CYBR3000

# Intro to (Cyber-)Attacks

Dr Dan Kim

Associate Professor in Cybersecurity,
School of EECS
The University of Queensland, Australia
Homepage: https://researchers.uq.edu.au/researcher/23703

# Learning objectives

- At the end of this lecture, you will be able to understand/explain
  - Framework: Cyber Kill Chain (CKC), CAPEC, ATT&CK
  - Malware
  - APT attacks
  - DoS attacks

# Outline

- Frameworks
- Malware
  - Overview
  - Advanced Persistent Threat (APT attacks)
  - Propagation
    - ✓ Infected content – Viruses
    - ✓ Vulnerability exploit – Worms
    - ✓ Social Engineering – Spam E-mail, Trojans
  - Payload
    - ✓ System Corruption
    - ✓ Attack Agent – Zombie, Bots
    - ✓ Stealthing – Backdoors, Rootkits
  - Countermeasures
- DoS attacks

# The Cyber Kill Chain (CKC) framework


- ✓ Developed by Lockheed Martin
- ✓ is part of the Intelligence Driven Defense model for identification and prevention of cyber intrusions activity.
- ✓ identifies what the adversaries must complete in order to achieve their objective.
- ✓ The seven steps enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures.

# Common Attack Pattern Enumeration and Classification (CAPEC)

- A resource for identifying and understanding attacks
- View list of attack patterns by
  - Mechanisms of attack - are frequently employed when exploiting a vulnerability
  - Domains of attack

**1000 - Mechanisms of Attack**

- Engage in Deceptive Interactions - *(156)*
- Abuse Existing Functionality - *(210)*
- Manipulate Data Structures - *(255)*
- Manipulate System Resources - *(262)*
- Inject Unexpected Items - *(152)*
- Employ Probabilistic Techniques - *(223)*
- Manipulate Timing and State - *(172)*
- Collect and Analyze Information - *(118)*
- Subvert Access Control - *(225)*

**3000 - Domains of Attack**

- Software - *(513)*
- Hardware - *(515)*
- Communications - *(512)*
- Supply Chain - *(437)*
- Social Engineering - *(403)*
- Physical Security - *(514)*

- Search function is provided.
- Web: https://capec.mitre.org/

# The MITRE's ATT&CK

- the **A**dversarial **T**actics **T**echniques and **C**ommon **K**nowledge
- Tactics
  - PRE-ATT&CK, Enterprise, Mobile, ICS
  - e.g., Enterprise tactics: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact
- Techniques
  - PRE-ATT&CK, Enterprise (Windows, macOS, Linux, Cloud), Mobile (Android, iOS), ICS
  - include Possible methods of detection and mitigation for each techniques
- Mitigations
  - Enterprise, Mobile, ICS

https://attack.mitre.org/tactics/enterprise/

# Enterprise tactics

| ID | Name | Description |
|---|---|---|
| TA0043 | Reconnaissance | The adversary is trying to gather information they can use to plan future operations. |
| TA0042 | Resource Development | The adversary is trying to establish resources they can use to support operations. |
| TA0001 | Initial Access | The adversary is trying to get into your network. |
| TA0002 | Execution | The adversary is trying to run malicious code. |
| TA0003 | Persistence | The adversary is trying to maintain their foothold. |
| TA0004 | Privilege Escalation | The adversary is trying to gain higher-level permissions. |
| TA0005 | Defense Evasion | The adversary is trying to avoid being detected. |
| TA0006 | Credential Access | The adversary is trying to steal account names and passwords. |
| TA0007 | Discovery | The adversary is trying to figure out your environment. |
| TA0008 | Lateral Movement | The adversary is trying to move through your environment. |
| TA0009 | Collection | The adversary is trying to gather data of interest to their goal. |
| TA0011 | Command and Control | The adversary is trying to communicate with compromised systems to control them. |
| TA0010 | Exfiltration | The adversary is trying to steal data. |
| TA0040 | Impact | The adversary is trying to manipulate, interrupt, or destroy your systems and data. |

Source: https://attack.mitre.org/tactics/enterprise/

# Mobile Tactics

| ID | Name | Description |
|---|---|---|
| TA0027 | Initial Access | The adversary is trying to get into your device. |
| TA0041 | Execution | The adversary is trying to run malicious code. |
| TA0028 | Persistence | The adversary is trying to maintain their foothold. |
| TA0029 | Privilege Escalation | The adversary is trying to gain higher-level permissions. |
| TA0030 | Defense Evasion | The adversary is trying to avoid being detected. |
| TA0031 | Credential Access | The adversary is trying to steal account names, passwords, or other secrets that enable access to resources. |
| TA0032 | Discovery | The adversary is trying to figure out your environment. |
| TA0033 | Lateral Movement | The adversary is trying to move through your environment. |
| TA0035 | Collection | The adversary is trying to gather data of interest to their goal. |
| TA0037 | Command and Control | The adversary is trying to communicate with compromised devices to control them. |
| TA0036 | Exfiltration | The adversary is trying to steal data. |
| TA0034 | Impact | The adversary is trying to manipulate, interrupt, or destroy your devices and data. |
| TA0038 | Network Effects | The adversary is trying to intercept or manipulate network traffic to or from a device. |
| TA0039 | Remote Service Effects | The adversary is trying to control or monitor the device using remote services. |

https://attack.mitre.org/tactics/mobile/

# Outline

- Frameworks
- Malware
  - Overview
  - Advanced Persistent Threat (APT attacks)
  - Propagation
    - ✓ Infected content – Viruses
    - ✓ Vulnerability exploit – Worms
    - ✓ Social Engineering – Spam E-mail, Trojans
  - Payload
    - ✓ System Corruption
    - ✓ Attack Agent – Zombie, Bots
    - ✓ Stealthing – Backdoors, Rootkits
  - Countermeasures
- DoS attacks

# Malware – **mal**icious soft**ware**

- [SOUP13] defines **malware** as:
  - “a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim.”
- we are concerned with
  - the threat malware poses to application programs, to utility programs, such as editors and compilers, and to kernel-level programs.
  - its use on compromised or malicious Web sites and servers, or in especially crafted spam e-mails or other messages, which aim to trick users into revealing sensitive personal information.

# APT Characteristics

- **A**dvanced
  - Used by the attackers of a wide variety of intrusion technologies and malware including the development of custom malware if required
  - The individual components may not necessarily be technically advanced but are carefully selected to suit the chosen target
- **P**ersistent
  - Determined application of the attacks over an extended period against the chosen target in order to maximize the chance of success
  - A variety of attacks may be progressively applied until the target is compromised
- **T**hreats
  - Threats to the selected targets as a result of the organized, capable, and well-funded attackers intent to compromise the specifically chosen targets
  - The active involvement of people in the process greatly raises the threat level from that due to automated attacks tools, and also the likelihood of successful attacks

# APT Attacks

- Aim:
  - Varies from theft of intellectual property or security and infrastructure related data to the physical disruption of infrastructure
- Techniques used:
  - Social engineering
  - Spear-phishing email
  - **Drive-by-downloads** from selected compromised websites likely to be visited by personnel in the target organization
- Intent:
  - To infect the target with sophisticated malware with multiple propagation mechanisms and payloads
  - Once they have gained initial access to systems in the target organization a further range of attack tools are used to maintain and extend their access

# Drive-By-Downloads

- Exploits browser vulnerabilities to download and installs malware on the system when the user views a Web page controlled by the attacker
- a common exploit in recent attack kits.
- In most cases does not actively propagate
- Spreads when users visit the malicious Web page

# Outline

- Frameworks
- Malware
  - Overview
  - Advanced Persistent Threat (APT attacks)
  - Propagation
    - ✓Infected content – Viruses
    - ✓Vulnerability exploit – Worms
    - ✓Social Engineering – Spam E-mail, Trojans
  - Payload
    - ✓System Corruption
    - ✓Attack Agent – Zombie, Bots
    - ✓Stealthing – Backdoors, Rootkits
  - Countermeasures
- DoS attacks

# Viruses, Worms and Network Propagation Systems

- Viruses
  - Malicious program that spreads by infecting various files
  - When infected file is opened, virus runs its program first and then opens the (now infected) file
  - Most viruses spread by transferring infected file between computers via email attachments

# Virus Classifications

- by target
  - Boot sector infector
    - Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus
  - File infector
    - Infects files that the operating system or shell considers to be executable
  - Macro virus
    - Infects files with macro or scripting code that is interpreted by an application
  - Multipartite virus
    - Infects multiple files in multiple ways
    - e.g., **Combination of Boot Sector and File Infector**

- by concealment strategy
  - Encrypted virus
    - A portion of the virus creates a random encryption key and encrypts the remainder of the virus
  - Stealth virus
    - A form of virus explicitly designed to hide itself from detection by anti-virus software
  - Polymorphic virus
    - A virus that mutates with every infection; encrypt the virus code; have a constant virus body, being encrypted with a different decryptor each instance.
  - Metamorphic virus
    - Obfuscate the virus code; a virus that mutates and rewrites itself completely at each iteration and may change behavior as well as appearance; the body of the virus itself changes from instance to instance

http://www.cs.virginia.edu/~cs351-dada/Lectures/PolyMetamorphic.pdf

# Virus Protection

- Effective protection is anti-virus S/W which:
  - scans e-mail attachments
  - checks for virus signatures
- Examples:
  - Norton (www.norton.com)
  - McAfee (www.mcafee.com)
  - V3 (www.ahnlab.com)
  - Most of these have versions which provide “push” technology and update a customer’s site automatically

# Worms

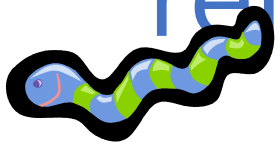
- Program that actively seeks out more machines to infect and each infected machine serves as an automated launching pad for attacks on other machines
- **Exploits software vulnerabilities** in client or server programs
- Can use network connections to spread from system to system
- Spreads through shared media (USB drives, CD, DVD data disks)
- E-mail worms spread in macro or script code included in attachments and instant messenger file transfers
- Upon activation the worm may replicate and propagate again
- Usually carries some form of payload
- First known implementation was done in Xerox Palo Alto Labs in the early 1980s

# Computer Virus vs. Worm


- Virus does not intentionally try to spread itself from that computer to other computers.
- In most cases, that's where humans come in.
- Worms is a program that is designed to copy itself from one computer to another over a network (e.g., by using e-mail).
- The worm spreads itself to many computers over a network

http://www.symantec.com/avcenter/reference/worm.vs.virus.pdf

# Worm Replication – means to access remote systems



| | |
|---|---|
| Electronic mail or instant messenger facility | • Worm e-mails a copy of itself to other systems<br>• Sends itself as an attachment via an instant message service |
| File sharing | • Creates a copy of itself or infects a file as a virus on removable media |
| Remote execution capability | • Worm executes a copy of itself on another system |
| Remote file access or transfer capability | • Worm uses a remote file access or transfer service to copy itself from one system to the other |
| Remote login capability | • Worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other |

# Target Discovery - network address scanning strategies

- Scanning (or fingerprinting)
  - First function in the propagation phase for a network worm
  - Searches for other systems to infect

**Random**

- Each compromised host probes *random* addresses in the IP address space using a different seed
- This produces a high volume of Internet traffic which may cause generalized disruption even before the actual attack is launched

**Hit-list**

- The attacker first compiles a long list of potential vulnerable machines
- Once the list is compiled the attacker begins infecting machines on the list
- Each infected machine is provided with a portion of the list to scan
- This results in a very short scanning period which may make it difficult to detect that infection is taking place

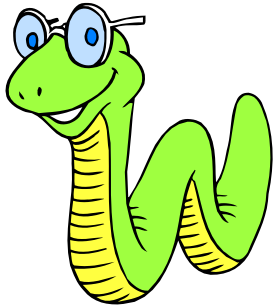
**Topological**

- This method uses information contained on an infected victim machine to find more hosts to scan

**Local subnet**

- If a host can be infected behind a firewall that host then looks for targets in its own local network
- The host uses the subnet address structure to find other hosts that would otherwise be protected by the firewall
- Code Red II and Nimda worms

# Morris Worm



- Earliest significant worm infection
- Released by Robert Morris in 1988
- Designed to spread on UNIX systems (OR cases)
  - It attempted to log on to a remote host as a legitimate user: Attempted to crack local password file to use login/password to logon to other systems
  - It exploited a bug in the finger protocol which reports the whereabouts of a remote user
  - It exploited a trapdoor in the debug option of the remote process that receives and sends mail
- Successful attacks achieved communication with the operating system command interpreter
  - Sent interpreter a bootstrap program to copy worm over
  - The bootstrap program then called back the parent program and downloaded the remainder of the worm.
  - The new worm was then executed.

# Worm Attacks (examples)

| Name | Appeared in | Description |
|---|---|---|
| Melissa<br>Melissa variant | 1998<br>1999 | e-mail worm (Microsoft Word macro embedded in an attachment)<br>first to include virus, worm and Trojan in one package<br>If the recipient open the e-mail attachment, the Word macro is activated. It sends itself to everyone on the mailing list.<br>Melissa variant: activated merely by opening an email that contains the virus, rather than by opening an attachment.<br>3 days for Melissa to infect over 100K computers. |
| Code Red | July 2001 | exploited Microsoft Internet Information Server (IIS) bug for which a patch had been available a month earlier; it disables the system file checker in Windows OS.<br>probes random IP addresses<br>consumes significant Internet capacity when active (by flooding the site with packets from numerous hosts) – over 360 K servers in 14 hrs. |
| Code Red II | August 2001 | also targeted Microsoft IIS with a different payload;<br>pseudo-randomly chose targets on the same or different subnets<br>installs a backdoor for access |
| Nimda | September 2001 | had worm, virus and mobile code characteristics<br>spread using e-mail, Windows file shares, Web servers (MS IIS), Web clients, backdoors access |
| SQL Slammer | Early 2003 | exploited a buffer overflow vulnerability in MS SQL server<br>compact and spread rapidly (infecting 90% of vulnerable hosts within 10 minutes) |
| Sobig.F | Late 2003 | exploited open proxy servers to turn infected machines into spam engines |
| Mydoom | 2004 | mass-mailing e-mail worm<br>installed a backdoor in infected machines |
| Warezov | 2006 | creates executables in system directories; sends itself as an e-mail attachment; can disable security related products |
| Conficker (Downadup) | November 2008 | exploits a Windows buffer overflow vulnerability<br>most widespread infection since SQL Slammer |
| Stuxnet | 2010 | restricted rate of spread to reduce chance of detection<br>targeted industrial control systems |

# An example: Slammer worm

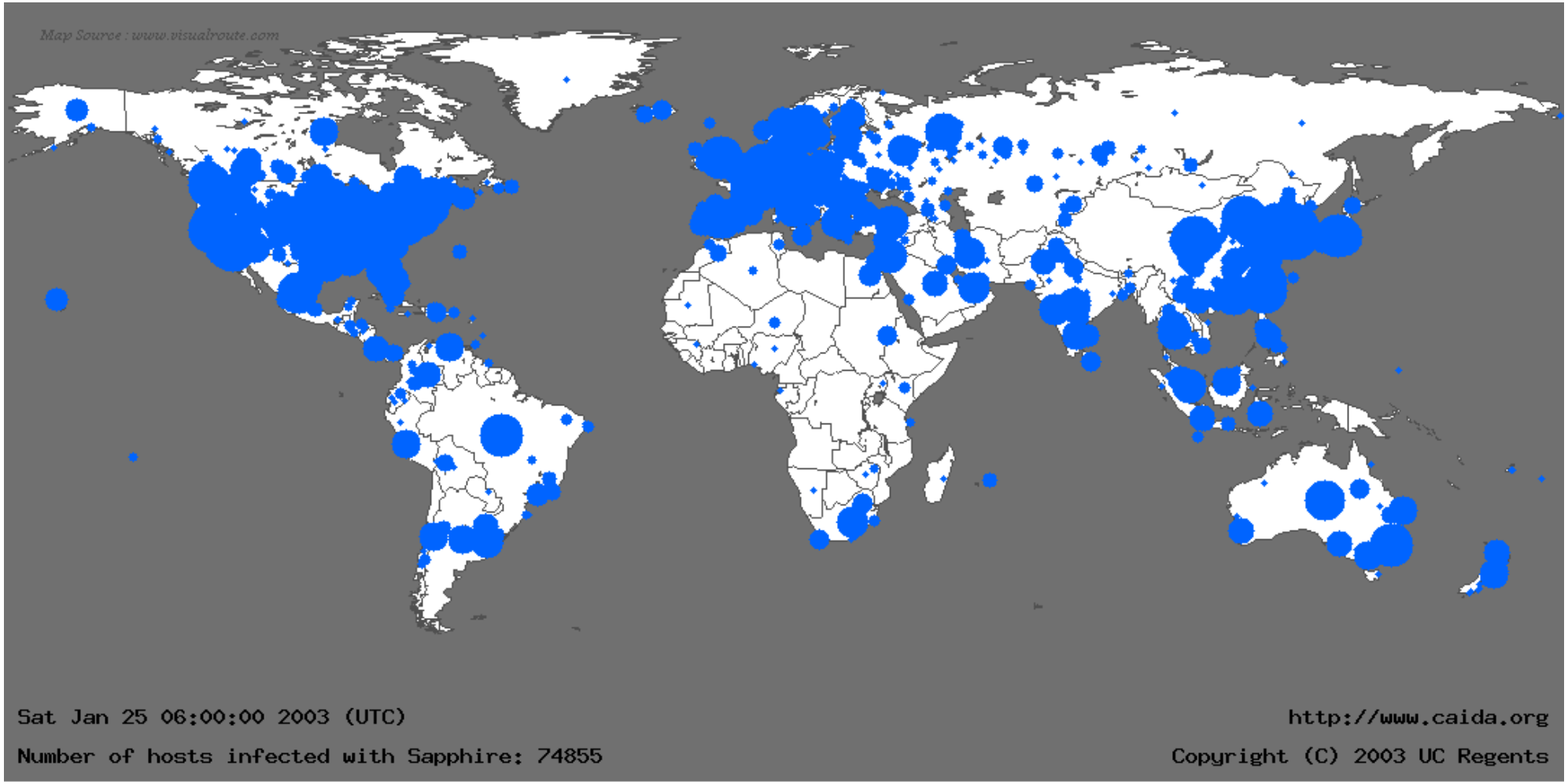
- W32.Slammer Overview
  - Aliases: SQL Slammer, Saphire, W32.SQLExp.Worm
  - Released:  January 25, 2003, at about 5:30 a.m. (GMT)
  - Fastest worm in history: Spread world-wide in under 10 minutes
  - Doubled infections every 8.5 seconds
  - Size: 376 bytes long

# Slammer worm (cont.)

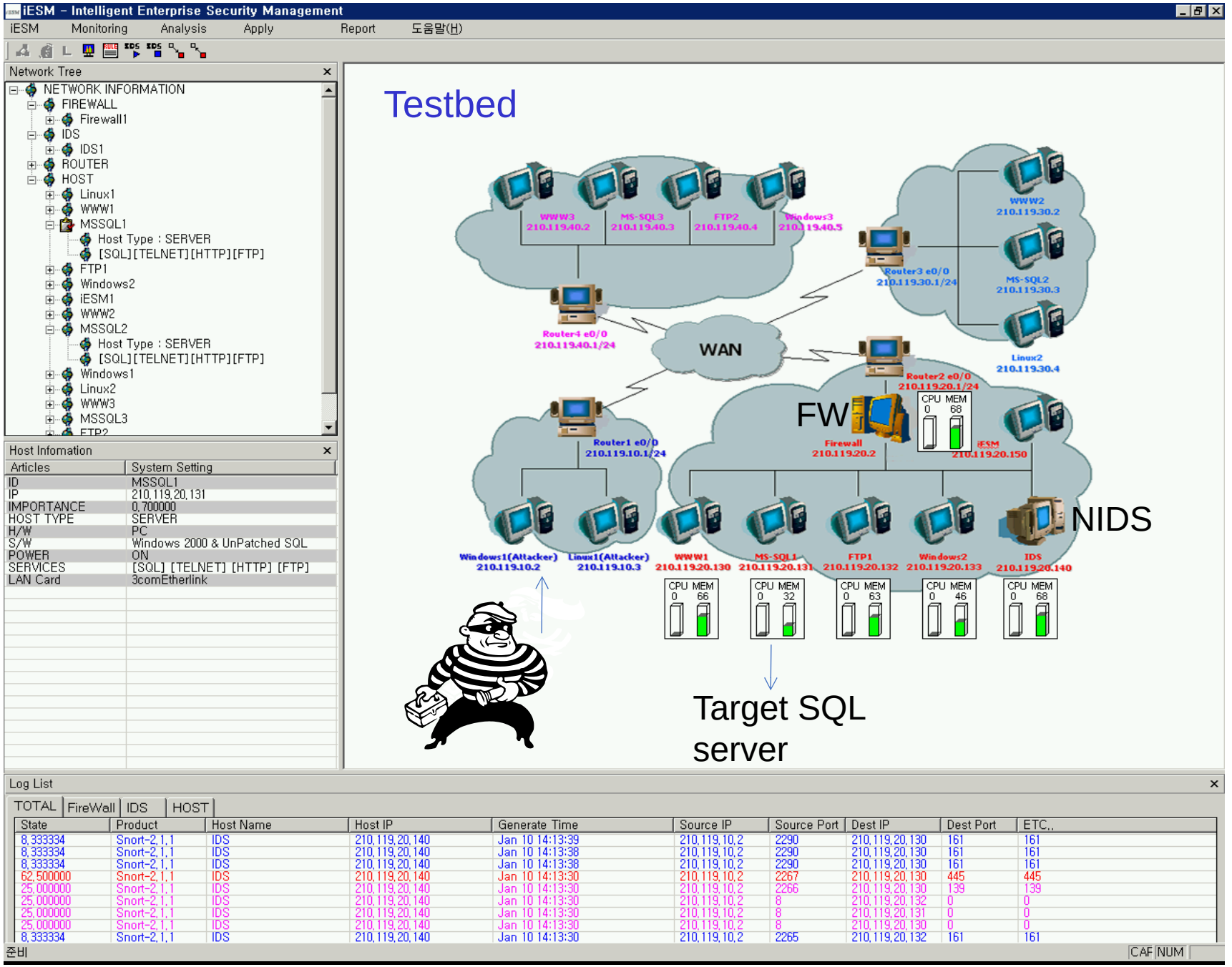
- Propagation Technique
  - Single UDP packet
  - Targets port 1434 (Microsoft-SQL-Monitor)
  - Causes buffer overflow
  - Continuously sends itself via UDP packets to pseudo-random IP addresses, including broadcast and multicast addresses
  - Does not check whether target machines exist

# Slammer worm (cont.)

- Infections 30 Minutes After Release




Source: http://www.caida.org/analysis/security/sapphire/


iESM – Intelligent Enterprise Security Management
iESM Monitoring Analysis Apply Report 도움말(H)
Network Tree
NETWORK INFORMATION
FIREWALL
Firewall1
IDS
IDS1
ROUTER
HOST
Linux1
WWW1
MSSQL1
Host Type : SERVER
[SQL][TELNET][HTTP][FTP]
FTP1
Windows2
iESM1
WWW2
MSSQL2
Host Type : SERVER
[SQL][TELNET][HTTP][FTP]
Windows1
Linux2
WWW3
MSSQL3
Host Infomation
Articles System Setting
ID MSSQL1
IP 210,119,20,131
IMPORTANCE 0.700000
HOST TYPE SERVER
H/W PC
S/W Windows 2000 & UnPatched SQL
POWER ON
SERVICES [SQL] [TELNET] [HTTP] [FTP]
LAN Card 3comEtherlink
Testbed
WWW3 210.119.40.2
MS-SQL3 210.119.40.3
FTP2 210.119.40.4
Windows3 210.119.40.5
Router4 e0/0 210.119.40.1/24
WAN
Router3 e0/0 210.119.30.1/24
WWW2 210.119.30.2
MS-SQL2 210.119.30.3
Linux2 210.119.30.4
Router2 e0/0 210.119.20.1/24
FW
Firewall 210.119.20.2
iESM 210.119.20.150
Router1 e0/0 210.119.10.1/24
Windows1(Attacker) 210.119.10.2
Linux1(Attacker) 210.119.10.3
WWW1 210.119.20.130
MS-SQL1 210.119.20.131
FTP1 210.119.20.132
Windows2 210.119.20.133
IDS 210.119.20.140
CPU MEM
NIDS
Target SQL server
Log List
TOTAL FireWall IDS HOST
State Product Host Name Host IP Generate Time Source IP Source Port Dest IP Dest Port ETC..
8.333334 Snort-2.1.1 IDS 210.119.20.140 Jan 10 14:13:39 210.119.10.2 2290 210.119.20.130 161 161
8.333334 Snort-2.1.1 IDS 210.119.20.140 Jan 10 14:13:38 210.119.10.2 2290 210.119.20.130 161 161
8.333334 Snort-2.1.1 IDS 210.119.20.140 Jan 10 14:13:38 210.119.10.2 2290 210.119.20.130 161 161
62.500000 Snort-2.1.1 IDS 210.119.20.140 Jan 10 14:13:30 210.119.10.2 2267 210.119.20.130 445 445
25.000000 Snort-2.1.1 IDS 210.119.20.140 Jan 10 14:13:30 210.119.10.2 2266 210.119.20.130 139 139
25.000000 Snort-2.1.1 IDS 210.119.20.140 Jan 10 14:13:30 210.119.10.2 8 210.119.20.132 0 0
25.000000 Snort-2.1.1 IDS 210.119.20.140 Jan 10 14:13:30 210.119.10.2 8 210.119.20.131 0 0
25.000000 Snort-2.1.1 IDS 210.119.20.140 Jan 10 14:13:30 210.119.10.2 8 210.119.20.130 0 0
8.333334 Snort-2.1.1 IDS 210.119.20.140 Jan 10 14:13:30 210.119.10.2 2265 210.119.20.132 161 161
준비
CAP NUM

Vul. scan for a SQL server

monitoring the network

# Worm Countermeasures

- Considerable overlap in techniques for dealing with viruses and worms
- Once a worm is resident on a machine anti-virus software can be used to detect and possibly remove it
- Perimeter network activity and usage monitoring can form the basis of a worm defense
- Worm defense approaches include:
  - **Signature**-based worm scan filtering: approach generates a worm signature
  - Filter-based worm containment: focuses on worm content; collaborative worm detection at end hosts
  - Payload-classification-based worm containment: looks for exploit code in network flows
  - Threshold random walk (TRW) scan detection: exploit randomness in picking destinations
    - ✓ e.g., Scan Detection Algorithm based on sequential hypothesis testing.
  - Rate limiting: limits the rate of scan-like traffic from an infected host.
  - Rate halting: : This approach immediately blocks outgoing traffic when a threshold is exceeded either in outgoing connection rate or in diversity of connection attempts

# Outline

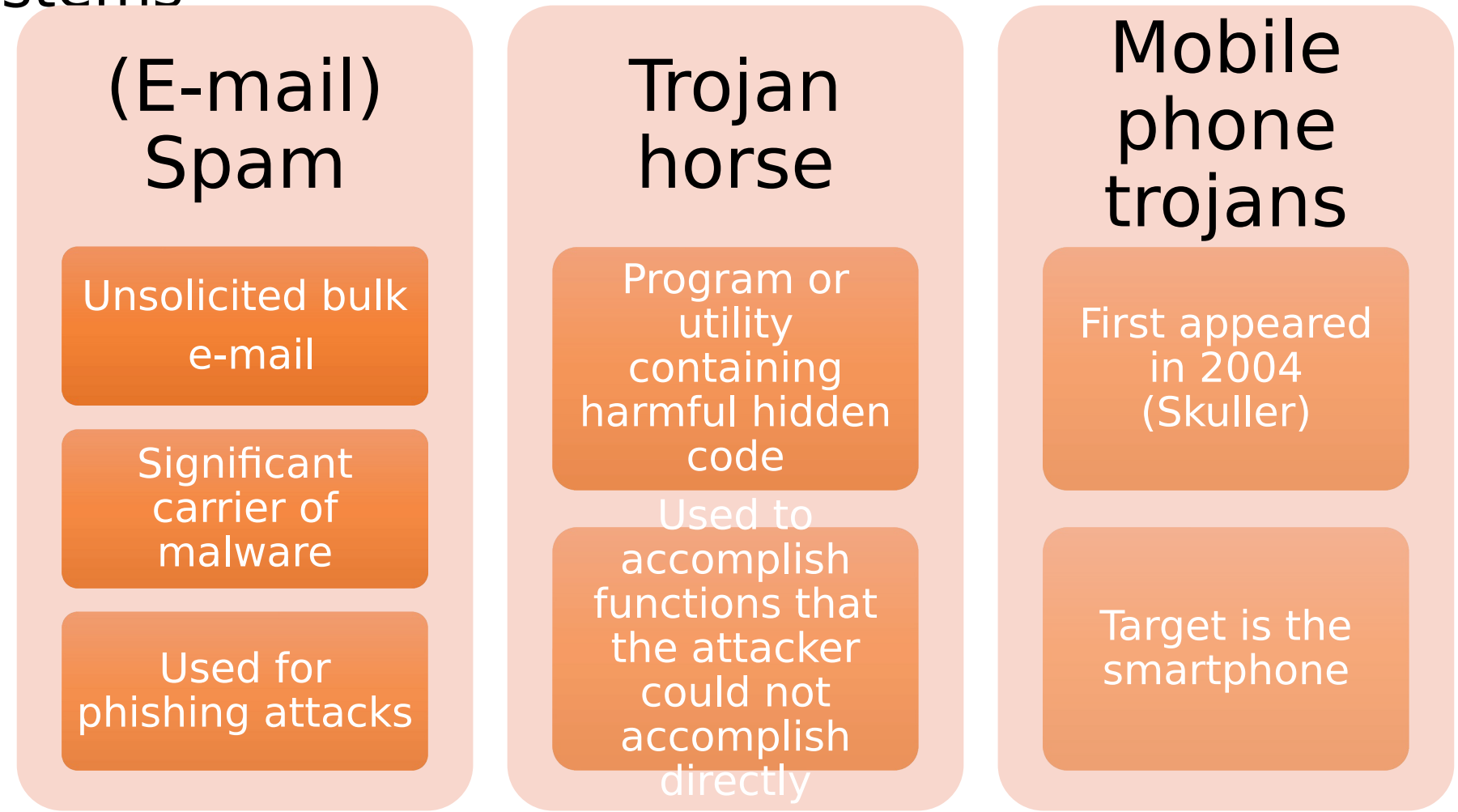
- Frameworks
- Malware
  - Overview
  - Advanced Persistent Threat (APT attacks)
  - Propagation
    - ✓ Infected content – Viruses
    - ✓ Vulnerability exploit – Worms
    - ✓ Social Engineering – Spam E-mail, Trojans
  - Payload
    - ✓ System Corruption
    - ✓ Attack Agent – Zombie, Bots
    - ✓ Stealthing – Backdoors, Rootkits
  - Countermeasures
- DoS attacks

# Social Engineering - examples

- Persuade someone to disclose sensitive information (e.g. Phishing attacks on bank customers, etc.)
- Persuade someone to run/install malicious or subverted software
- Invite someone to log into a bogus web site such as a spoofed bank web site
- Impersonating new employee who has forgotten user ID/password
- Impersonating a technical support staff member and requesting a user login to ‘check’ accounts

# Social Engineering

- “Tricking” users to assist in the compromise of their own systems



# Social Engineering - Phishing

- Phishing (electronic fishing) attacks - mass distribution of 'spoofed' e-mail
  - Appears to come from banks, insurance agencies, retailers or credit card companies
  - e-mail messages that guide recipients to legitimate-looking but fake Web sites and try to get them to supply personal information like account passwords.
  - Because these emails look “official”, up to 5% of recipients may respond, resulting in financial losses, theft etc.

# Phishing Attack – Example

**Westpak  Australia's First Bank**

No offense to Westpak

Dear client of the Westpak Bank,

The recent cases of fraudulent use of clients accounts forced the Technical services of the bank to update the software. We regret to acknowledge, that some data on users accounts could be lost. The administration kindly asks you to follow the reference given below and to sign in to your online banking account:

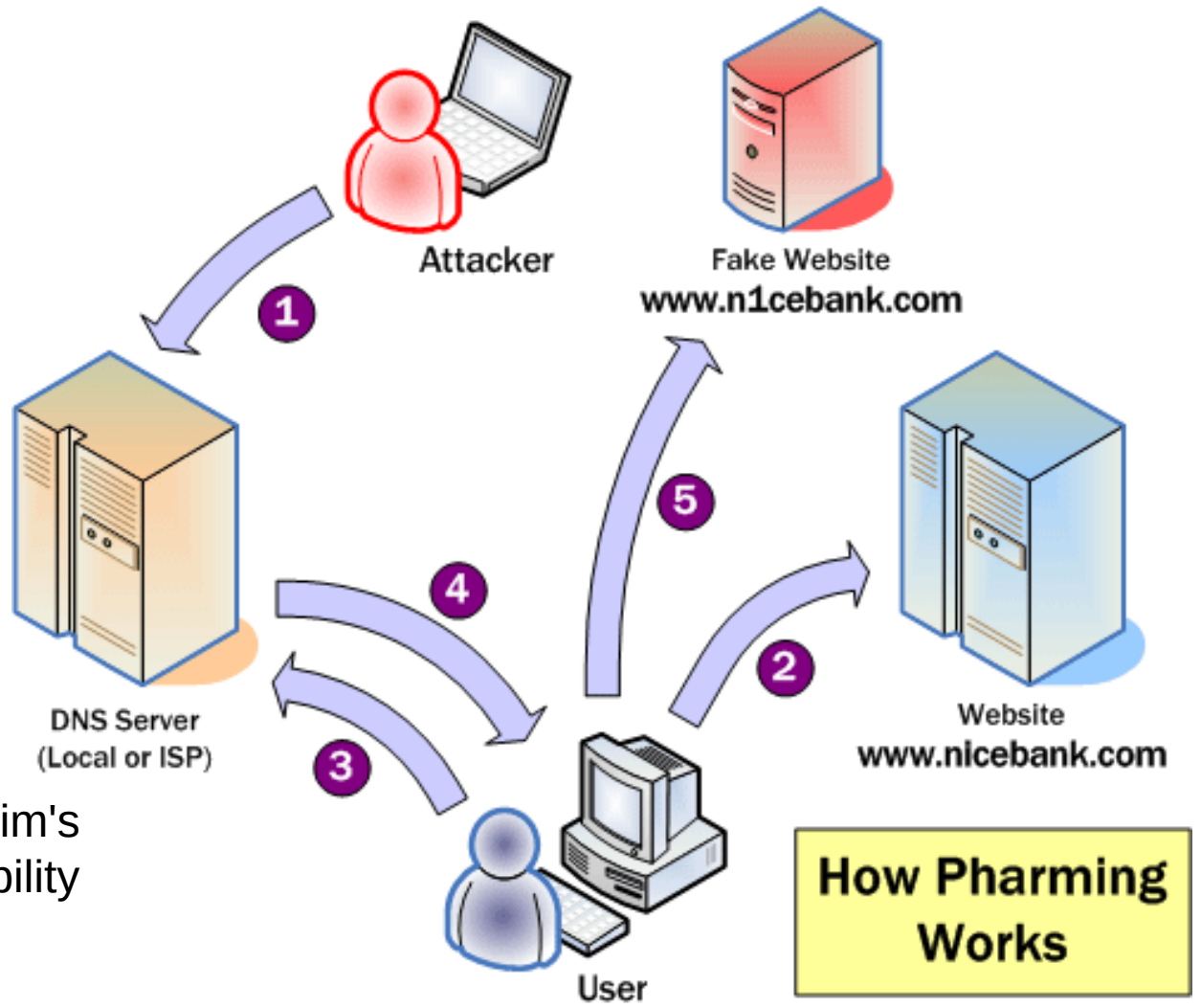
https://oIb.westpak.com.au/ib/defaulI.asp

We are grateful for your cooperation.

# Social Engineering - Pharming

- is a hacker's attack aiming to redirect a website's traffic to another (bogus) website, even though the browser seems to be displaying the Web address you wanted to visit.
- **tampers with the domain-name server (DNS)** system so that traffic to a Web site is secretly redirected to a different site altogether,
- has become of major concern to businesses hosting E-commerce and online banking websites

# Pharming - example

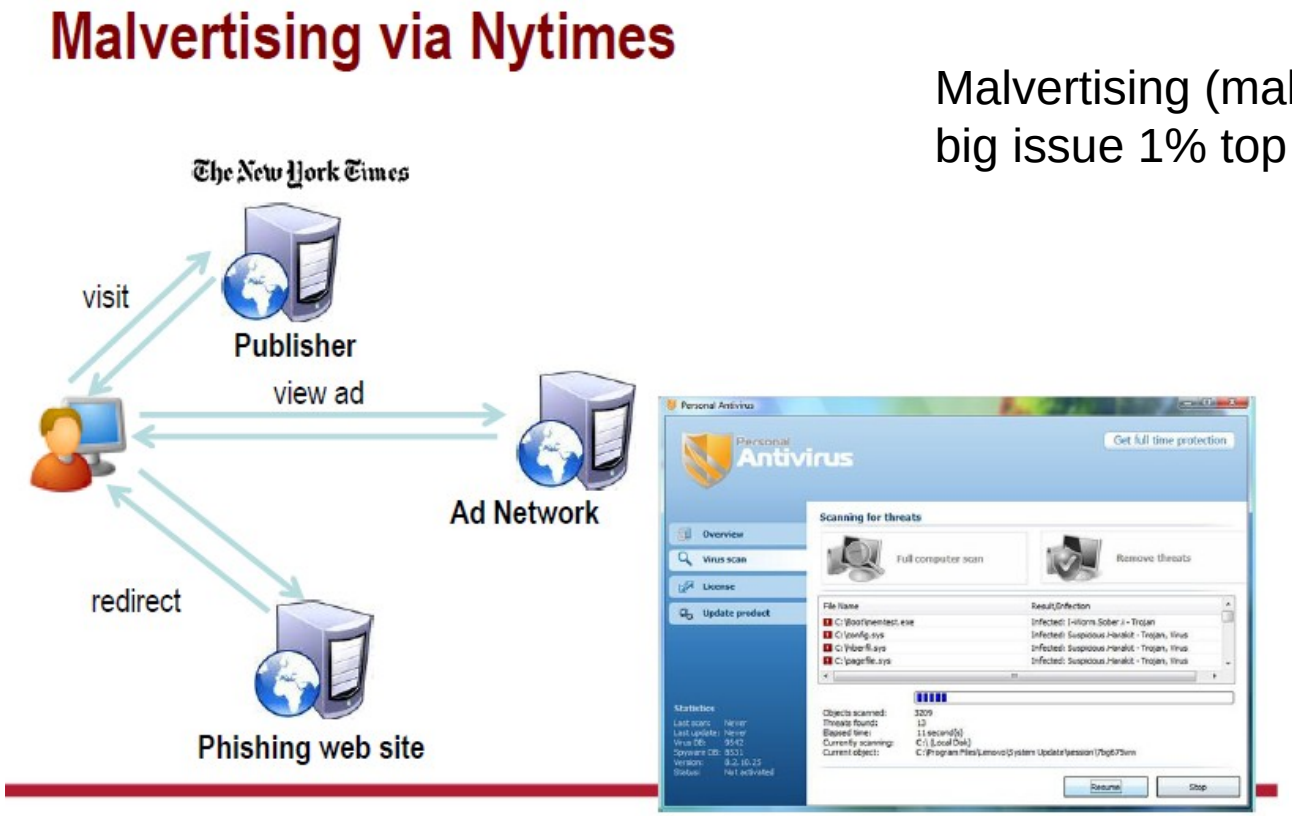



by changing the hosts file on a victim's computer or by exploitation of a vulnerability in **DNS** server software

http://palpapers.plynt.com/images/pharming-diagram.png

# Malvertising

- used to place malware on websites without actually compromising them




Malvertising (malicious advertising ) is a big issue 1% top publishers are infected

**e.g., PDF malware, popup ads, Drive-by download, drive-by install**

Source: X. Wang, MS faculty summit 2012

# Outline

- Frameworks
- Malware
  - Overview
  - Advanced Persistent Threat (APT attacks)
  - Propagation
    - ✓ Infected content – Viruses
    - ✓ Vulnerability exploit – Worms
    - ✓ Social Engineering – Spam E-mail, Trojans
  - Payload
    - ✓ System Corruption
    - ✓ Attack Agent – Zombie, Bots
    - ✓ Stealthing – Backdoors, Rootkits
  - Countermeasures
- DoS attacks

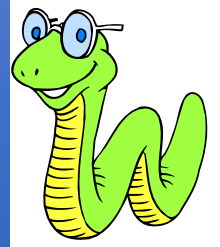
# Payload System Corruption - Data

## Chernobyl virus

- First seen in 1998
- Windows 95 and 98 **virus**
- Infects executable files and corrupts the entire file system when a trigger date (April 26, 1999) is reached
- Destorying data: Deletes data on the infected system by overwriting the first megabyte of the HDD with 0s
- > 1 M computers affected

## Klez

- Mass mailing **worm** infecting Windows 95 to XP systems
- First seen in October 2001
- Spreads by emailing copies of itself to addresses found in the address book and in files on the system
- Can stop and delete some anti-virus programs
- Destroying data: On trigger date causes files on the hard drive to



## Ransomware

- Encrypts the user's data and demands payment in order to access the key needed to recover the information
- PC Cyborg Trojan (1989)
- Gpcode Trojan (2006)
- The user needed to pay a ransom, or to make a purchase from certain sites, in order to receive the key to decrypt this data.

# Ransomware


- Ransom + Ware (software)
- A major ransomware attack has affected many organizations across the world reportedly including Telefonica in Spain, the National Health Service in the UK, and FedEx in the US.
- The malware responsible for this attack is a ransomware variant known as 'WannaCry'.
- scan heavily over TCP port 445 (Server Message Block/SMB), spreading similar to a worm, compromising hosts, encrypting files stored on them then demanding a ransom payment in the form of Bitcoin

http://blog.talosintelligence.com/2017/05/wannacry.html?m=1


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 12:36:07
Time Left
02:23:58:49
Your files will be lost on
5/19/2017 12:36:07
Time Left
06:23:58:49
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt

# Ransomware

- a type of malware that prevents users from being able to use their device until a specified ransom is paid
- can generally be split into two modes of malicious operation: 1) locker-ransomware and 2) crypto-ransomware
- Locker-ransomware
  - prevents a user from using their devices by locking a component of their system (i.e., screen, browser, Master Boot Record)
  - more commonly targets mobile devices because it is harder on these devices to bypass a locking attack then it is on a PC
- Crypto-ransomware
  - uses cryptography to encrypt a victim’s files to force them into a paying a ransom
  - apply a hybrid cryptographic approach by using a symmetric key to encrypt user data and then an asymmetric public key to encrypt the symmetric key

# Ransomware

- Crypto-ransomware - two different encryption models

1. only targets valuable information based on its file extension

2. encrypt all user files regardless of extension

# Hackers hit San Francisco transport systems

- The hackers have made a ransom demand of 100 Bitcoin, which amounts to about $70,000 (£56,000 ; €66,000).
- As a precaution, staff shut off all ticketing machines on the network.
- Computers across the city’s transport network, including at stations, were disabled with screens displaying a message from the attackers.
- The message read: "You Hacked, ALL Data Encrypted. Contact For Key(cryptom27@yandex.com)ID:681 ,Enter”.
- Yandex is a Russian internet company that, among other things, provides email and social networking tools.
- The trains themselves were not affected - and city officials said a full investigation was underway.
- **'2,000 machines hacked'**

http://www.bbc.com/news/technology-38127096

# Some news

- High-impact ransomware attacks, such as the one which targeted Colonial Oil in May 2021 and took a major US fuel pipeline offline, are obviously dangerous to the continuity of vital services.

- In January 2023, there was a ransomware attack on the Royal Mail in the UK that led to the suspension of international deliveries. It took over a month for service levels to get back to normal. This attack would have had a significant direct impact on the Royal Mail's revenue and reputation.

- ALPHV ransomware gang targets Melbourne pathology firm TissuPath
  - NEWS04 Sep 2023

- Hackers Attacking MSSQL Servers To Deploy Ransomware
  - Threat actors have been utilizing brute force attacks to compromise exposed MSSQL databases to distribute the FreeWorld ransomware.

# Payload System Corruption – Physical Equipment damage

- Real-world damage: Causes damage to physical equipment
  - Chernobyl virus not only corrupts data but attempts to rewrite BIOS code
  - Stuxnet worm Targets specific industrial control system software
    - ✓ the worm replaces the original control code with code that deliberately drives the controlled equipment outside its normal operating range, resulting in the failure of the attached equipment.
  - There are concerns about using sophisticated targeted malware for industrial sabotage
- A key component of data corrupting malware is the logic bomb
  - Code embedded in the malware that is set to “explode” when certain conditions are met
  - Examples of conditions: a particular day of the week or date, a particular version or configuration of some software, or a particular user running the application.
  - Once triggered, a bomb may alter or delete data or entire files, cause a machine halt, or do some other damage.

# Outline

- Frameworks
- Malware
  - Overview
  - Advanced Persistent Threat (APT attacks)
  - Propagation
    - ✓ Infected content – Viruses
    - ✓ Vulnerability exploit – Worms
    - ✓ Social Engineering – Spam E-mail, Trojans
  - Payload
    - ✓ System Corruption
    - ✓ Attack Agent – Zombie, Bots
    - ✓ Stealthing – Backdoors, Rootkits
  - Countermeasures
- DoS attacks

# Payload – Information Theft: Keyloggers and Spyware

- consider payloads where the malware gathers data stored on the infected system for use by the attacker.
  - A common target is the user's login and password credentials to banking, gaming, and related sites, which the attacker then uses to impersonate the user to access these sites for gain.
- How?
- Keylogger
  - Captures keystrokes to allow attacker to monitor sensitive information
  - Typically uses some form of filtering mechanism that only returns information close to keywords ("login", "password")
  - Countermeasure: e.g., a graphical applet
- (general) Spyware
  - Subverts the compromised machine to allow monitoring of a wide range of activity on the system
    - ✓ Monitoring history and content of browsing activity
    - ✓ Redirecting certain Web page requests to fake sites
    - ✓ Dynamically modifying data exchanged between the browser and certain Web sites of interest
    - ✓ e.g., Zeus banking Trojan: steals banking and financial credentials using both a key logger and capturing and possibly altering form data for certain web sites

# Payload – Attack Agents/Bots

- Malware subverts the computational and network resources of the infected system for use by the attacker.
- Takes over another Internet attached computer and uses that computer to launch or manage attacks
- Botnet - collection of bots capable of acting in a coordinated manner
- Uses:
  - Distributed denial-of-service (DDoS) attacks
  - Spamming
  - Sniffing traffic: used to retrieve sensitive information like usernames and passwords.
  - Keylogging: without decrypting encrypted messages, attackers can retrieve sensitive info.
  - Spreading new malware
  - Installing advertisement add-ons and browser helper objects (BHOs)
  - Attacking Internet Relay Chat (IRC) chat networks
  - Manipulating online polls/games
  - …

# Payload – Information Theft Phishing

- Exploits social engineering to leverage the user's trust by masquerading as communication from a trusted source
  - Include a URL in a spam e-mail that links to a fake Web site that mimics the login page of a banking, gaming, or similar site
  - Suggests that urgent action is required by the user to authenticate their account
  - Attacker exploits the account using the captured credentials

- Spear-phishing
  - Recipients are carefully researched by the attacker
  - E-mail is crafted to specifically suit its recipient, often quoting a range of information to convince them of its authenticity

# Payload – (Stealthing) Backdoor

- hide its presence on the infected system, and to provide covert access to that system.
- Also known as a trapdoor
- Secret entry point into a program allowing the attacker to gain access and bypass the security access procedures
- Maintenance hook is a backdoor used by Programmers to debug and test programs
- Difficult to implement operating system controls for backdoors in applications

# Payload – (Stealthing) Rootkit

- Is a set of hidden programs installed on a system to maintain covert access to that system
- Hides by subverting the mechanisms that monitor and report on the processes, files, and registries on a computer
- Gives administrator (or root) privileges to attacker
  - Can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand

# An example of rootkit

- **Sony BMG copy protection rootkit scandal**
  - First4Internet XCP copy protection software
  - design flaw in Sony's web-based uninstaller
    - ✓CodeSupport to download and run code from URL

https://freedom-to-tinker.com/blog/felten/sonys-web-based-uninstaller-opens-big-security-hole-sony-recall-discs/

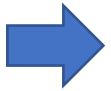
# Malware Countermeasure Approaches

- Ideal solution to the threat of malware is prevention
  - Do not allow malware to get into the system in the first place,
  - or block the ability of it to modify the system.
  - This goal is, in general, nearly impossible to achieve
- Four main elements of prevention:
  - Policy – to implement appropriate preventative countermeasures (patches; access controls on the apps and data)
  - Awareness and training – for social engineering
  - Vulnerability mitigation
  - Threat mitigation
- If prevention fails, technical mechanisms can be used to support the following threat mitigation options:
  - Detection - Once the infection has occurred, determine that it has occurred and locate the malware.
  - Identification - Once detection has been achieved, identify the specific malware that has infected the system.
  - Removal - Once the specific malware has been identified, remove all traces of malware virus from all infected systems so that it cannot spread further.

# Outline

- Frameworks
- Malware
  - Overview
  - Advanced Persistent Threat (APT attacks)
  - Propagation
    - ✓ Infected content – Viruses
    - ✓ Vulnerability exploit – Worms
    - ✓ Social Engineering – Spam E-mail, Trojans
  - Payload
    - ✓ System Corruption
    - ✓ Attack Agent – Zombie, Bots
    - ✓ Stealthing – Backdoors, Rootkits
  - Countermeasures
- DoS/DDoS attacks

# DoS - Outline



- Denial-of-service attacks
- Flooding attacks
- Distributed denial-of-service attacks
- Application-based bandwidth attacks
- Reflector and amplifier attacks
- Defenses against DoS attacks

# Denial-of-Service (DoS) Attack

- The NIST Computer Security Incident Handling Guide defines a DoS attack as:
  - “An action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space.”

# Denial-of-Service (DoS)

- A form of attack on the availability of some service
- Categories of resources that could be attacked are:

**Network bandwidth**

Relates to the capacity of the network links connecting a server to the Internet

For most organizations this is their connection to their Internet Service Provider (ISP)

**System resources**

Aims to overload or crash the network handling software

**Application resources**

Typically involves a number of valid requests, each of which consumes significant resources, thus limiting the ability of the server to respond to requests from other users

# Outline

- Denial-of-service attacks
- Flooding attacks
- Distributed denial-of-service attacks
- Application-based bandwidth attacks
- Reflector and amplifier attacks
- Defenses against DoS attacks

# Flooding Attacks

- Classified based on network protocol used
- Intent is to overload the network capacity on some link to a server
- Virtually any type of network packet can be used

**ICMP flood**

- **Ping flood using ICMP echo request packets**
- **Traditionally network administrators allow such packets into their networks because ping is a useful network diagnostic tool**

**UDP flood**

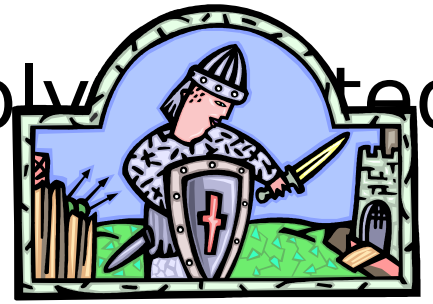
- **Uses UDP packets directed to some port number on the target system**

**TCP SYN flood**

- **Sends TCP packets to the target system**
- **Total volume of packets is the aim of the attack rather than the system code**

# Classic DoS Attacks

- Flooding ping command
  - Aim of this attack is to overwhelm the capacity of the network connection to the target organization
  - Traffic can be handled by higher capacity links on the path, but packets are discarded as capacity decreases
  - Source of the attack is clearly identified unless a spoofed address is used
  - Network performance is noticeably affected



# Source Address Spoofing

- Use forged source addresses
  - Usually via the raw socket interface on operating systems
  - Makes attacking systems harder to identify
- Attacker generates large volumes of packets that have the target system as the destination address
- Congestion would result in the router connected to the final, lower capacity link
- Requires network engineers to specifically query flow information from their routers
- Backscatter (i.e. deflection) traffic
  - The ICMP echo response packets generated in response to a ping flood using randomly spoofed source addresses is a good example.
  - Advertise routes to unused IP addresses to monitor attack traffic

# SYN Spoofing

- Common DoS attack
- Attacks the ability of a server to respond to future connection requests by overflowing the tables used to manage them
- Thus, legitimate users are denied access to the server
- Hence an attack on system resources, specifically the network handling code in the operating system

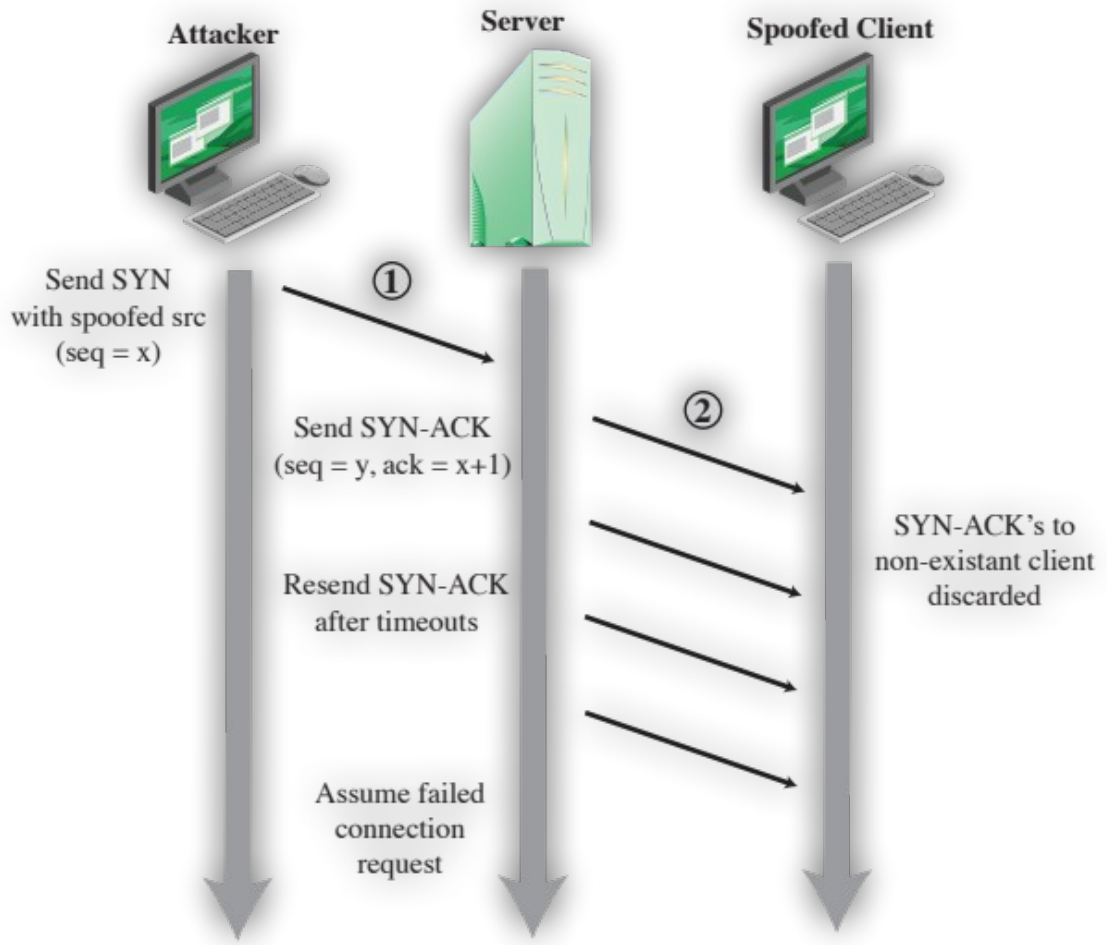



**Figure7.3 TCP SYN Spoofing Attack**

# TCP SYN spoofing attacks

- A SYN spoofing attack exploits this behavior on the targeted server system.
- The attacker generates a number of SYN connection request packets with forged source addresses.
  - For each of these the server records the details of the TCP connection request and sends the SYN-ACK packet to the claimed source address, as shown in Figure 7.3 .
  - If there is a valid system at this address, it will respond with a **RST** (reset) packet to cancel this unknown connection request.
  - When the server receives this packet, it cancels the connection request and removes the saved information.
  - However, if the source system is too busy, or there is no system at the forged address, then no reply will return.
  - In these cases, the server will resend the SYN-ACK packet a number of times before finally assuming the connection request has failed and deleting the information saved concerning it.
- In this period between when the original SYN packet is received and when the server assumes the request has failed, the server is using an entry in its table of known TCP connections.
- This table is typically sized on the assumption that most connection requests quickly succeed and that a reasonable number of requests may be handled simultaneously.

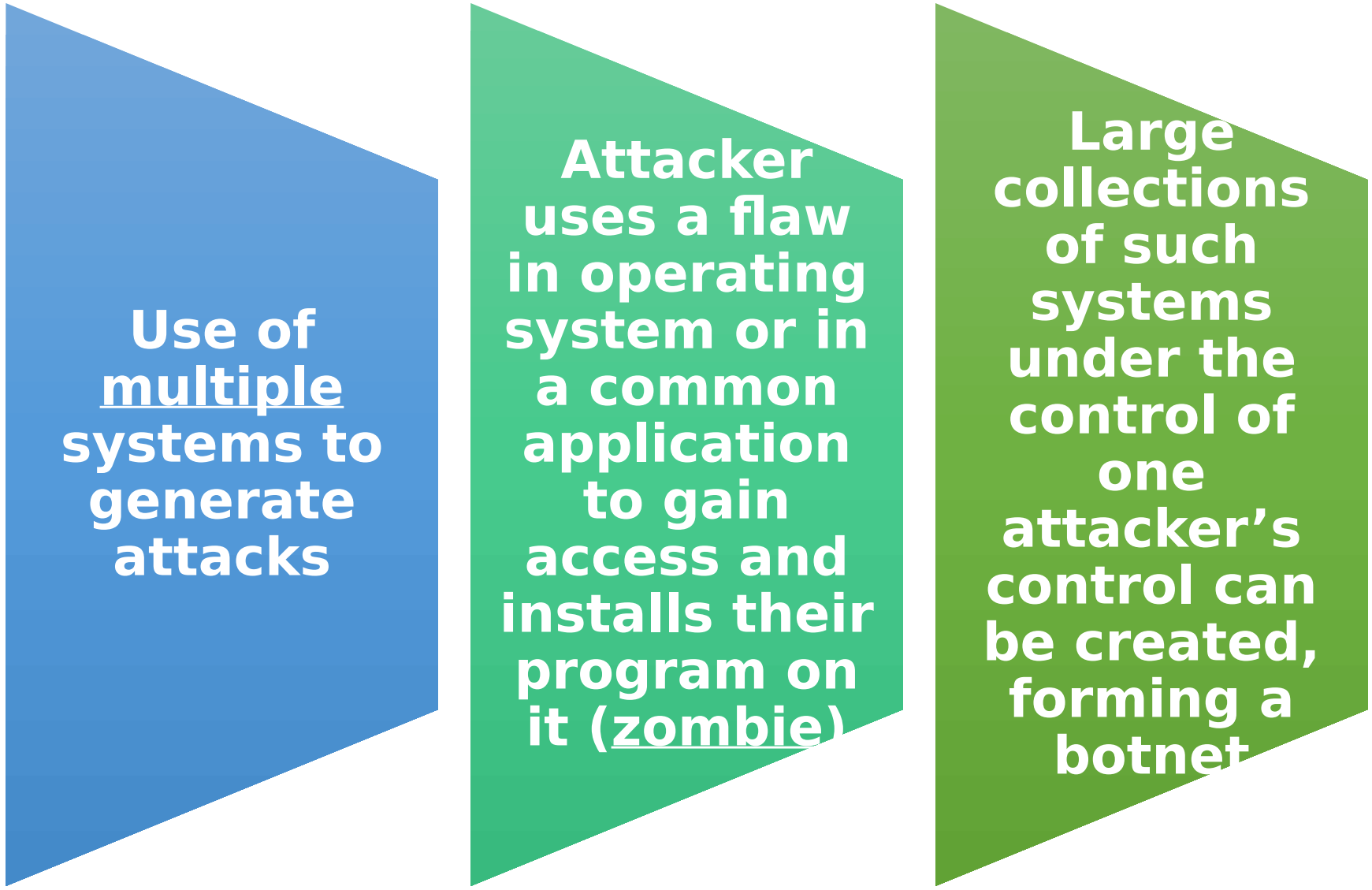
# TCP SYN spoofing attacks (cont.)

- However, in a SYN spoofing attack, the attacker directs a very large number of forged connection requests at the targeted server.
  - These rapidly fill the table of known TCP connections on the server.
  - Once this table is full, any future requests, including legitimate requests from other users, are rejected.
  - The table entries will time out and be removed, which in normal network usage corrects temporary overflow problems.
  - However, if the attacker keeps a sufficient volume of forged requests flowing, this table will be constantly full and the server will be effectively cut off from the Internet, unable to respond to most legitimate connection requests.

# Outline

- Denial-of-service attacks
- Flooding attacks
- Distributed denial-of-service attacks
- Application-based bandwidth attacks
- Reflector and amplifier attacks
- Defenses against DoS attacks

# Distributed Denial of Service DDoS Attacks



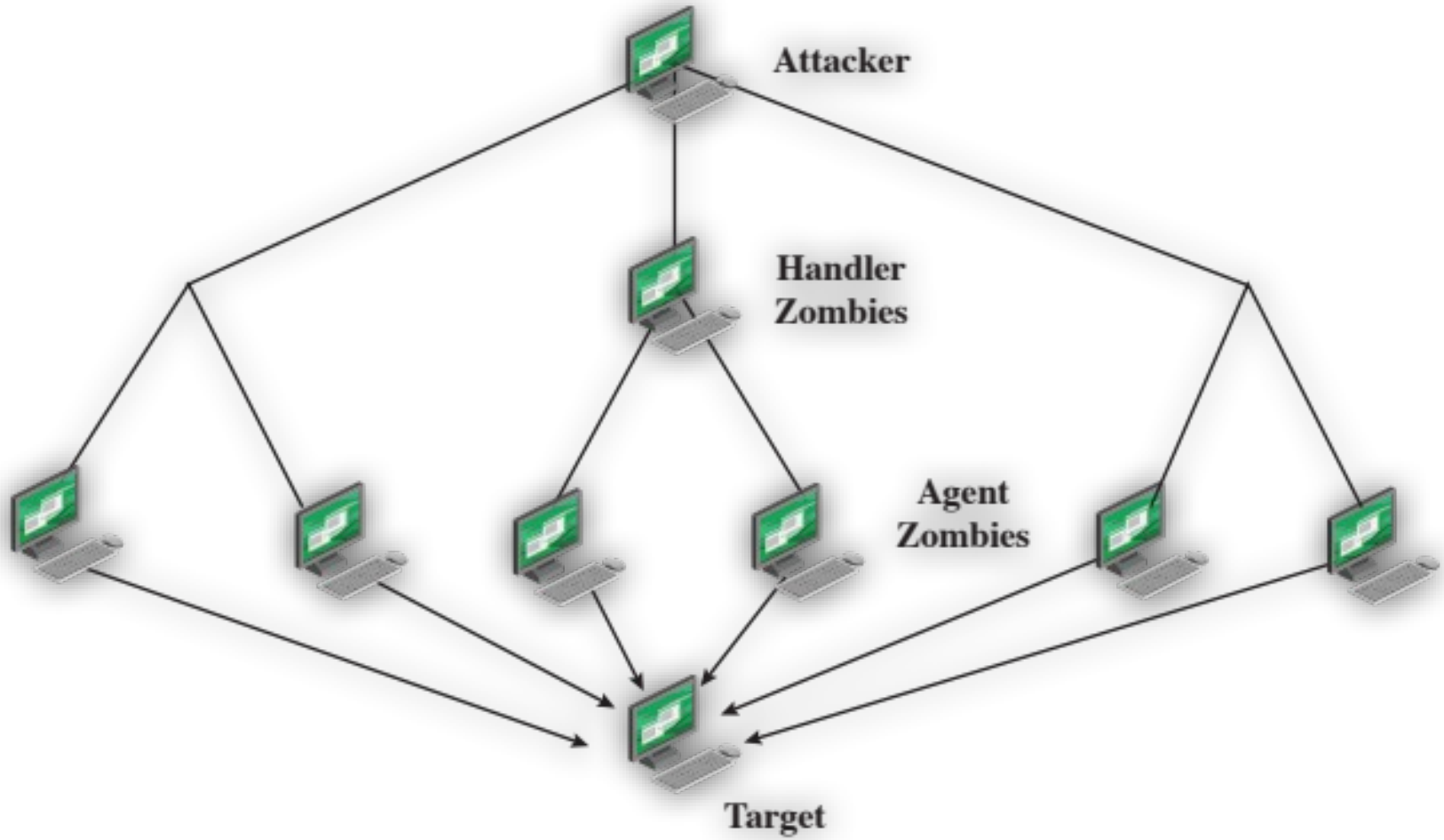



**Figure 7.4 DDoS Attack Architecture**

# Bots and Botnets

- A bot (also called webcrawlers) is a software agent which interacts with other network services intended for people as if it were a real person.
- One typical use of bots is to gather information.
- The term is derived from the word robot.
- A botnet is a collection of software robots or bots, which run autonomously.
  - Usually a collection of compromised machines running worms, Trojans or backdoors

# A botnet example

- A botnet is created and used to send email spam
  1. A botnet operator sends out viruses or worms, infecting ordinary users' PCs, whose payload is a malicious application—the bot.
  2. The bot on the infected PC logs into a particular C&C (command-and-control) server.
  3. A spammer purchases the services of the botnet from the operator.
  4. The spammer provides the spam messages to the operator, who instructs the compromised machines via the control panel on the web server, causing them to send out spam messages.


http://en.wikipedia.org/wiki/Botnet


71

# Outline

- Denial-of-service attacks
- Flooding attacks
- Distributed denial-of-service attacks
- Application-based bandwidth attacks
- Reflector and amplifier attacks
- Defenses against DoS attacks

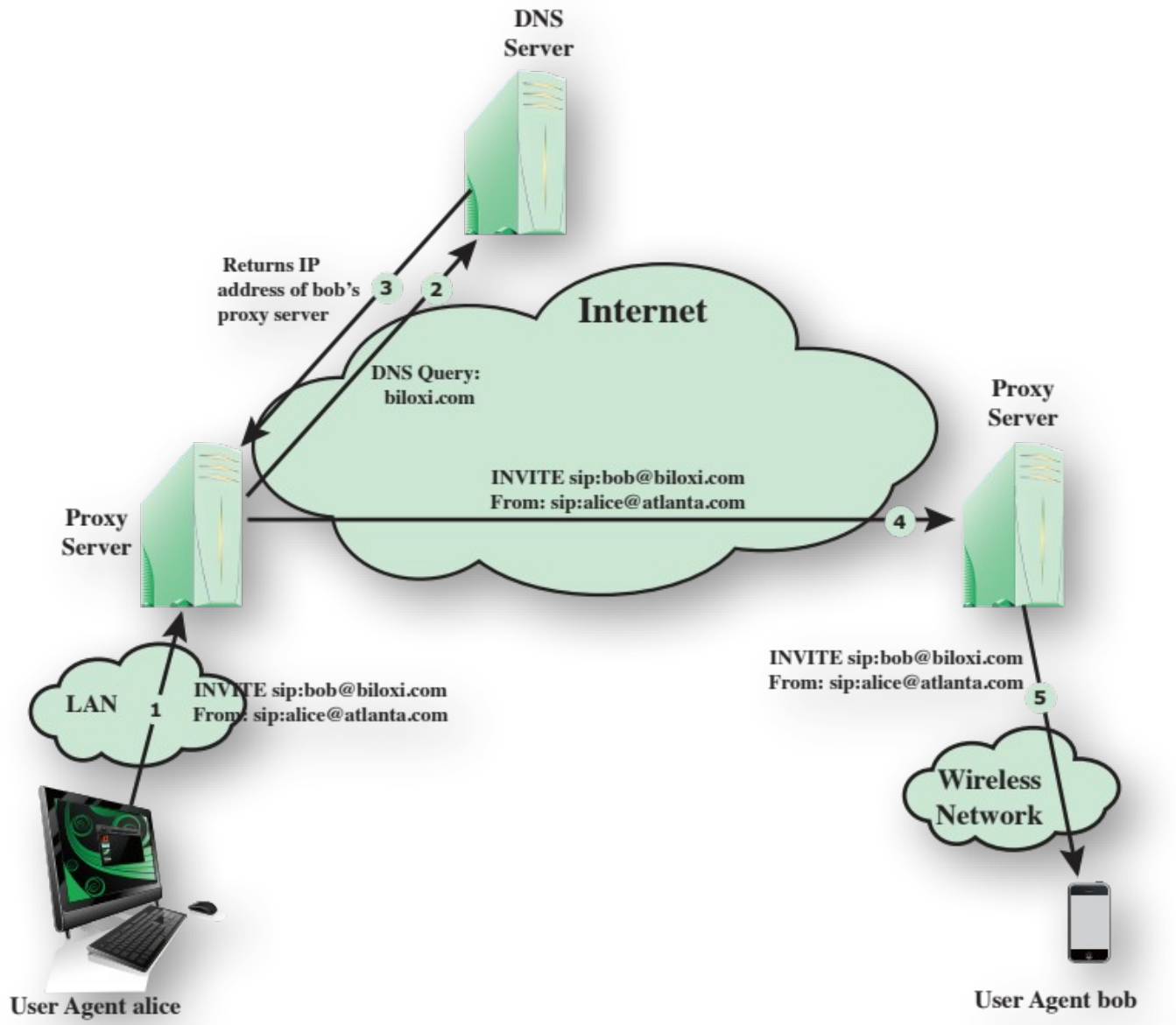



**Figure 7.5 SIP INVITE Scenario**

- SIP protocol is similar to HTTP protocol (requests and responses)
- A SIP flood attack exploits the fact that a single INVITE request triggers considerable resource consumption.
- The attacker
  - can flood a SIP proxy with numerous INVITE requests with spoofed IP addresses,
  - or alternately a DDoS attack using a botnet to generate numerous INVITE request.
- This attack puts a load on the SIP proxy servers in two ways.
  - First, their server resources are depleted in processing the INVITE requests.
  - Second, their network capacity is consumed. Call receivers are also victims of this attack.
- A target system will be flooded with forged VoIP calls, making the system unavailable for legitimate incoming calls.

# Hypertext Transfer Protocol (HTTP) Based Attacks

- HTTP flood
  - Attack that bombards Web servers with HTTP requests (DDoS attacks)
    - ✓ legitimate HTTP GET and POST requests
  - does not contain any forged or malformed packets, IP spoofing, or reflection attacks
  - Typically, HTTP requests from many different bots
  - Consumes considerable resources
    - ✓ e.g., downloading a large file; consumes memory, processing and transmission resources
- A Variant: a recursive HTTP flood
  - Bots starting from a given HTTP link and following all links on the provided Web site in a recursive way
  - requests an array of web pages from a server, inspects the replies, and iteratively requests every website item to exhaust the server's resources

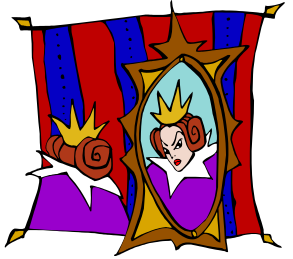
- Slowloris
  - Attempts to monopolize by sending HTTP requests that never complete
  - Eventually consumes Web server's connection capacity
  - Utilizes legitimate HTTP traffic
    - ✓ Sends an incomplete request that does not include the terminating newline sequence; sends additional header lines periodically to keep the
  - E

```
GET /doc/test.php HTTP/1.1[CRLF]
Pragma: no-cache[CRLF]
Cache-Control: no-cache[CRLF]
Host: example.vulnweb.com[CRLF]
Connection: Keep-alive[CRLF]
Accept: image/gif, image/jpeg, */*[CRLF]
Accept-Language: en-us[CRLF]
Accept-Encoding: gzip,deflate[CRLF]
User-Agent: Mozilla/5.0 [CRLF]
Content-Length: 35[CRLF]
```

# Outline

- Denial-of-service attacks
- Flooding attacks
- Distributed denial-of-service attacks
- Application-based bandwidth attacks
- Reflector and amplifier attacks
- Defenses against DoS attacks

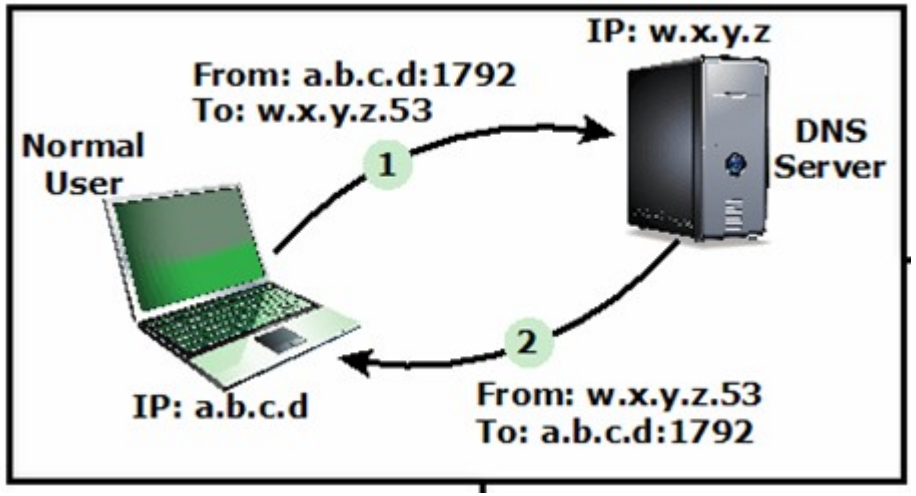
# Reflection Attacks



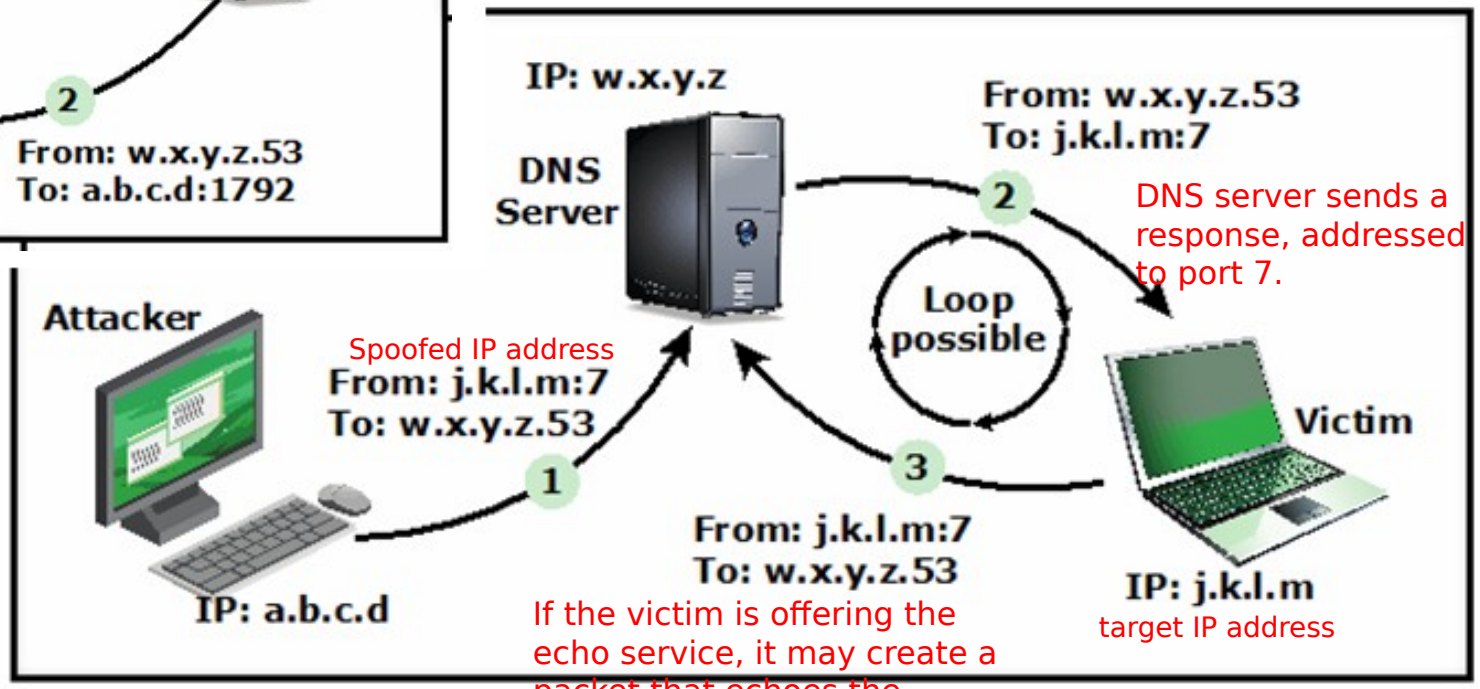
- Attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system
- When intermediary responds, the response is sent to the target
- “Reflects” the attack off the intermediary (reflector)
- Goal is to generate enough volumes of packets to flood the link to the target system without alerting the intermediary
- The basic defense against these attacks is blocking spoofed-source packets
- A further variation of the reflector attack establishes a self-contained loop between the intermediary and the target system.

# DNS Reflection Attacks

Normal DNS operation



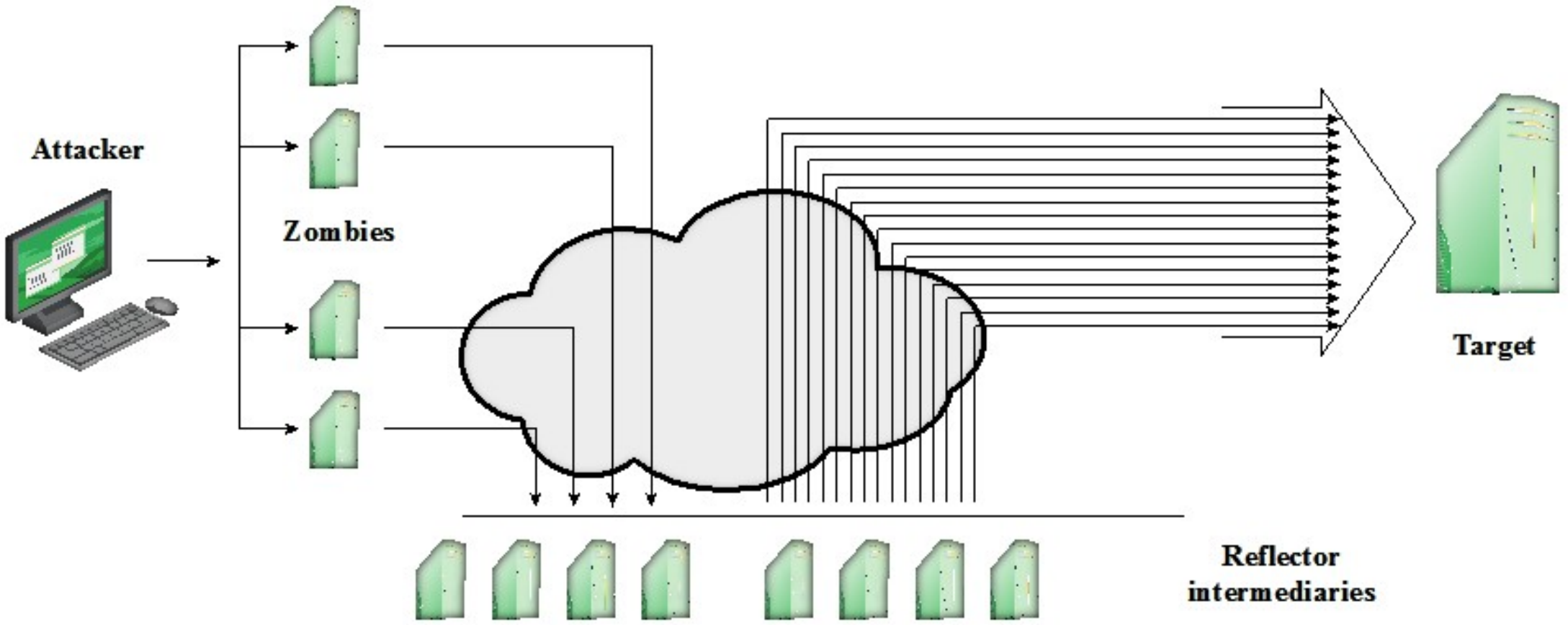

a reflection attack using DNS




The attacker uses port 7, which is associated with echo, reflector service

If the victim is offering the echo service, it may create a packet that echoes the received data back to the DNS server; this can cause a loop between the DNS server and the victm.

# DNS Amplification attacks




- are a variant of reflector attacks

# DNS Amplification Attacks (cont.)

- Use packets directed at a legitimate DNS server as the intermediary system
- Attacker creates a series of DNS requests containing the spoofed source address of the target system
- Exploit DNS behavior to convert a small request to a much larger response (amplification)
  - Using the classic DNS protocol, a 60-byte UDP request packet can easily result in a 512-byte UDP response, the maximum traditionally allowed.
  - More recently, the DNS protocol has been extended to allow much larger responses of over 4000 bytes to support extended DNS features such as IPv6, security, and others.
  - By targeting servers that support the extended DNS protocol, significantly greater amplification can be achieved than with the classic DNS protocol.
- Target is flooded with responses
- Basic defense against this attack is to prevent the use of spoofed source addresses

# Other (Potential) Amplification attacks

| Protocol | Bandwidth Amplification Factor | Vulnerable Command |
|---|---|---|
| **DNS** | 28 to 54 | see: TA13-088A (US CERT) |
| **NTP** | 556.9 | see: TA14-013A (US CERT) |
| **SSDP** | 30.8 | SEARCH request |
| **CharGEN** | 358.8 | Character generation request |
| **QOTD** | 140.3 | Quote request |
| **BitTorrent** | 3.8 | File search |
| **Kad** | 16.3 | Peer list exchange |
| **Quake Network Protocol** | 63.9 | Server info exchange |
| **RIPv1** | 131.24 | Malformed request |
| **Portmap (RPCbind)** | 7 to 28 | Malformed request |

Source: https://www.ddosbootcamp.com/course/reflection-ddos-attacks

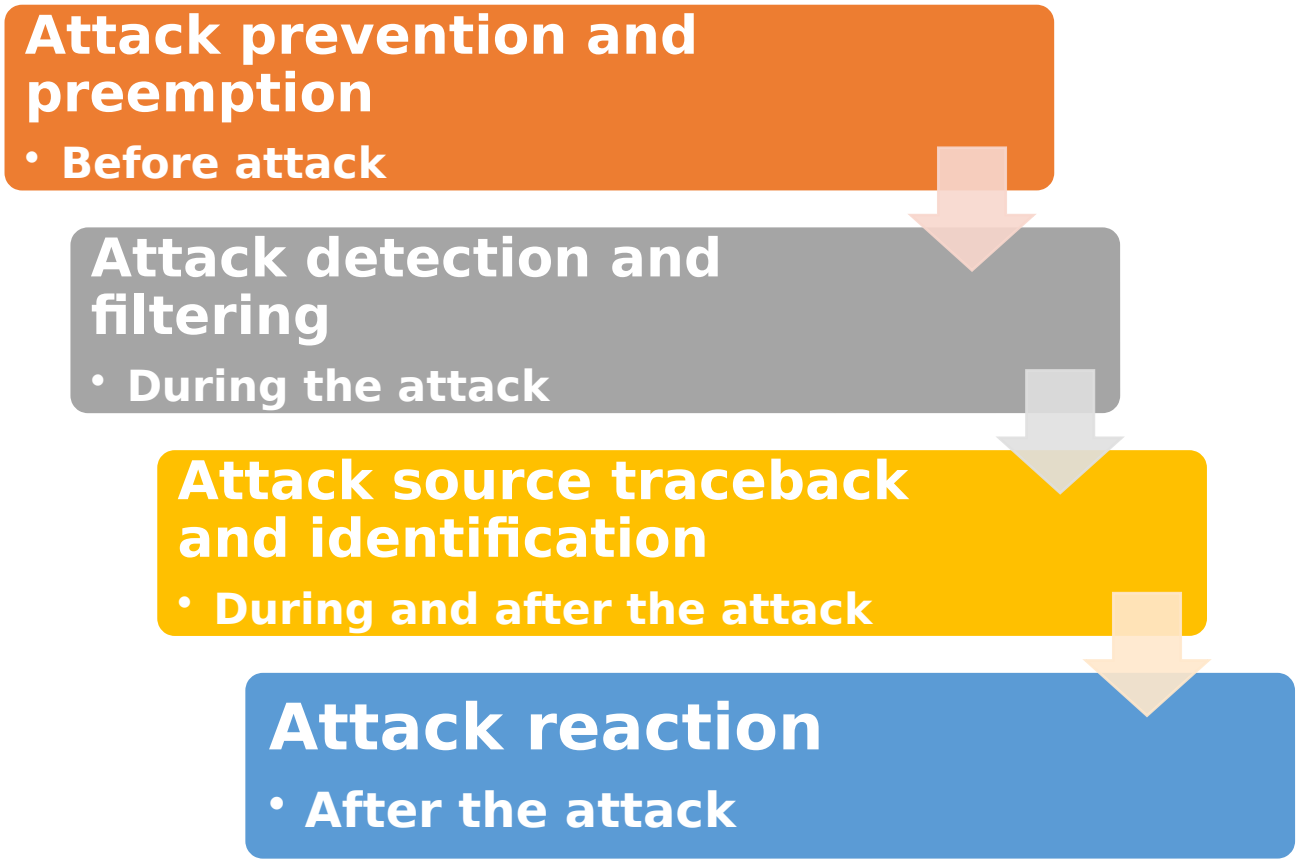
# Outline

- Denial-of-service attacks
- Flooding attacks
- Distributed denial-of-service attacks
- Application-based bandwidth attacks
- Reflector and amplifier attacks
- DNS amplification attacks
- Defenses against DoS attacks

# DoS Attack Defenses

- These attacks cannot be prevented entirely
- High traffic volumes may be legitimate
  - High publicity about a specific site
  - Activity on a very popular site
  - Described as slashdotted, flash crowd, or flash event

Four lines of defense against DDoS attacks



# DoS Attack Prevention

- Block spoofed source addresses
  - On routers as close to source as possible
- Filters may be used to ensure path back to the claimed source address is the one being used by the current packet
  - Filters must be applied to traffic before it leaves the ISP's network or at the point of entry to their network
- Use modified TCP connection handling code
  - Cryptographically encode critical information in a cookie that is sent as the server's initial sequence number
    - ✓ Legitimate client responds with an ACK packet containing the incremented sequence number cookie
  - Drop an entry for an incomplete connection from the TCP connections table when it overflows

# DoS Attack Prevention

- Block IP directed broadcasts
- Block suspicious services and combinations
- Manage application attacks with a form of graphical puzzle (captcha) to distinguish legitimate human requests
- Good general system security practices
- Use mirrored and replicated servers when high-performance and reliability is required

# Responding to DoS Attacks

**Good Incident Response Plan**

- Details on how to contact technical personal for ISP
- Needed to impose traffic filtering upstream
- Details of how to respond to the attack
  - Antispoofing, directed broadcast, and rate limiting filters should have been implemented
  - Ideally have network monitors and IDS to detect and notify abnormal traffic patterns

# Responding to DoS Attacks

- Identify type of attack
  - Capture and analyze packets
  - Design filters to block attack traffic upstrea
  - Or identify and correct system/application bu
- Have ISP trace packet flow back to source
  - May be difficult and time consuming
  - Necessary if planning legal action
- Implement contingency plan
  - Switch to alternate backup servers
  - Commission new servers at a new site with new addresses
- Update incident response plan
  - Analyze the attack and the response for future handling