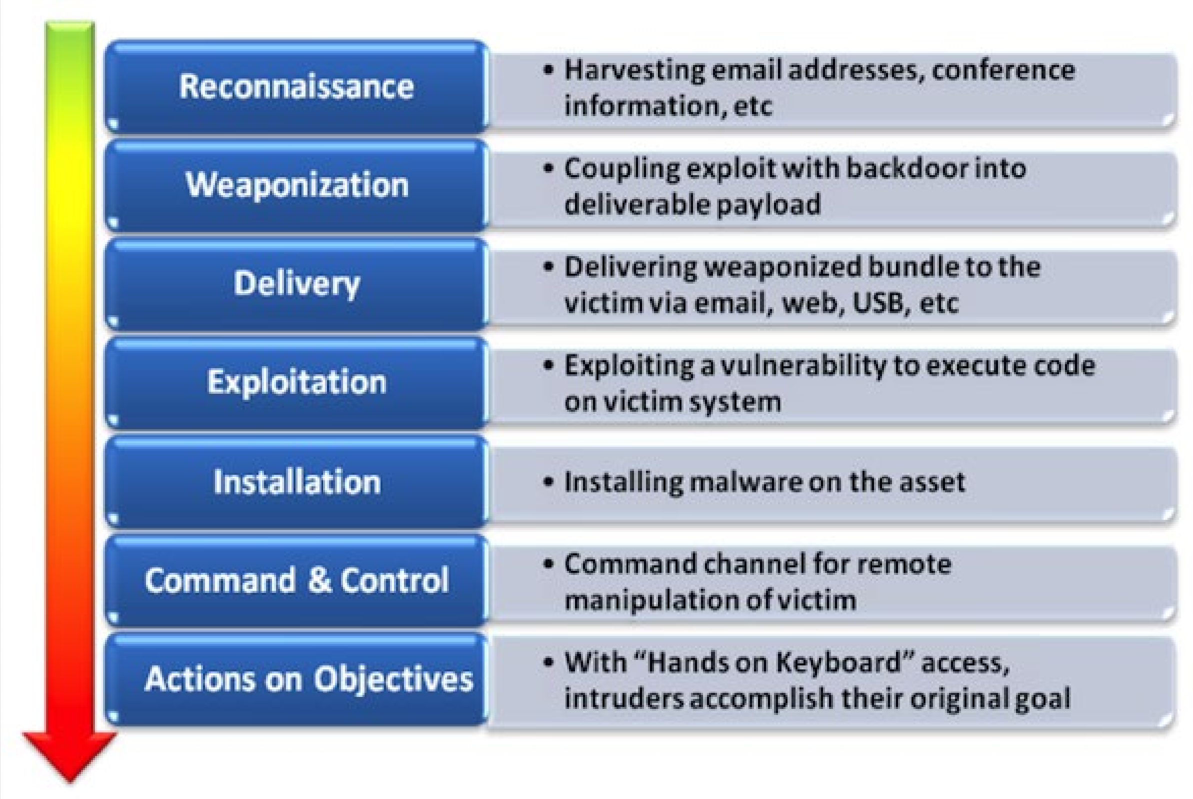
6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES

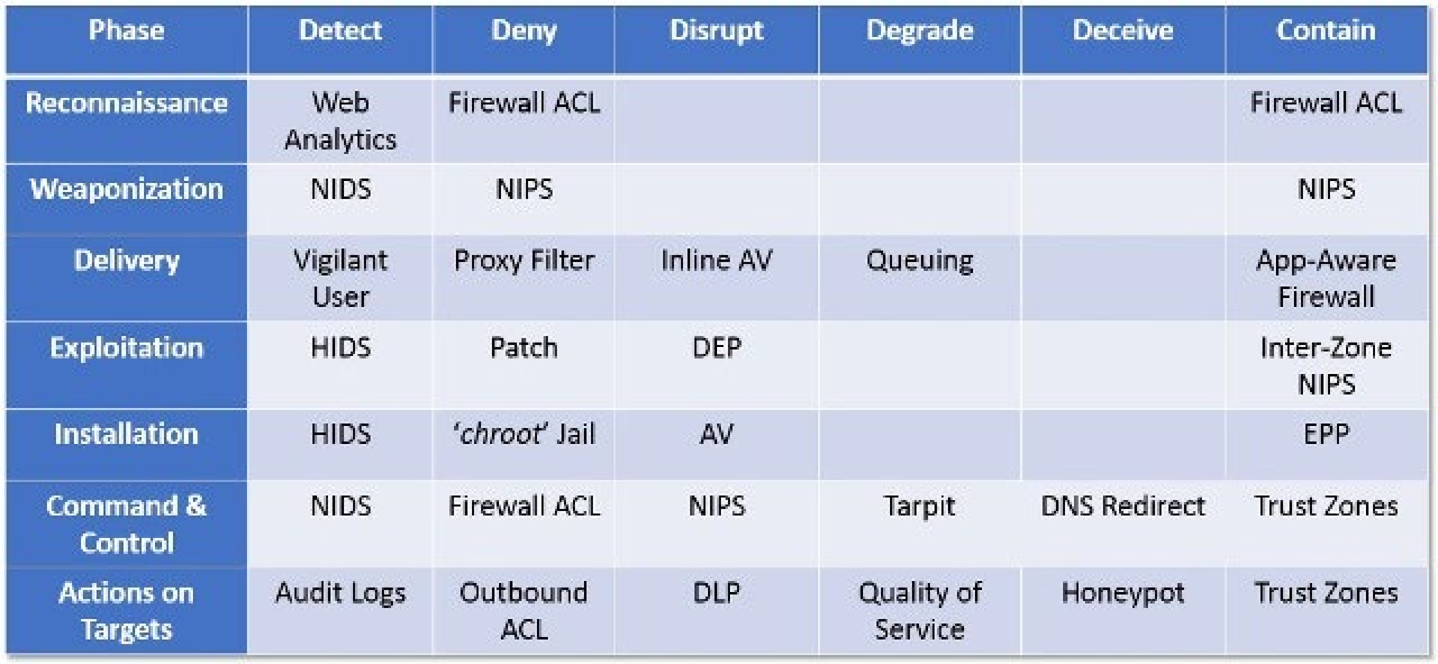
With 'Hands on Keyboard' access, intruders accomplish their original goals

Understand the Tactics and Techniques



Reconnaissance	• Harvesting email addresses, conference information, etc
Weaponization	• Coupling exploit with backdoor into deliverable payload
Delivery	• Delivering weaponized bundle to the victim via email, web, USB, etc
Exploitation	• Exploiting a vulnerability to execute code on victim system
Installation	• Installing malware on the asset
Command & Control	• Command channel for remote manipulation of victim
Actions on Objectives	• With "Hands on Keyboard" access, intruders accomplish their original goal

Layered Defense



Phase	Detect	Deny	Disrupt	Degrade	Deceive	Contain
Reconnaissance	Web Analytics	Firewall ACL				Firewall ACL
Weaponization	NIDS	NIPS				NIPS
Delivery	Vigilant User	Proxy Filter	Inline AV	Queuing		App-Aware Firewall
Exploitation	HIDS	Patch	DEP			Inter-Zone NIPS
Installation	HIDS	'*chroot*' Jail	AV			EPP
Command & Control	NIDS	Firewall ACL	NIPS	Tarpit	DNS Redirect	Trust Zones
Actions on Targets	Audit Logs	Outbound ACL	DLP	Quality of Service	Honeypot	Trust Zones

Next Lecture

- Authentication.
- Readings for next lecture:
  - Anderson’s Book – section 2.4, 2.5, 15.1, 15.3 and 15.9.