# DDoS Attacks & Botnet

CSE3482
By: Yang Liu, Harshilkumar Patel, Melissa Soon

## Purpose

- Extortion
- Bussiness competition
- Hacktivism
- Script kiddies
- Security Feints
- Internal Testing

## Consequences

- Disable a specific computer, service, or entire network
- Hit system resources like bandwidth, disk space, processor time, or routing information
- Crash the operating system
- Loss of revenue, brand damage, and angry customers

## DDoS = Distributed denial of service

- Multiple systems target a single system to take down a service, compromising availability
- These multiple systems are referred to a botnet

Visualization of DDos attack on World of Warcraft servers at Blizzard

### Issues

- DDoS attacks cannot be stopped by [illegible] access to a single IP address
- Difficult to distinguish the real user traffic from the attacking traffic
- DDoS [illegible] from flooding the network

### Types of Attacks

- Protocol attacks: Use up all available connections to infrastructure
- Volumetric attacks – Consumes the bandwidth causing congestion
- Application attacks – The application layer is targeted

## Questions and Answers

What is the main goal of DDoS Attacks?

- To hinder a server or a system [illegible]

What does the command structure for botnets look like?

- From top to bottom: Botnet Master → Command and Control servers → Zombie Bots

How long do most DDoS attacks last for?

- One half of all DDoS attacks [illegible] 30 minutes or less

Thank You!

## Types of attacks: Volumetric attacks

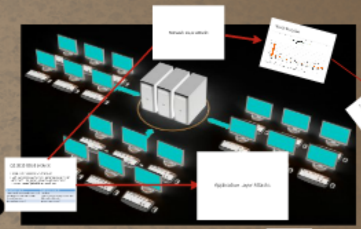
- Also known as floods
- Account for 65% of DDoS attacks
- Causes congestion by sending lots of traffic which overwhelm the sites bandwidth
- Example: ICMP floods

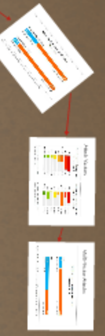
## Types of attacks: Protocol

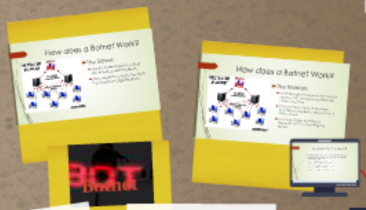
- Target the connection state tables in infrastructure such as the firewall, load-balancers and web application servers
- Account for 20% of reported DDoS attacks in 2014
- Example: Ping of death –

## Types of Attacks: Application-layer

- 17% of DDoS attacks
- Over-exercises specific functions or features of a website with the intention to disable those functions or features
- Examples: HTTP flood







How does a Botnet Work?

BOT
Botnet

## What is a Botnet?

- A network of similar machines trying to complete repetitive tasks and objectives
- Devices include: web servers, personal or work computer, mobile devices, or cable modems

## What does a Botnet do?

- A botnet can perform tasks such as:
  - Scanning for new targets
  - Exfiltrating data
  - Distributing malicious software (Malware such as viruses, worms, and keyloggers)
  - Stealing personal information or intellectual property
  - Attacking other targets (DDoS attacks)

## Purpose

- Extortion
- Bussiness competition
- Hacktivism
- Script kiddies
- Security Feints
- Internal Testing

## Consequences

- Disable a specific computer, service, or entire network
- Hit system resources like bandwidth, disk space, processor time, or routing information
- Crash the operating system
- Loss of revenue, brand damage, and angry customers

### Types of Attacks

- Protocol attacks- Use up all available connections to infrastructure
- Volumetric attacks – Consumes the bandwidth causing congestion
- Application attacks - The application layer is targeted

### Questions and Answers

What is the main goal of DDoS Attacks?

- [illegible]

What does the command structure for botnets look like?

- [illegible]

How long do most DDoS attacks last for?

- One half of all DDoS attacks lasted 30 minutes or less

### Types of attacks: Volumetric attacks

- Also known as floods
- Account for 65% of DDoS attacks
- Causes congestion by sending lots of traffic which overwhelm the sites bandwidth
- Example: ICMP floods

### Types of attacks: Protocol

- Target the connection state tables in infrastructure such as the firewall, load-balancers and web application servers
- Account for 20% of reported DDoS attacks in 2014
- Example: Ping of death –

### Types of Attacks: Application-layer

- 17% of DDoS attacks
- Over-exercises specific functions or features of a website with the intention to disable those functions or features
- Examples: HTTP flood

Thank You!

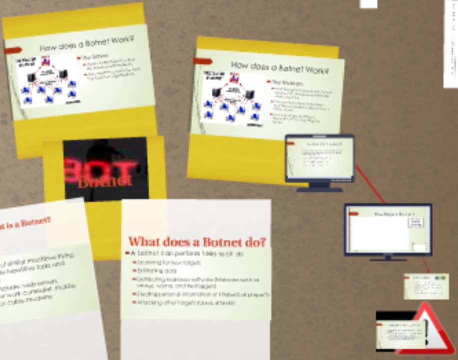
### DDoS = Distributed denial of service

- Multiple systems target a single system to take down a service, compromising availability
- These multiple systems are referred to a botnet

Visualization of DDoS attack on World of Warcraft servers at Blizzard

### Issues

- DDoS attacks cannot be stopped by preventing access to a single IP address
- Difficult to distinguish normal user traffic from the attacking traffic
- DDoS prevents intended users from accessing the network



### What is a Botnet?

- A network of similar machines trying to complete repetitive tasks and objectives
- Devices include: web servers, personal or work computers, mobile devices, or cable modems

### What does a Botnet do?

- A botnet can perform tasks such as:
  - Scanning for new targets
  - Exfiltrating data
  - Distributing malicious software (Malware such as viruses, worms, and keyloggers)
  - Stealing personal information or intellectual property
  - Attacking other targets (DDoS attacks)

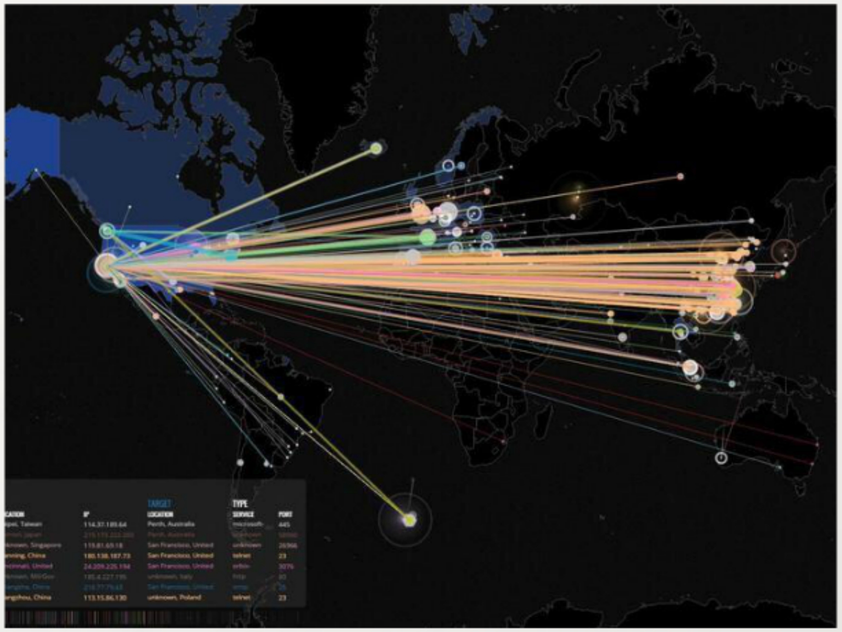
# DDoS Attacks & Botnet

CSE3482

By: Yang Liu, Harshilkumar Patel, Melissa Soon

# DDoS = Distributed denial of service

- Multiple systems target a single system to take down a service, compromising availability
- These multiple systems are referred to a botnet



|  |  | TARGET | TYPE |  |
|---|---|---|---|---|
| CATION | IP | LOCATION | SERVICE | PORT |
| ipei, Taiwan | 114.37.185.64 | Perth, Australia | microsoft- | 445 |
| [illegible] Japan | [illegible] | Perth, Australia | unknown | [illegible] |
| known, Singapore | 115.81.65.18 | San Francisco, United | unknown | 26966 |
| nning, China | 180.138.187.73 | San Francisco, United | telnet | 23 |
| cinnati, United | 24.209.225.194 | San Francisco, United | orbix- | 3076 |
| known, MilGov | 185.4.227.195 | unknown, Italy | http | 80 |
| angzhou, China | 218.77.79.43 | San Francisco, United | smtp | 25 |
| angzhou, China | 113.15.86.130 | unknown, Poland | telnet | 23 |

Visualization of DDos attack on World of Warcraft servers at Blizzard

# Issues

- DDoS attacks cannot be stopped by preventing access to a single IP address
- Difficult to distinguish normal user traffic from the attacking traffic
- DDoS prevents intended users from accessing the network

## Purpose

- Extortion
- Bussiness competition
- Hacktivism
- Script kiddies
- Security Feints
- Internal Testing

## Consequences

- Disable a specific computer, service, or entire network
- Hit system resources like bandwidth, disk space, processor time, or routing information
- Crash the operating system
- Loss of revenue, brand damage, and angry customers

# Purpose

- Extortion
-
- Bussiness competition
-
- Hacktivism
-
- Script kiddies
-
- Security Feints
-
- Internal Testing

- Disable a
entire ne
- Hit syster
disk spac
informati
- Crash the
- Loss of rev
angry custo

# Consequences

- Disable a specific computer, service, or entire network
- Hit system resources like bandwidth, disk space, processor time, or routing information
- Crash the operating system
- Loss of  revenue, brand damage, and angry customers

- Pro co
- Vol ba
- Ap lay

# Types of  Attacks

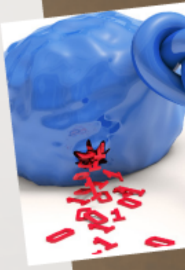
- Protocol attacks– Use up all available connections to infrastructure
- Volumetric attacks – Consume the bandwidth causing congestion
- Application attacks – The application layer is targetted

## Types of attacks: Volumetric attacks

- Also known as floods
- Account for 65% of DDoS attacks
- Causes congestion by sending lots of traffic which overwhelm the sites bandwidth
- Example: ICMP floods

## Types of attacks: Protocol

- Target the connection state tables in infrastructure such as the firewall, load-balancers and web application servers
- Account for 20% of reported DDoS attacks in 2014
- Example: Ping of death –



## Types of Attacks: Application-layer

- 17% of DDoS attacks
- Over-exercises specific functions or features of a website with the intention to disable those functions or features
- Examples: HTTP flood

Q2 2015 DDoS analysis

- DDoS: Distributed Denial of Service
- Lost business opportunities, loss of consumer trust, data theft, intellectual property loss, significant financial losses ($40,000 per hour), etc

| Network Layer Attacks | Application Layer attacks |
|---|---|

# Types of  attacks: Volumetric attacks

- Also known as floods
- Account for 65% of  DDoS attacks
- Causes congestion by sending lots of traffic which overwhelm the sites bandwidth
- Example: ICMP floods

Typ

- 17%
- Over-
functi

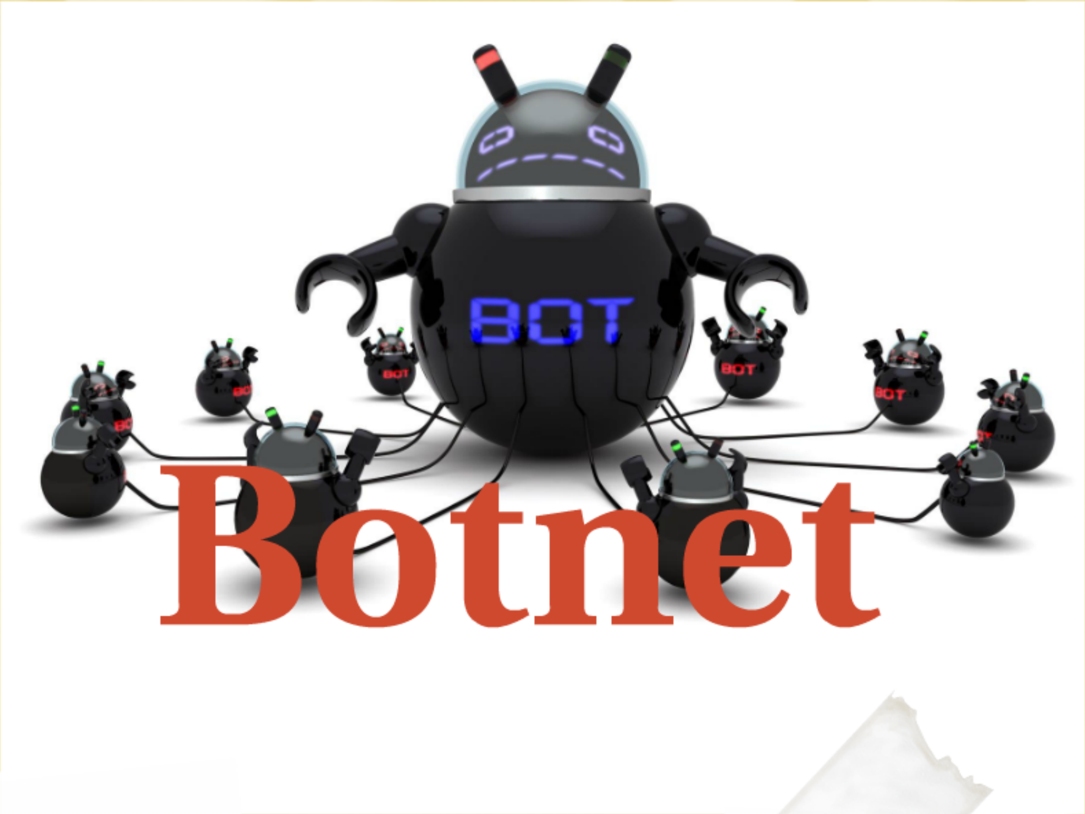
# Types of Attacks: Application-layer

- 17% of DDoS attacks
- Over-exercises specific functions or features of a website with the intention to disable those functions or features
- Examples: HTTP flood

# Types of attacks: Protocol

- Target the connection state tables in infrastructure such as the firewall, load-balancers and web application servers
- Account for 20% of reported DDoS attacks in 2014
- Example: Ping of death –

tion-layer



# Botnet

## Botnet?

machines trying

## What does

- A botnet can perfo

# Botnet

## What is a Botnet?

- A network of similar machines trying to complete repetitive tasks and objectives
- Devices include: web servers, personal or work computer, mobile devices, or cable modems

## What does a Botnet d

- A botnet can perform tasks such as:
  - Scanning for new targets
  - Exfiltrating data
  - Distributing malicious software (Malware such viruses, worms, and keyloggers)
  - Stealing personal information or intellectual pro
  - Attacking other targets (DDoS attacks)

# What is a Botnet?

- A network of similar machines trying to complete repetitive tasks and objectives
- Devices include: web servers, personal or work computer, mobile devices, or cable modems

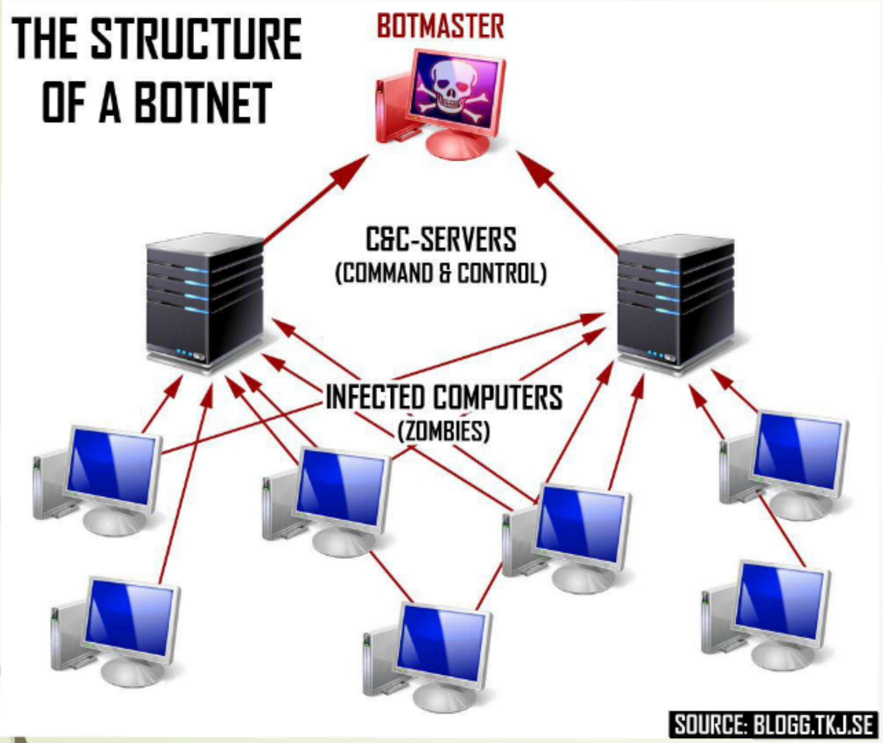
# Wh

- A botn
  - Scann
  - Exfiltra
  - Distribu viruses,
  - Stealing
  - Attackin

# What does a Botnet do?

- A botnet can perform tasks such as:
  - Scanning for new targets
  - Exfiltrating data
  - Distributing malicious software (Malware such as viruses, worms, and keyloggers)
  - Stealing personal information or intellectual property
  - Attacking other targets (DDoS attacks)

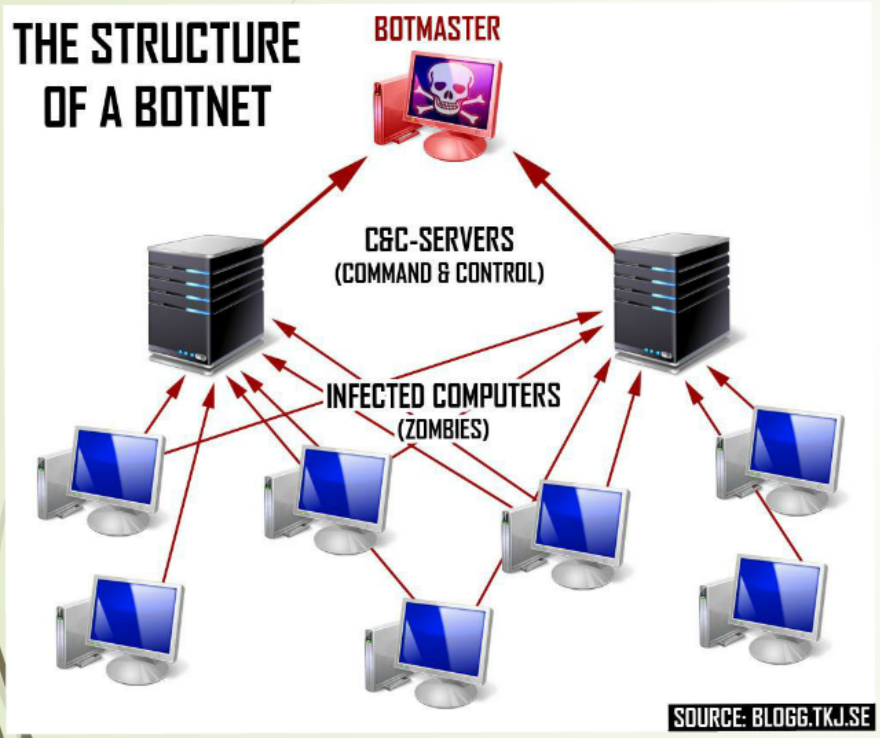
# How does a Botnet Work?



SOURCE: BLOGG.TKJ.SE

- The Slaves
  - Mostly victim machines that are infected with malware
  - slave machines could be from individuals or organizations

# How does a Botnet Work?



SOURCE: BLOGG.TKJ.SE

- The Masters
  - Work through Command and Control servers (C2s) and serve as the brains of the operation
  - C2s issue instructions of the slave machines to perform tasks such as a DDoS attack
  - Structure: single, multiple, or hierarchical C2s controlling the botnet

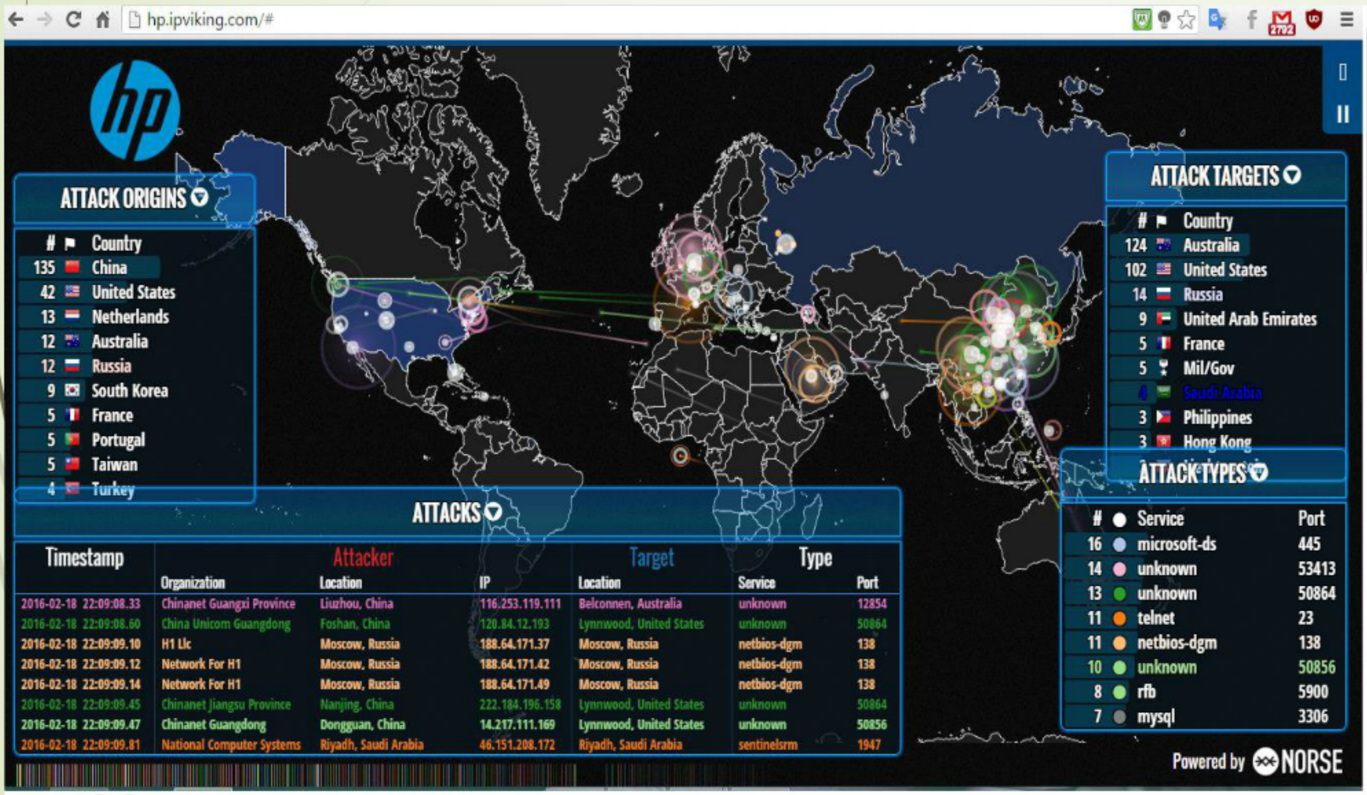
Who are the Slave

- The botnet zombie army is mostly consisted of infected co
- The top five countries with the highest absolute unique IP v communicating with C2s are
  unique-victim IP addresses

# Who are the Slaves?

- The botnet zombie army is mostly consisted of infected computers
- The top five countries with the highest absolute unique IP victims communicating with C2s are
  - China – 532,000 unique-victim IP addresses
  - United States – 528,000 unique-victim IP addresses
  - Norway – 213,000 unique-victim IP addresses
  - Spain –129,000 unique-victim IP addresses
  - Ukraine – 124,000 unique-victim IP addresses

# How Big is a Botnet?



ATTACK ORIGINS

| # | | Country |
|---|---|---|
| 135 | | China |
| 42 | | United States |
| 13 | | Netherlands |
| 12 | | Australia |
| 12 | | Russia |
| 9 | | South Korea |
| 5 | | France |
| 5 | | Portugal |
| 5 | | Taiwan |
| 4 | | Turkey |

ATTACK TARGETS

| # | | Country |
|---|---|---|
| 124 | | Australia |
| 102 | | United States |
| 14 | | Russia |
| 9 | | United Arab Emirates |
| 5 | | France |
| 5 | | Mil/Gov |
| 4 | | Saudi Arabia |
| 3 | | Philippines |
| 3 | | Hong Kong |

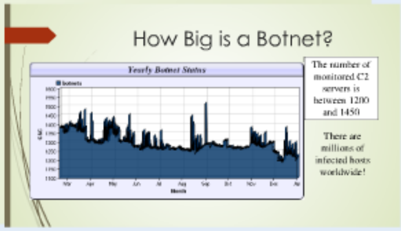
ATTACK TYPES

| # | ● | Service | Port |
|---|---|---|---|
| 16 | ● | microsoft-ds | 445 |
| 14 | ● | unknown | 53413 |
| 13 | ● | unknown | 50864 |
| 11 | ● | telnet | 23 |
| 11 | ● | netbios-dgm | 138 |
| 10 | ● | unknown | 50856 |
| 8 | ● | rfb | 5900 |
| 7 | ● | mysql | 3306 |

ATTACKS

| Timestamp | Attacker | | | Target | Type | |
|---|---|---|---|---|---|---|
| | Organization | Location | IP | Location | Service | Port |
| 2016-02-18 22:09:08.33 | Chinanet Guangxi Province | Liuzhou, China | 116.253.119.111 | Belconnen, Australia | unknown | 12854 |
| 2016-02-18 22:09:08.60 | China Unicom Guangdong | Foshan, China | 120.84.12.193 | Lynnwood, United States | unknown | 50864 |
| 2016-02-18 22:09:09.10 | H1 Llc | Moscow, Russia | 188.64.171.37 | Moscow, Russia | netbios-dgm | 138 |
| 2016-02-18 22:09:09.12 | Network For H1 | Moscow, Russia | 188.64.171.42 | Moscow, Russia | netbios-dgm | 138 |
| 2016-02-18 22:09:09.14 | Network For H1 | Moscow, Russia | 188.64.171.49 | Moscow, Russia | netbios-dgm | 138 |
| 2016-02-18 22:09:09.45 | Chinanet Jiangsu Province | Nanjing, China | 222.184.196.158 | Lynnwood, United States | unknown | 50864 |
| 2016-02-18 22:09:09.47 | Chinanet Guangdong | Dongguan, China | 14.217.111.169 | Lynnwood, United States | unknown | 50856 |
| 2016-02-18 22:09:09.81 | National Computer Systems | Riyadh, Saudi Arabia | 46.151.208.172 | Riyadh, Saudi Arabia | sentinelsrm | 1947 |

The average number of infected hosts per C2 is 1700

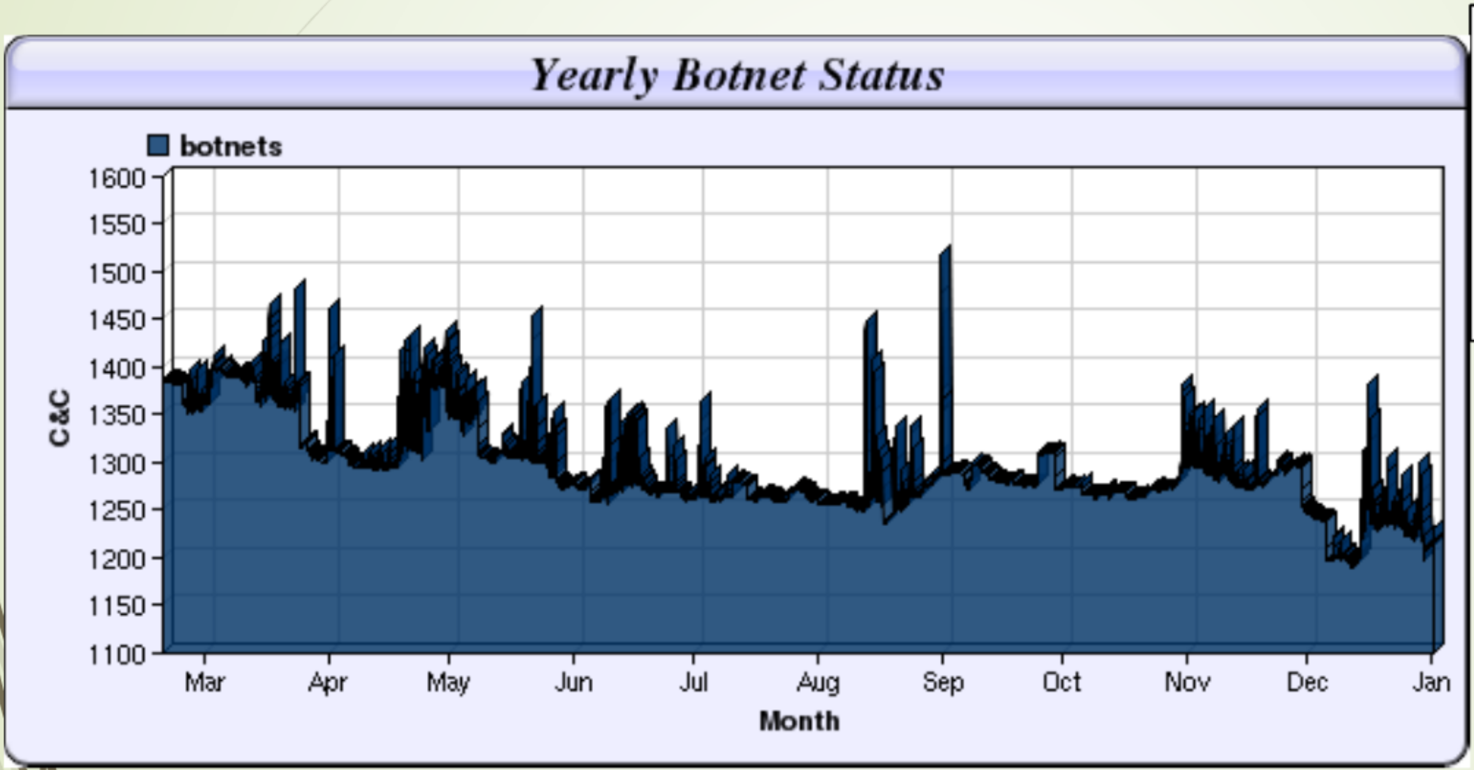


How Big is a Botnet?

The number of monitored C2 servers is between 1200 and 1450

There are millions of infected hosts worldwide!

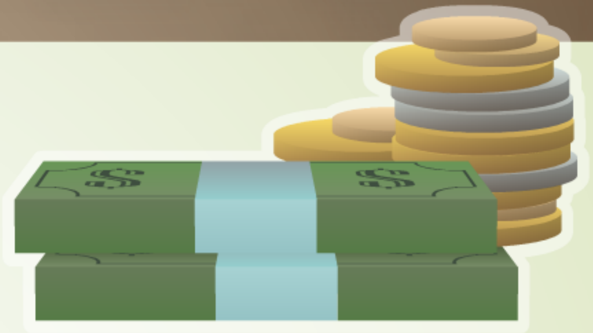
# How Big is a Botnet?



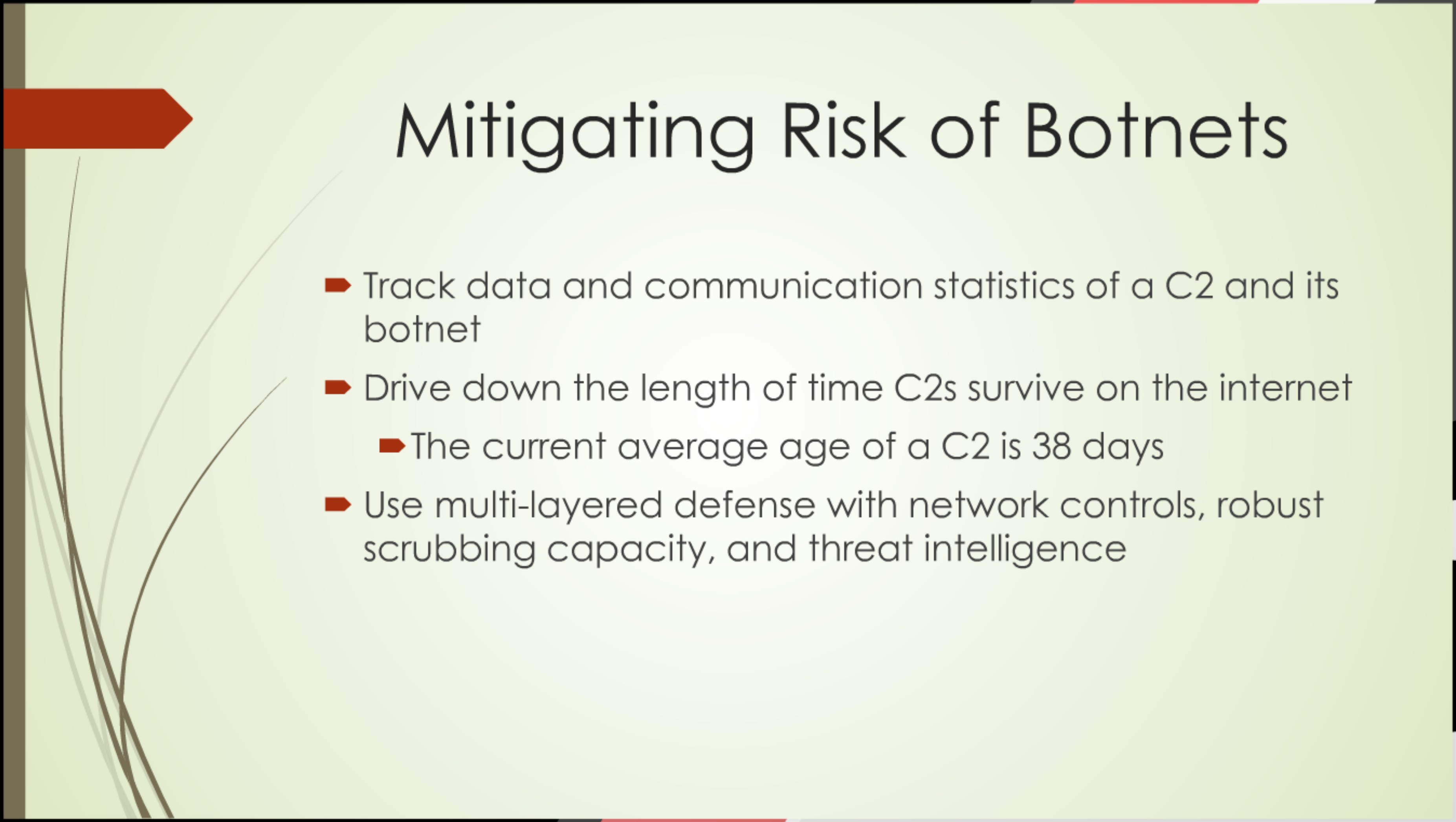
The number of monitored C2 servers is between 1200 and 1450

There are millions of infected hosts worldwide!

# Botnet as a Business



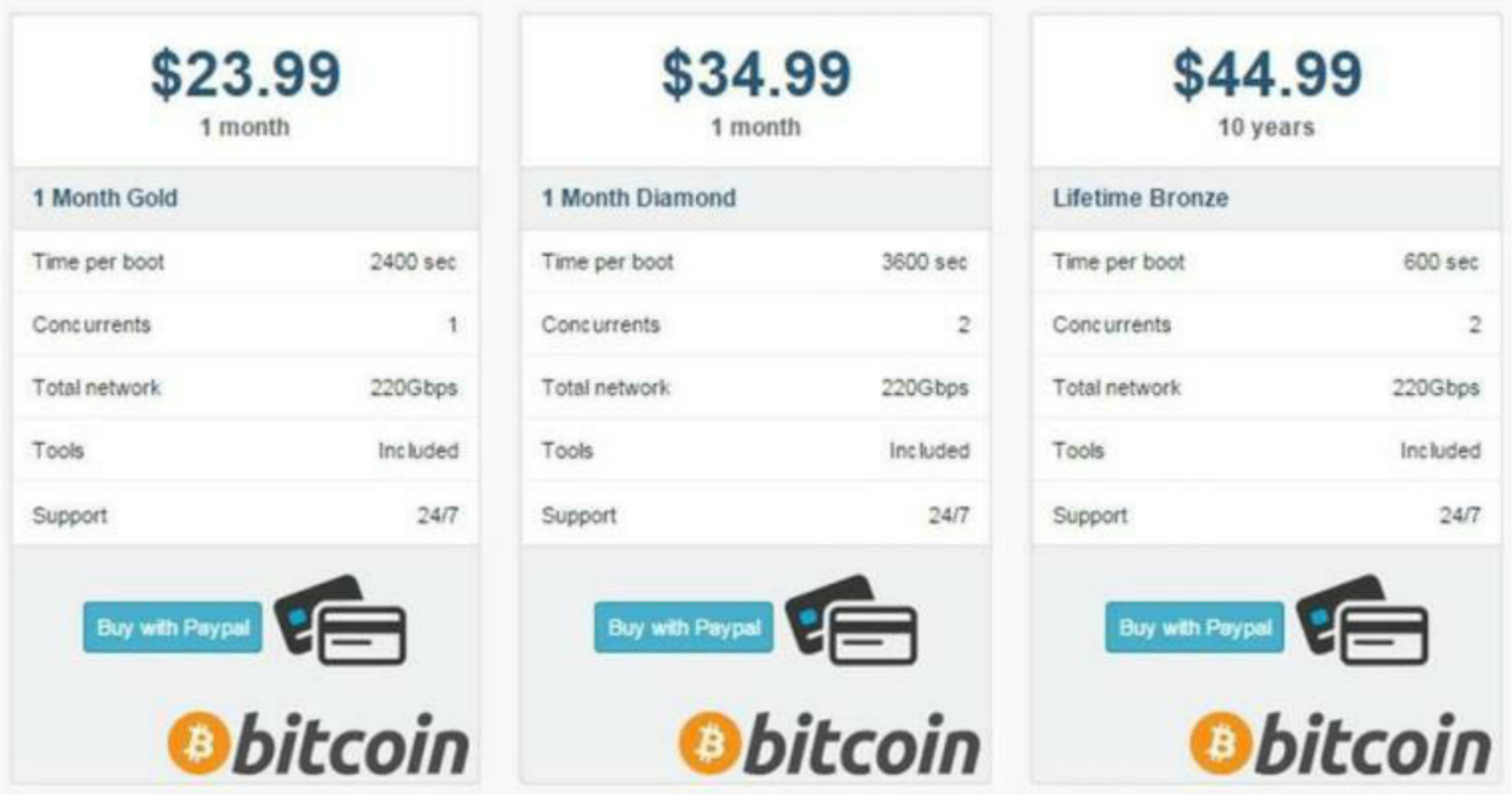
- lucrative business with simple setup.
- Operational costs to create, maintain and move a botnet are low
- Blocked botnets can come back online often within hours of being shut down.
- Botnet as a for-hire business:
  - USD$190/month for access to 1000 unique servers



# Mitigating Risk of Botnets

- Track data and communication statistics of a C2 and its botnet
- Drive down the length of time C2s survive on the internet
  - The current average age of a C2 is 38 days
- Use multi-layered defense with network controls, robust scrubbing capacity, and threat intelligence

# Botnet-for-Hire



**$23.99**
1 month

| 1 Month Gold | |
|---|---|
| Time per boot | 2400 sec |
| Concurrents | 1 |
| Total network | 220Gbps |
| Tools | Included |
| Support | 24/7 |

**$34.99**
1 month

| 1 Month Diamond | |
|---|---|
| Time per boot | 3600 sec |
| Concurrents | 2 |
| Total network | 220Gbps |
| Tools | Included |
| Support | 24/7 |

**$44.99**
10 years

| Lifetime Bronze | |
|---|---|
| Time per boot | 600 sec |
| Concurrents | 2 |
| Total network | 220Gbps |
| Tools | Included |
| Support | 24/7 |

*Figure 8: Example of botnet-for-hire advertised prices and capacities*

# Q2 2015 DDoS analysis

- DDoS: Distributed Denial of Service
- Lost business opportunities, loss of consumer trust, data theft, intellectual property loss, significant financial losses ($40,000 per hour), etc

| Network Layer Attacks | Application Layer attacks |
|---|---|
| Target network and transport layers (3 and 4) | Target layer 7 |
| Assaults that use much of the available bandwidth resources | Overbear server’s processing resource with a high number of requests |
| Gbps (gigabits per second) | RPS (requests per second) |

# Network Layer Attacks

# Attack Duration

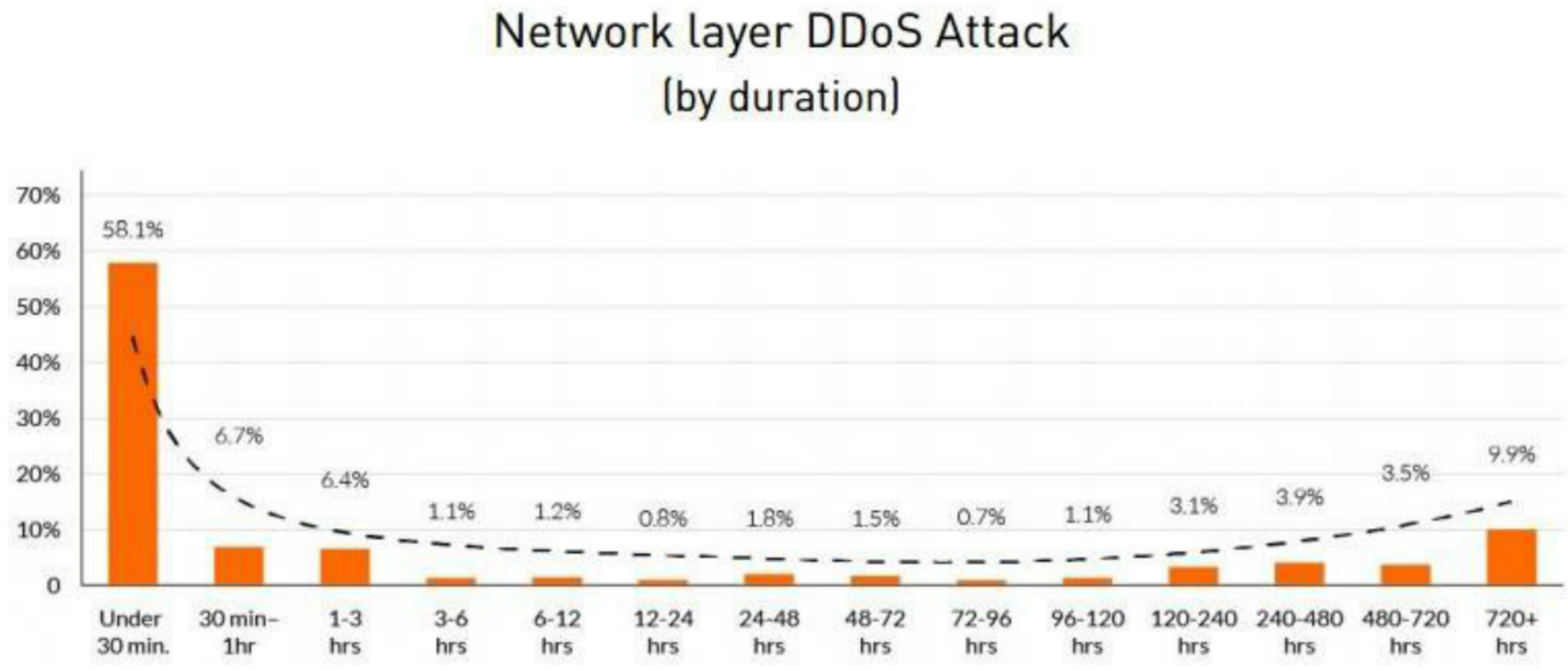


*Figure 2: Distribution of network layer DDoS attacks, by duration*

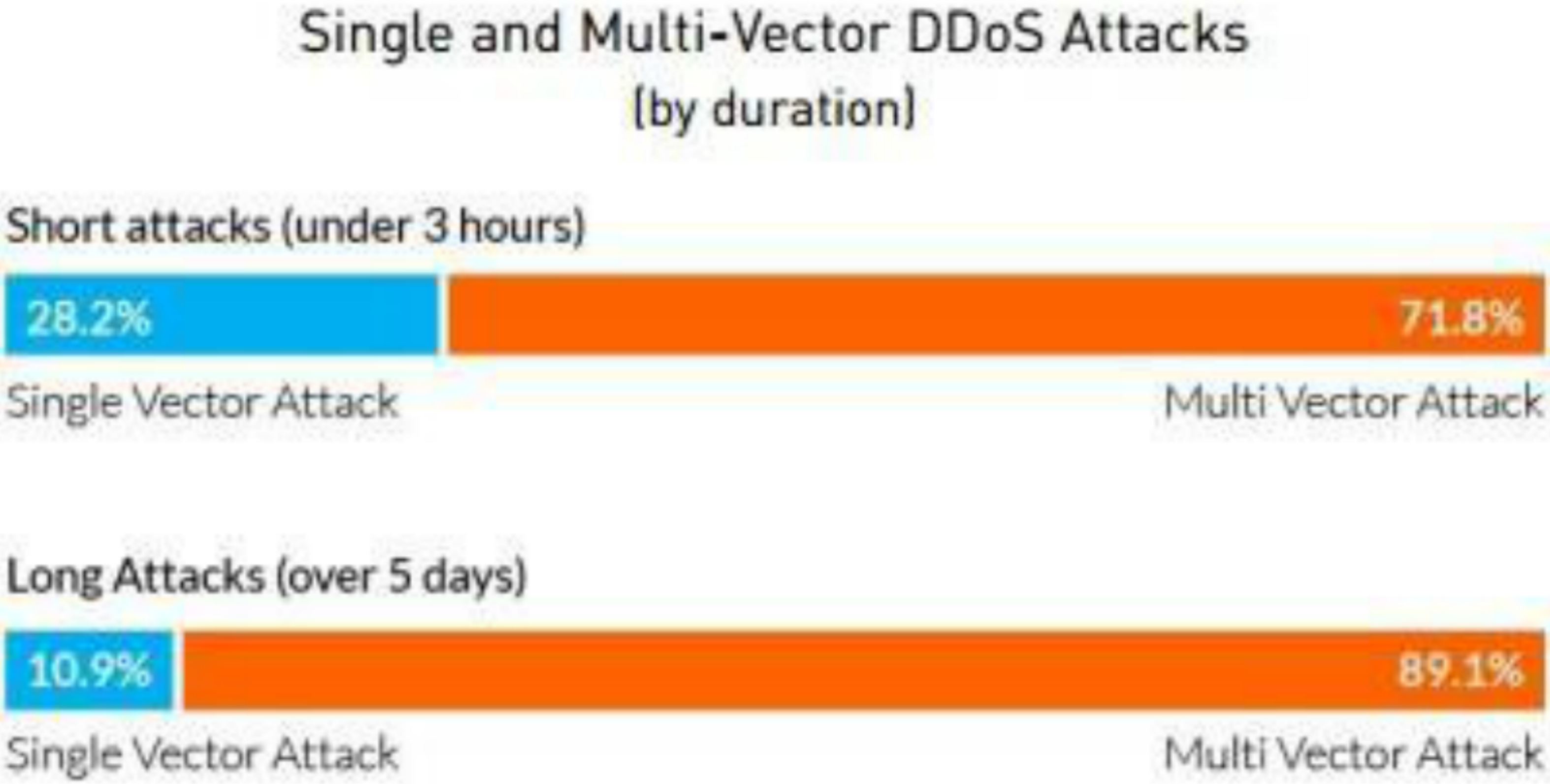
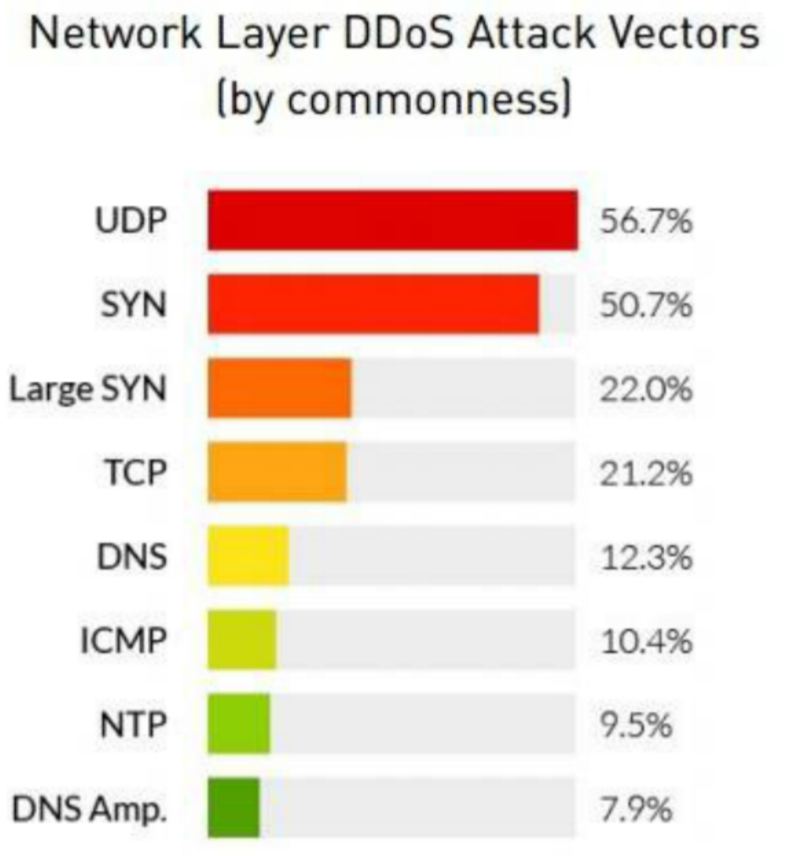


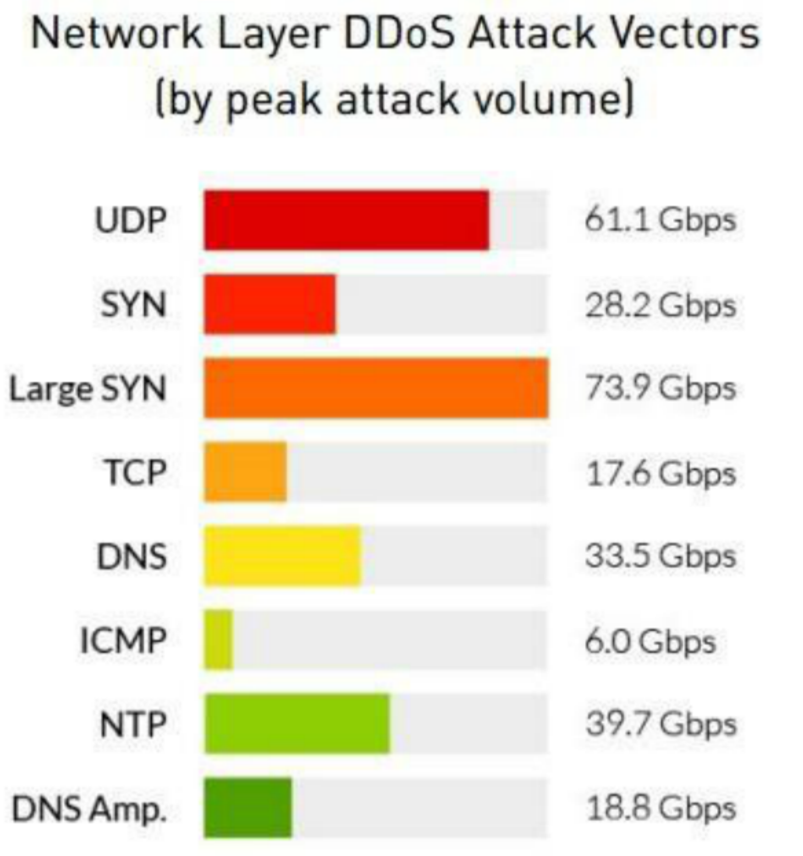
*Figure 3: Distribution of single and multi-vector DDoS attacks, by duration*

# Attack Vectors



Network Layer DDoS Attack Vectors (by commonness)

*Figure 4: Distribution of DDoS attack vectors, by commonness*



Network Layer DDoS Attack Vectors (by peak attack volume)

*Figure 5: Distribution of DDoS attack vectors, by peak attack volume*

# Multi-Vector Attacks

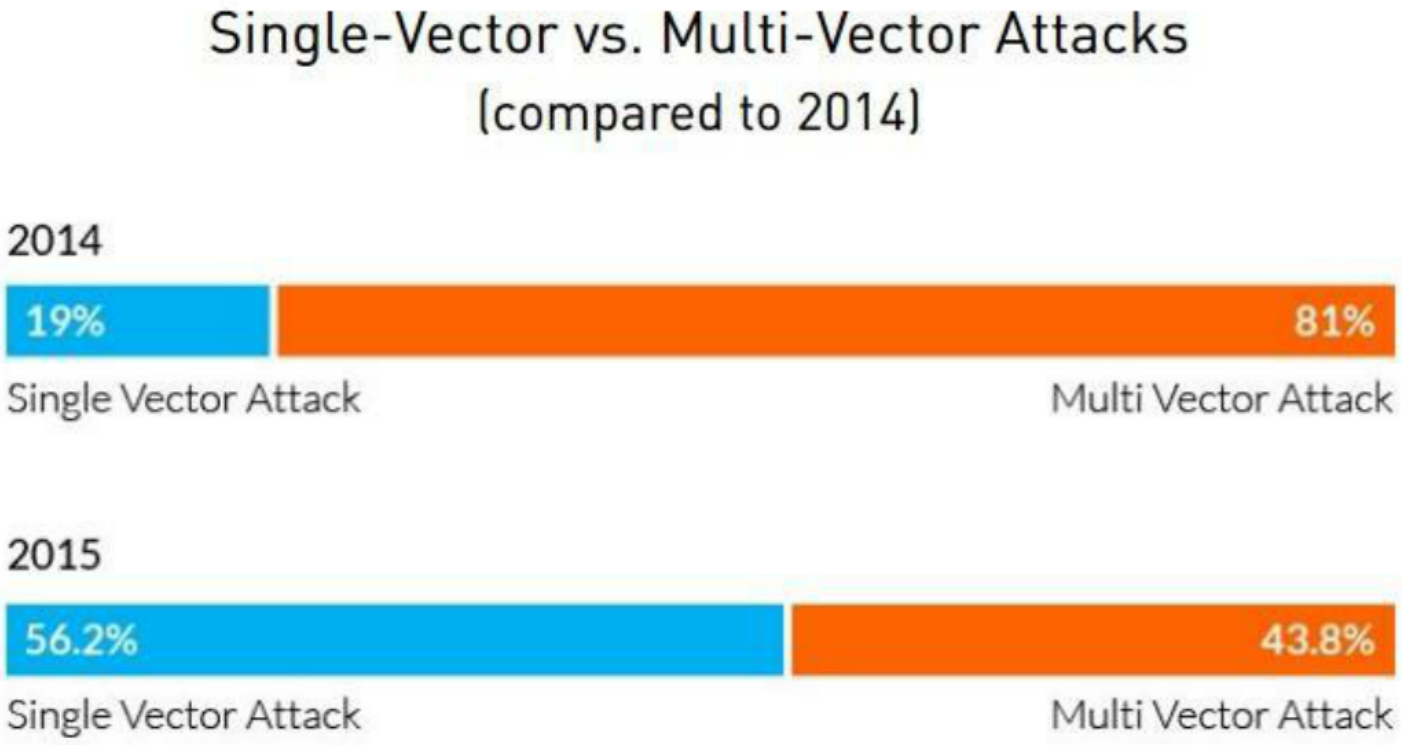


*Figure 6: Distribution of single-vector vs. multi-vector attacks, compared to 2014*

# Application Layer Attacks

# Attack Duration and Frequency

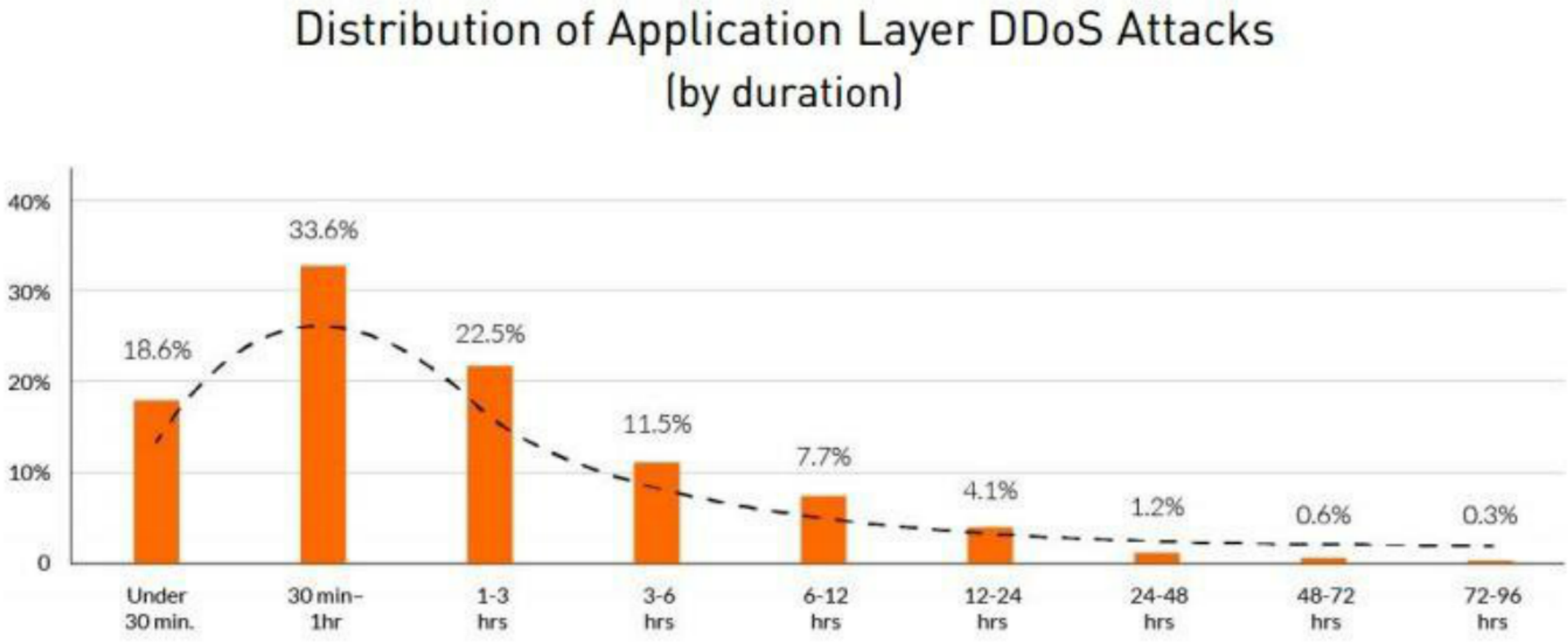


*Figure 10: Distribution of application layer DDoS attacks, by duration*

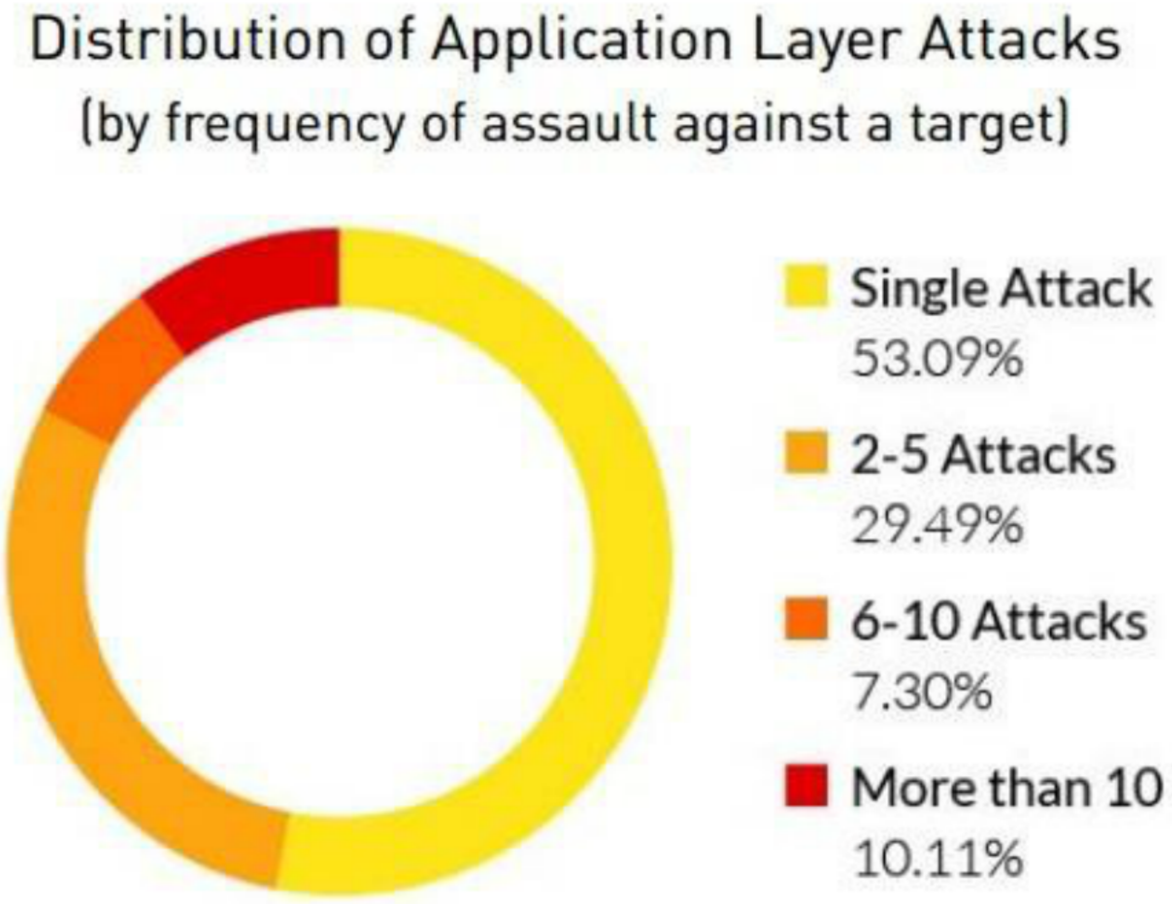


*Figure 11: Distribution of application layer attacks, by frequency of assault against a target*

# Botnet Activity and Geolocation

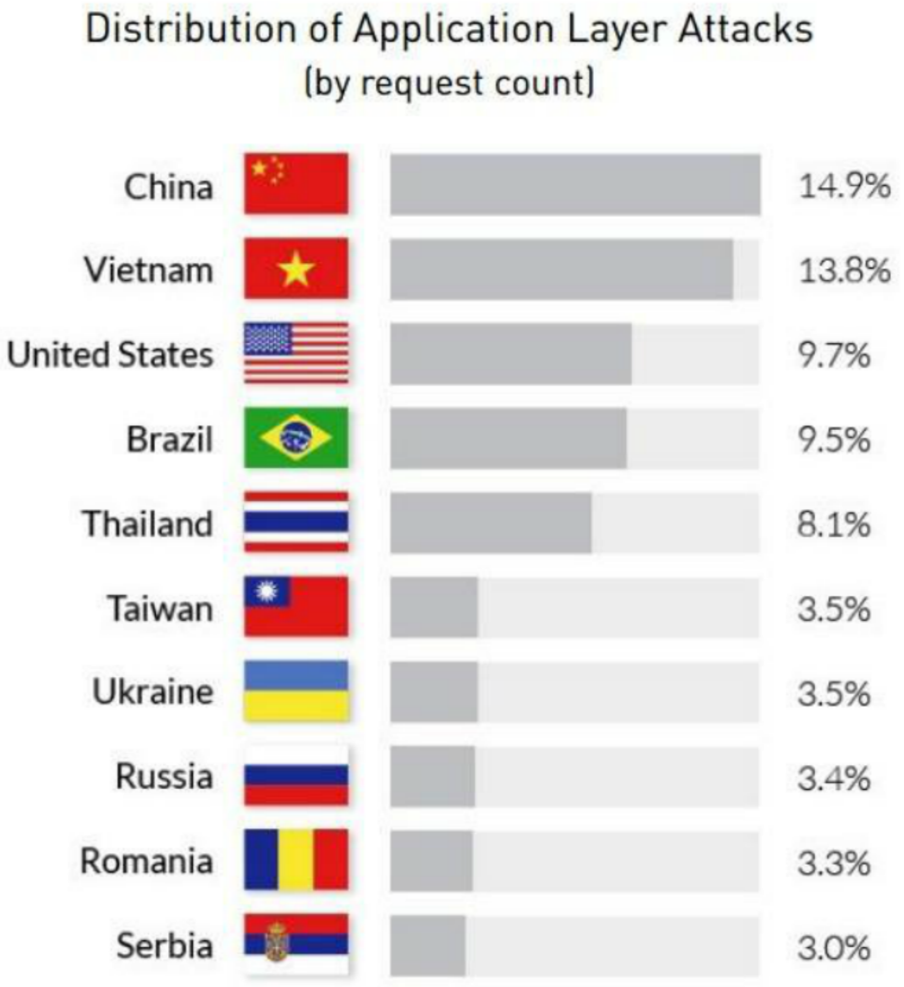


*Figure 12: Distribution of application layer attacks, by request count*

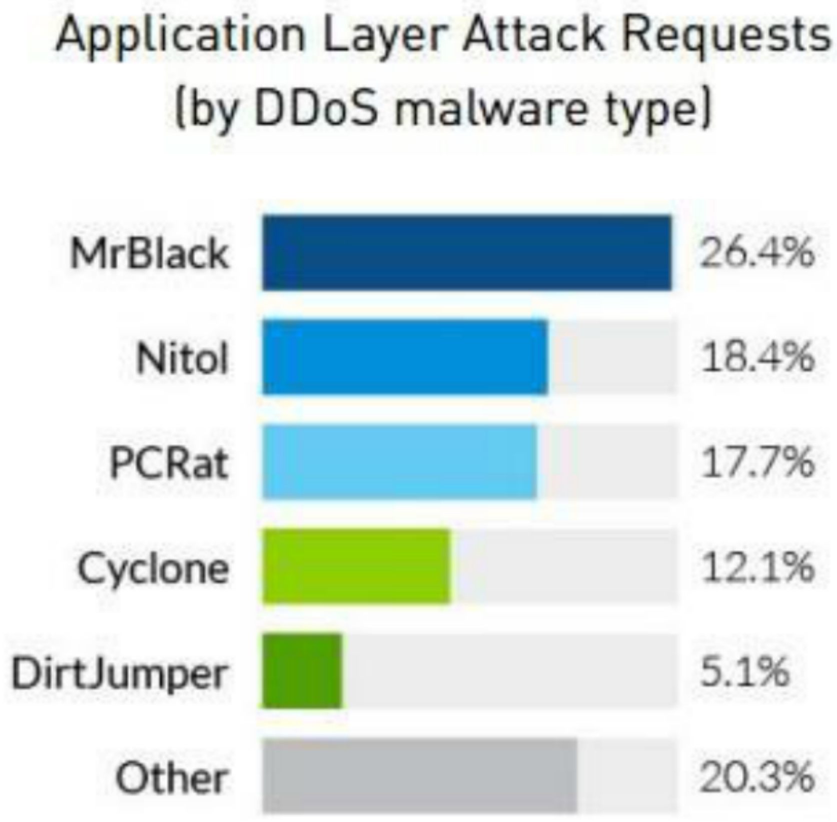


*Figure 13: Distribution of application layer attack requests, by DDoS malware type*

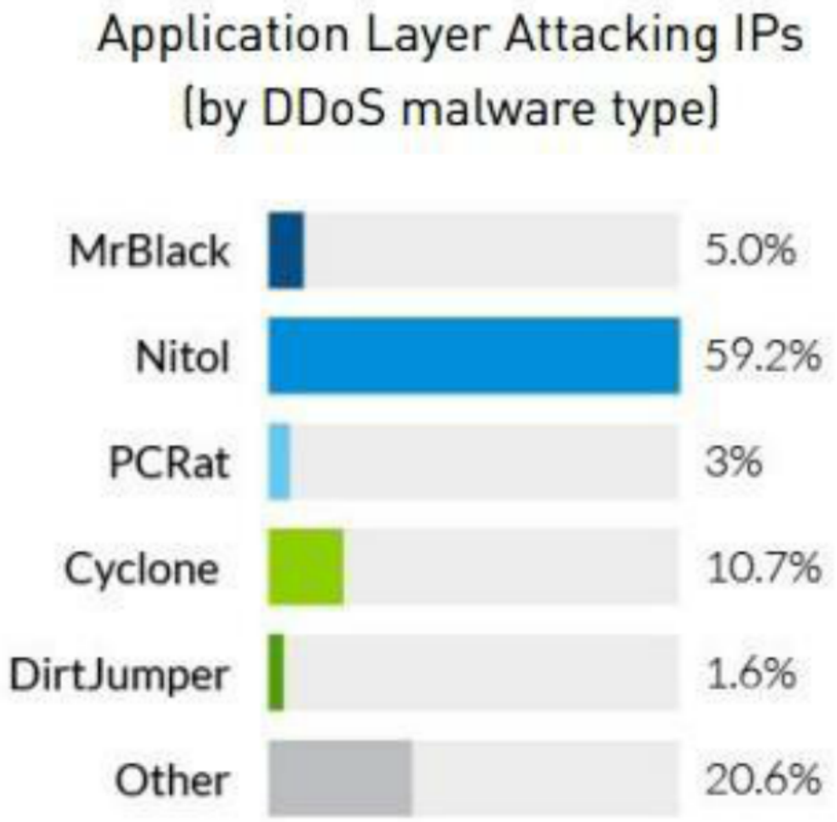


*Figure 14: Distribution of application layer attacking IPs, by DDoS malware type*

# Questions and Answers

## What is the main goal of DDoS Attacks?

> To render a server or a system unable to function and service its intended users

## What does the command structure for botnets look like?

> From top to bottom: Botnet Master -> Command and Control servers -> Zombie Bots

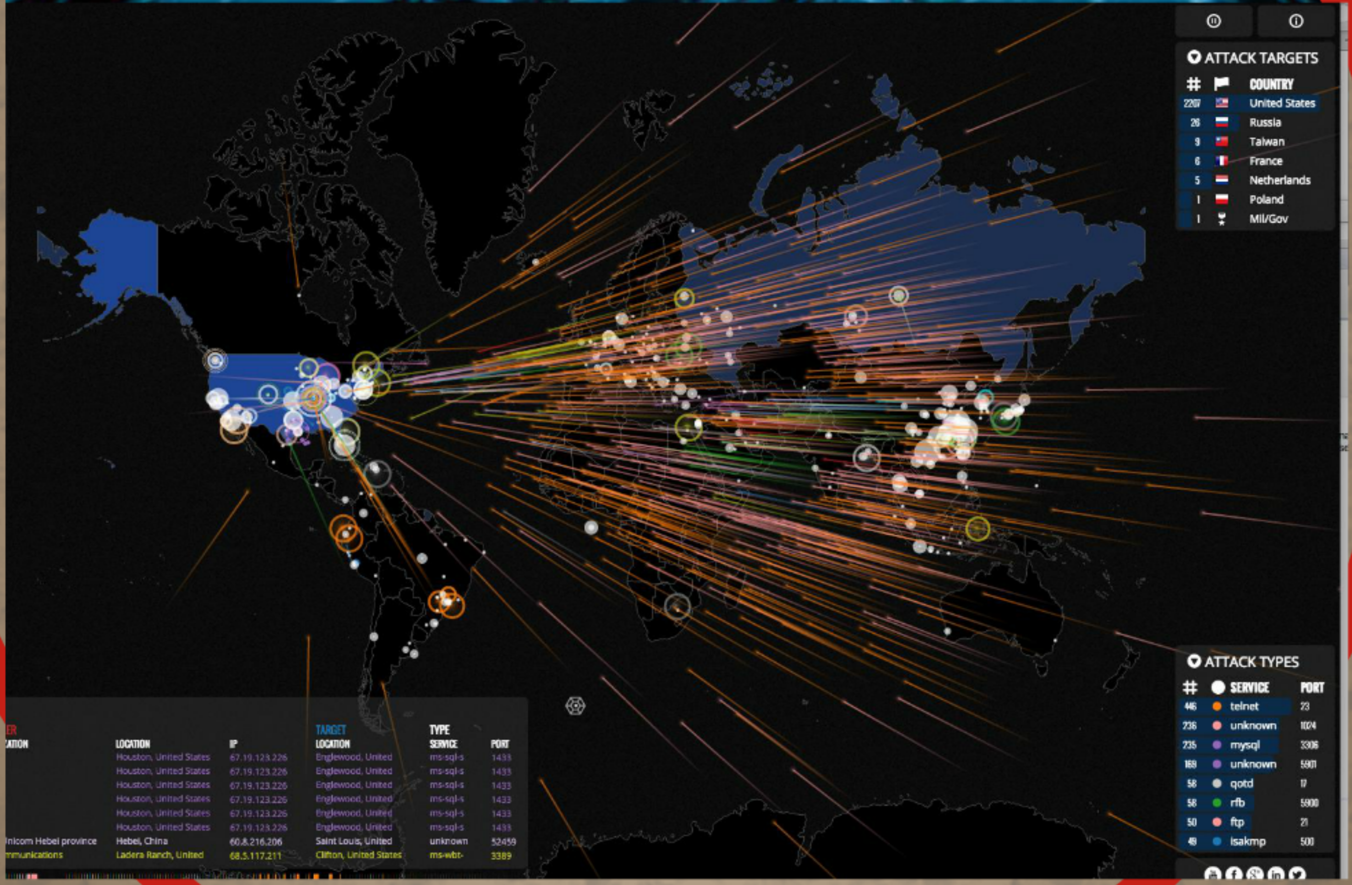
## How long do most DDoS attacks last for?

> Over half of all DDoS attacks last 30 minutes or less

ed by
IP

al user
affic
rs from

# Thank You!



ATTACK TARGETS

| # | ⚑ | COUNTRY |
|---|---|---|
| 2207 | 🇺🇸 | United States |
| 26 | 🇷🇺 | Russia |
| 9 | 🇹🇼 | Taiwan |
| 6 | 🇫🇷 | France |
| 5 | 🇳🇱 | Netherlands |
| 1 | 🇵🇱 | Poland |
| 1 | ★ | Mil/Gov |

| ER | | | TARGET | TYPE | |
|---|---|---|---|---|---|
| ATION | LOCATION | IP | LOCATION | SERVICE | PORT |
| | Houston, United States | 67.19.123.226 | Englewood, United | ms-sql-s | 1433 |
| | Houston, United States | 67.19.123.226 | Englewood, United | ms-sql-s | 1433 |
| | Houston, United States | 67.19.123.226 | Englewood, United | ms-sql-s | 1433 |
| | Houston, United States | 67.19.123.226 | Englewood, United | ms-sql-s | 1433 |
| | Houston, United States | 67.19.123.226 | Englewood, United | ms-sql-s | 1433 |
| | Houston, United States | 67.19.123.226 | Englewood, United | ms-sql-s | 1433 |
| Jnicom Hebei province | Hebei, China | 60.8.216.206 | Saint Louis, United | unknown | 52459 |
| mmunications | Ladera Ranch, United | 68.5.117.211 | Clifton, United States | ms-wbt- | 3389 |

ATTACK TYPES

| # | ● | SERVICE | PORT |
|---|---|---|---|
| 446 | ● | telnet | 23 |
| 236 | ● | unknown | 1024 |
| 235 | ● | mysql | 3306 |
| 169 | ● | unknown | 5901 |
| 58 | ● | qotd | 17 |
| 58 | ● | rfb | 5900 |
| 50 | ● | ftp | 21 |
| 49 | ● | isakmp | 500 |

## Purpose

- Extortion
- Bussiness competition
- Hacktivism
- Script kiddies
- Security Feints
- Internal Testing

## Consequences

- Disable a specific computer, service, or entire network
- Hit system resources like bandwidth, disk space, processor time, or routing information
- Crash the operating system
- Loss of revenue, brand damage, and angry customers

### Types of Attacks

- Protocol attacks- Use up all available connections to infrastructure
- Volumetric attacks – Consumes the bandwidth causing congestion
- Application attacks – The application layer is targeted

### Questions and Answers

What is the main goal of DDoS Attacks?

- To hinder a server or a system [illegible] function and [illegible]

What does the command structure for botnets look like?

- From top to bottom: Botnet Master -> Command and Control servers -> Zombie Bots

How long do most DDoS attacks last for?

- One half of all DDoS attacks lasted 30 minutes or less

### Types of attacks: Volumetric attacks

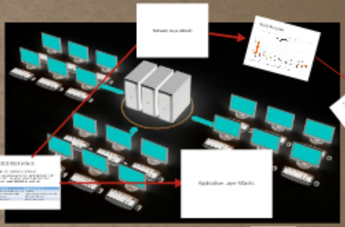
- Also known as floods
- Account for 65% of DDoS attacks
- Causes congestion by sending lots of traffic which overwhelm the sites bandwidth
- Example: ICMP floods

### Types of attacks: Protocol

- Target the connection state tables in infrastructure such as the firewall, load-balancers and web application servers
- Account for 20% of reported DDoS attacks in 2014
- Example: Ping of death –

### Types of Attacks: Application-layer

- 17% of DDoS attacks
- Over-exercises specific functions or features of a website with the intention to disable those functions or features
- Examples: HTTP flood



### DDoS = Distributed denial of service

- Multiple systems target a single system to take down a service, compromising availability
- These multiple systems are referred to a botnet

Visualization of DDos attack on World of Warcraft servers at Blizzard

### Issues

- DDoS attacks cannot be stopped by preventing access to a single IP address
- Difficult to distinguish normal user traffic from the attacking traffic
- DDoS prevents intended users from accessing the network

Thank You!

### How does a Botnet Work?

### How does a Botnet Work?

### What is a Botnet?

- A network of similar machines trying to complete repetitive tasks and objectives
- Devices include: web servers, personal network computers, mobile devices, or cable modems

### What does a Botnet do?

- A botnet can perform tasks such as:
  - Scanning for new targets
  - Exfiltrating data
  - Distributing malicious software (Malware such as viruses, worms, and keyloggers)
  - Stealing personal information or intellectual property
  - Attacking other targets (DDoS attacks)

# DDoS Attacks & Botnet

**CSE3482**
**By: Yang Liu, Harshilkumar Patel, Melissa Soon**