Brace Yo'Self: DDoS is Coming!

Dima Bekerman

IMPERVA®

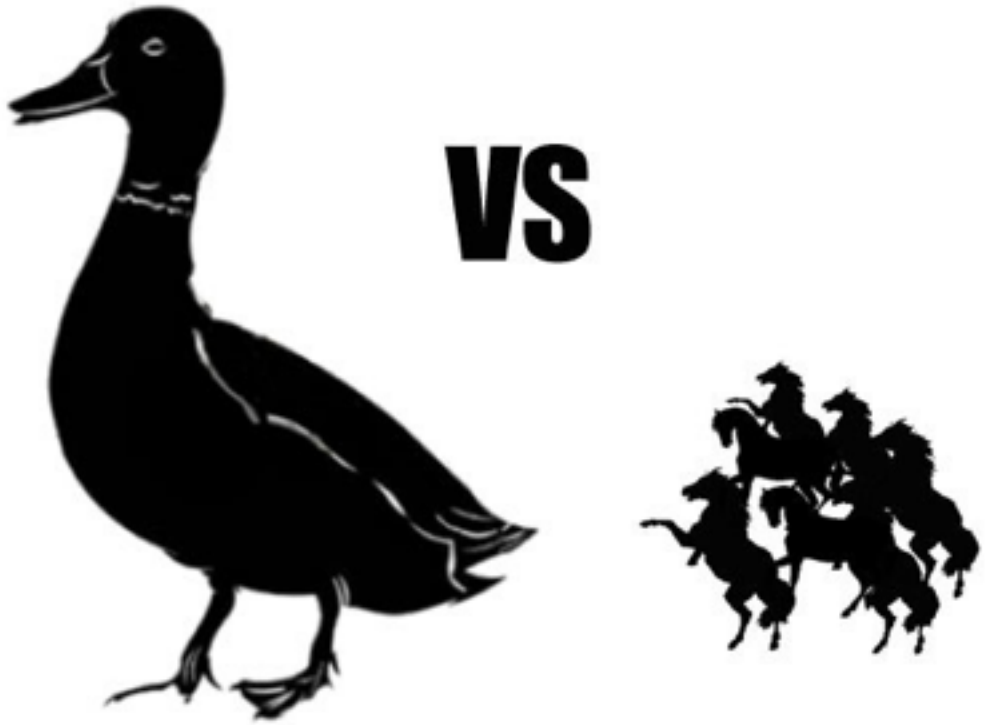
dima.about()

```
> dima.history
<· ["Machine Learning", "Sec. Analysis"]
> dima.employer
<· "Imperva Incapsula"
> dima.positionX
<· "Security Researcher"
> dima.social
<· {"TWT": "@unxmaster", "LNK": "Dima Bekerman"}
```

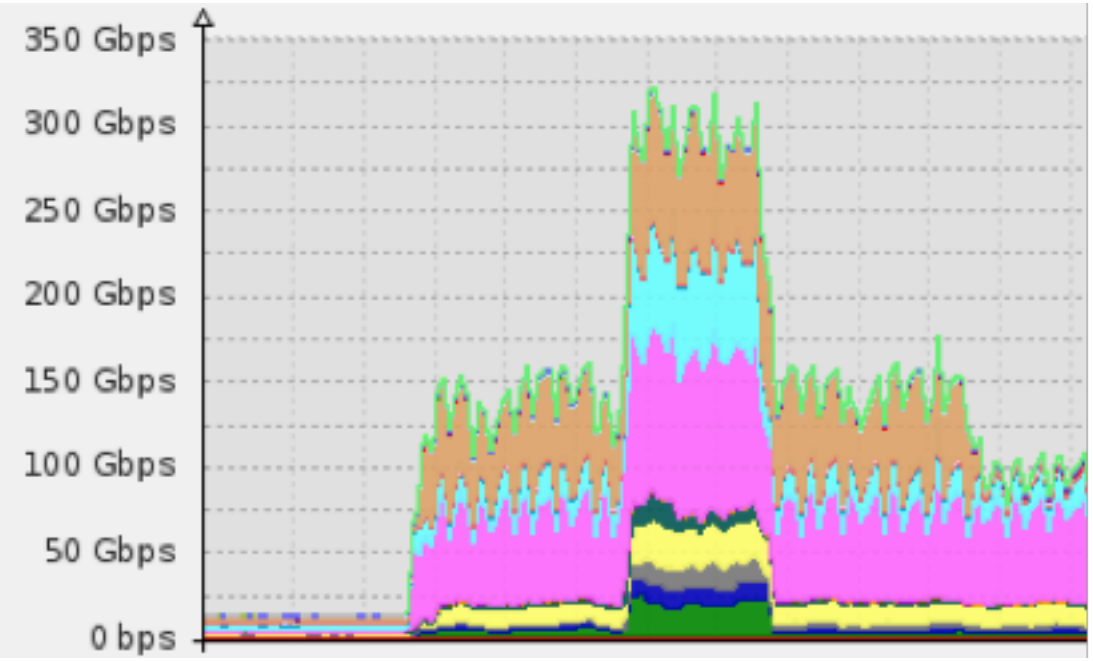
Remember…

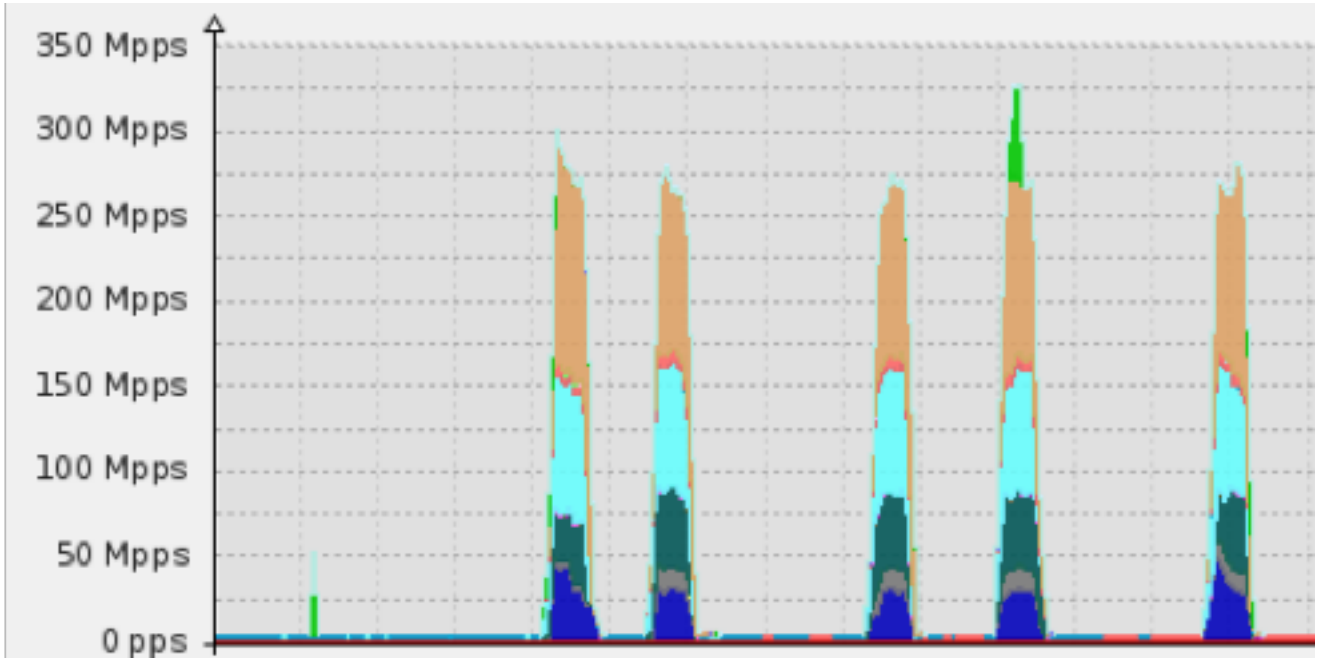
What happens in Lisbon stays in Lisbon

WHAT?

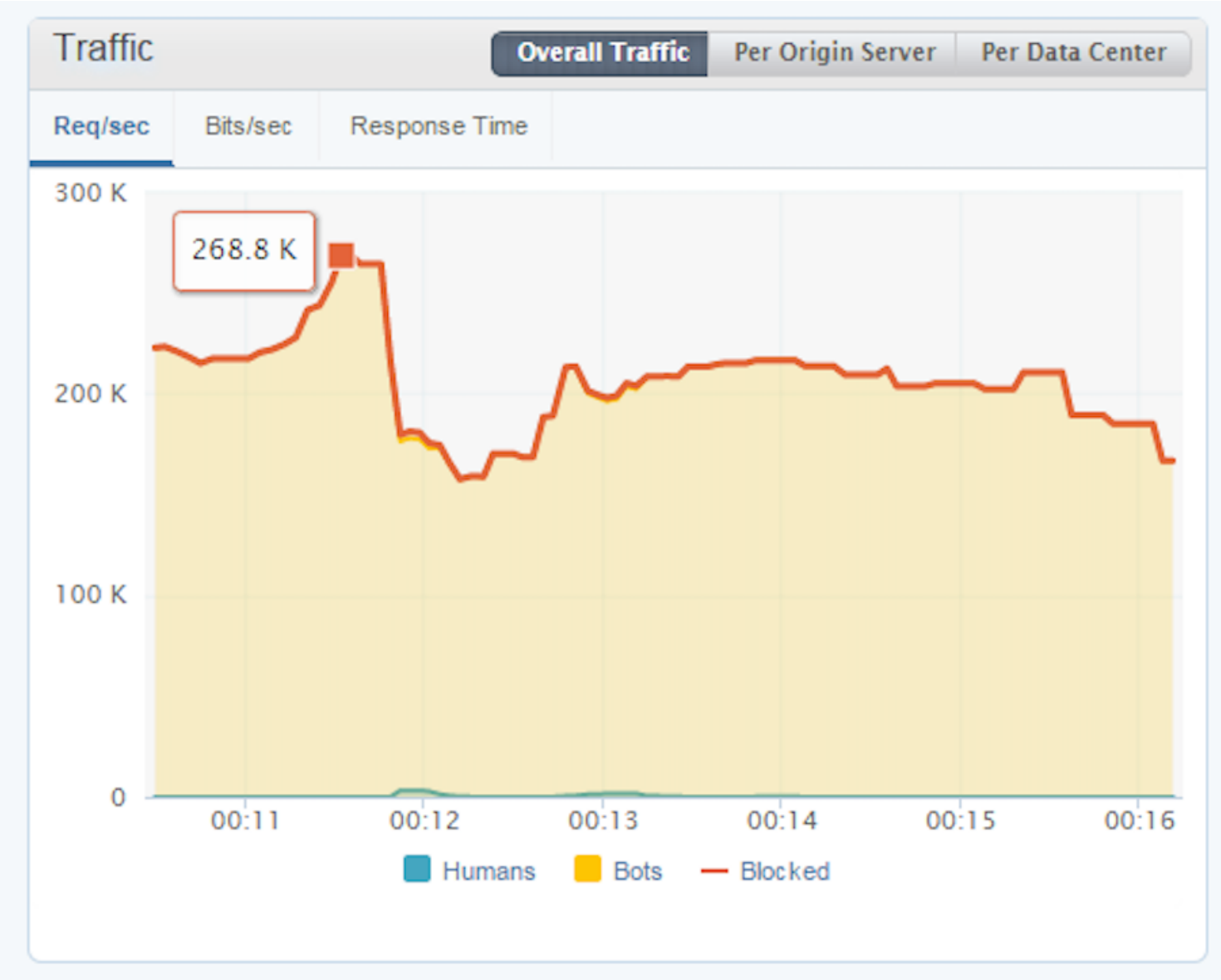


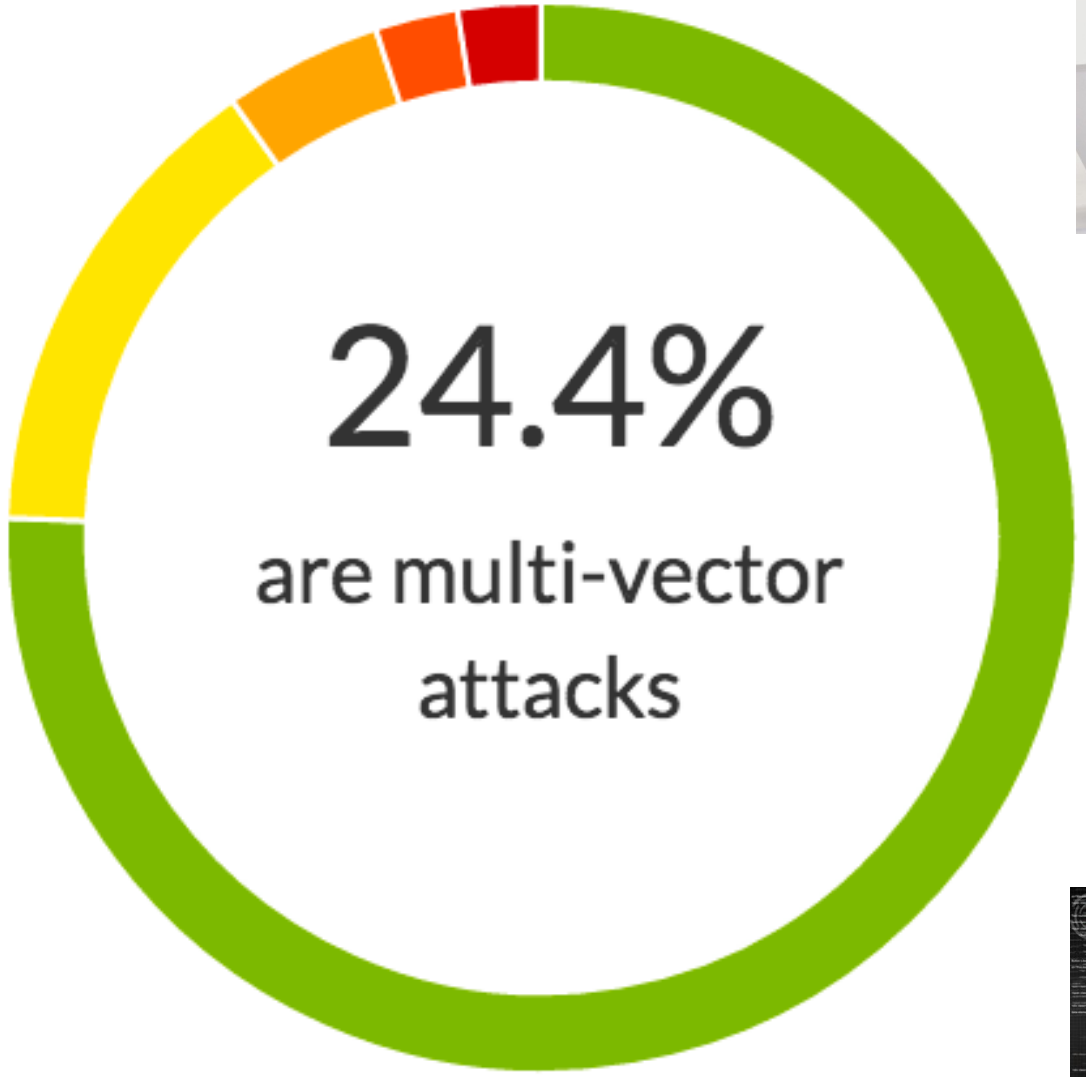
Volumetric Attacks





Layer 7 Attacks





1 vector
75.6%

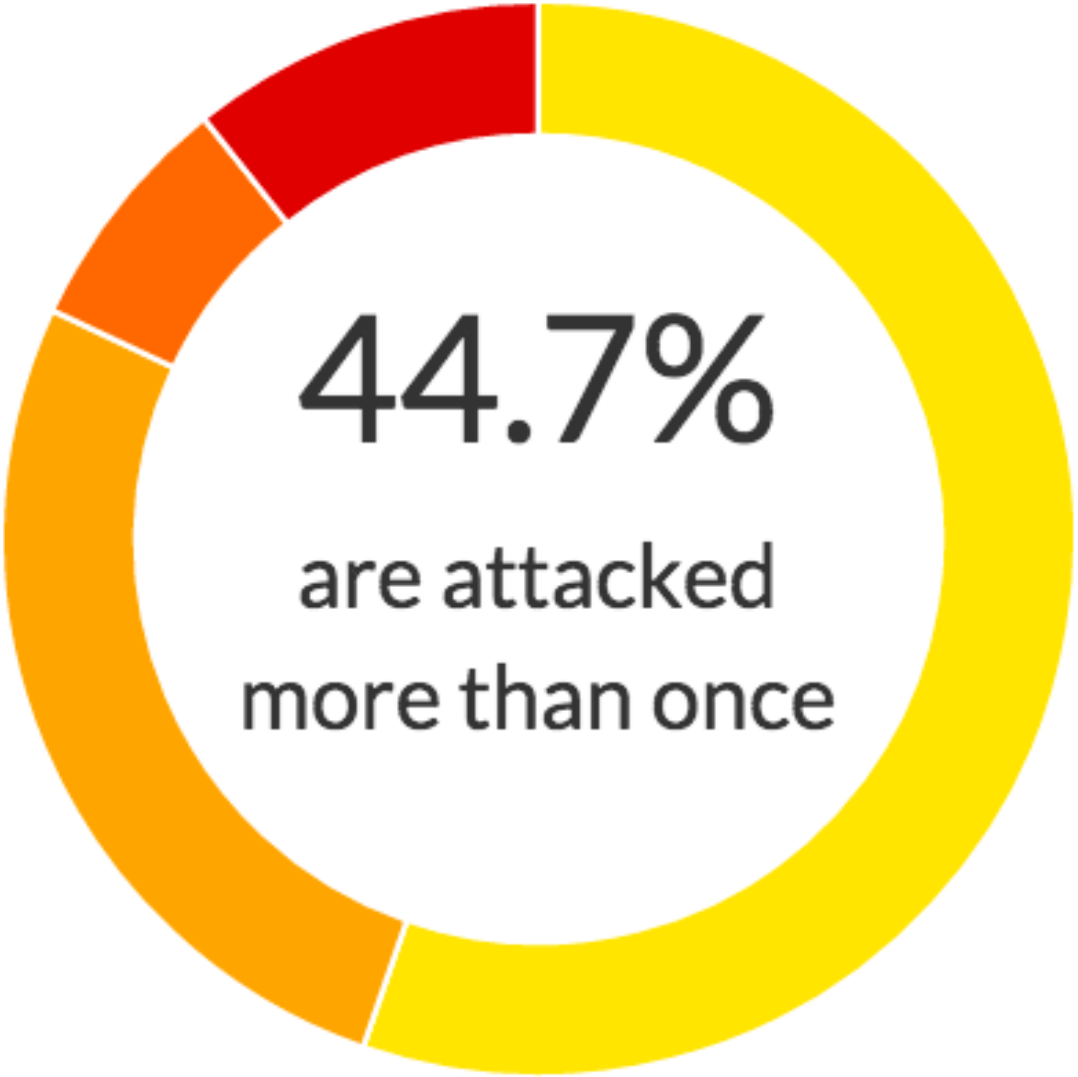
2 vector
14.6%

3 vector
4.8%

4 vector
2.5%

5+ vector
2.6%

IMPERVA®



Single Attack
55.3%

2-5 Attacks
26.7%

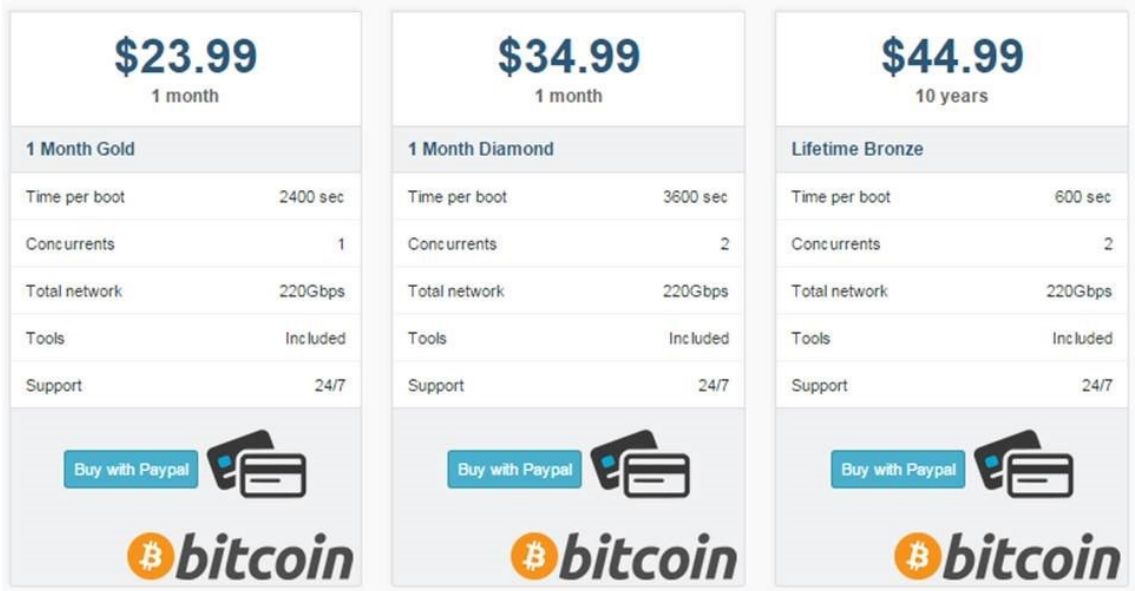
6-10 Attacks
7.3%

More than 10
10.7%

WHY?

Business Rivalry

- Causing financial impact or embarrassment to a business competitor
- Attacks are long in duration and target resources responsible for revenue generation
- New DDoS-for-hire services make this type of attack more common



Extortion

Sent: Monday, November 23, 2015 at 7:02 AM
From: [redacted]
To: [redacted]@cryptocoinsnews.com
Subject: Attacking Your Website

Hello,

We are attacking your website now and we have been taking it down for around 3 hours now.

Pay us 2 Bitcoins now to:
18RJA5BpFe4CGDFQG59jLNhPqYCRaEFng1

Or we will keep attacking your website, we have only used 20% of the machines we have enslaved

If you don't pay those 2 BTC today, you will have to pay 3 BTC tomorrow

Also, if I don't receive those 2 BTC within an hour, I will start mailing all the advertisers on your we

Pay me those 2 BTC and I will tell you the fatal security vulnetabilities on your site. Pay me those 2

Jon

All <redacted> sites are going under attack unless you pay 100 Bitcoin.

Pay to 1NbhLM43duL2J2tBX2qQWBojEm5fNSoMEp

Please note that it will not be easy to mitigate our attack, because
our current UDP flood power is 400-500 Gbps, so don't even bother.

Right now we are running small demonstrative attack just on your
<redacted>
Don't worry it will stop in 1 hour.
It's just to prove that we are serious.

We are aware that you probably don't have 100 BTC at the moment, so we are giving you 24 hours to get it and pay us.

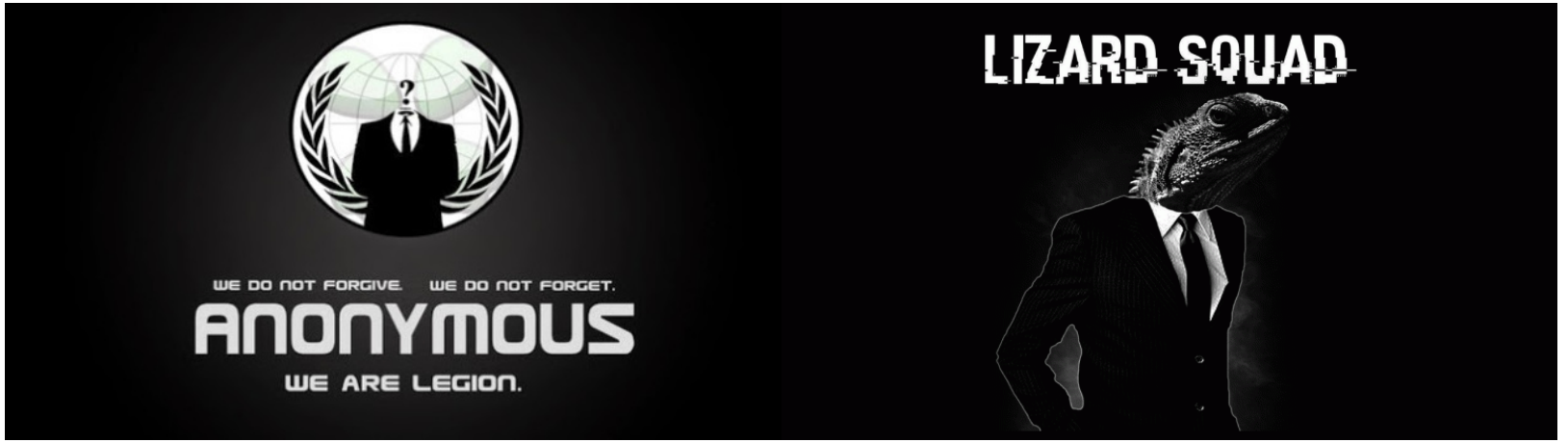
It's easy to get BTC from Webmoney. Just exchange WMZ to WMX and make withdrawal request to our BTC address at
https://wmx.wmtransfer.com/en-US/Home/Withdraw#

Or check this for best exchanger: http://howtobuybitcoins.info/

Current price of 1 BTC is about 220 USD.

“Hacktivists”

- Promoting a specific political agenda
- Often preceded by a public statement detailing a specific manifesto
- Victims of these attacks – well established brands or companies
- "Anonymous" - targeting Bank of America, Visa, MasterCard, the Church of Scientology and many others



State-Sponsored / Cyber-Terrorism

- Silencing of speech from certain sources
- Disruption to the target's telecommunications infrastructure and commerce
- Much larger and better orchestrated due to the significant resources of the attacker

- *March 2015: Code management platform GitHub (SFO, US) was attacked by DDoS originating from China (due to hosting anti-China resources)*
- *April 2007: Estonia got disconnected from the internet after being attacked by a three week DDoS attack. The attack was linked to a political dispute with Russia.*

Revenge / Personal Vandetta

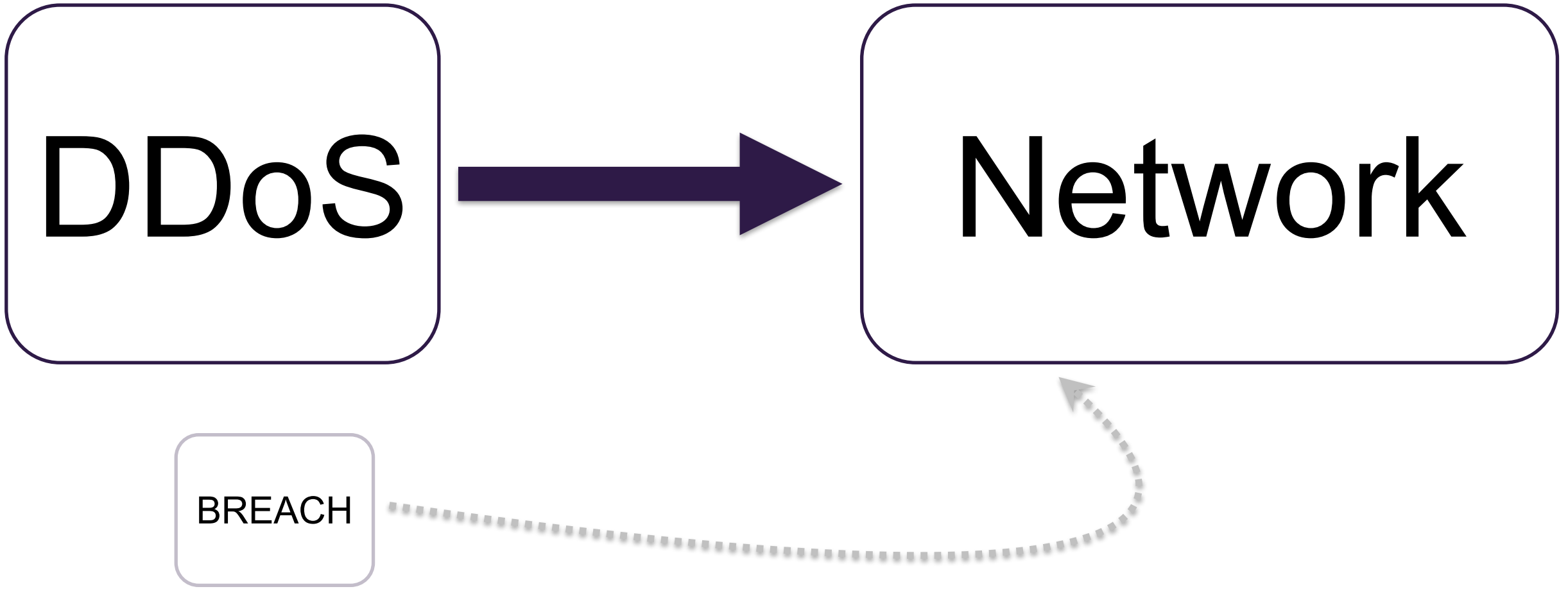
- Online disputes between individuals or small groups

"A UK man has been given eight and a half months in prison for launching a series of distributed denial-of-service attacks in 2013.

The 51 year old father of six had targeted sites including the UK Conservative Party, British Airways and a number of banks by flooding their websites with traffic and knocking them offline, a technique known as a distributed denial of service (DDoS) attack.

...the personal nature of the targets chosen suggest the DDoS attacks were more of a personal vendetta than an organized group effort..."

Smoke Screen



LOLZ

Mirai & Dyn

21 KrebsOnSecurity Hit With Record DDoS

SEP 16

October 21, 2016

Mirai botnets linked to massive DDoS attacks on Dyn DNS, Flashpoint says

Massive Cyberattack Hits America—Will Russia Take Down the Entire Internet if We Go to War?

10:00AM EDT 10/24/2016 | MICHAEL SNYDER

TWITTER EXPERIENCES OUTAGE FOLLOWING REPORTED DDOS ATTACK ON WIKILEAKS

7 Nov 2016

Massive DDoS Attacks Disable Internet Access Throughout Liberia

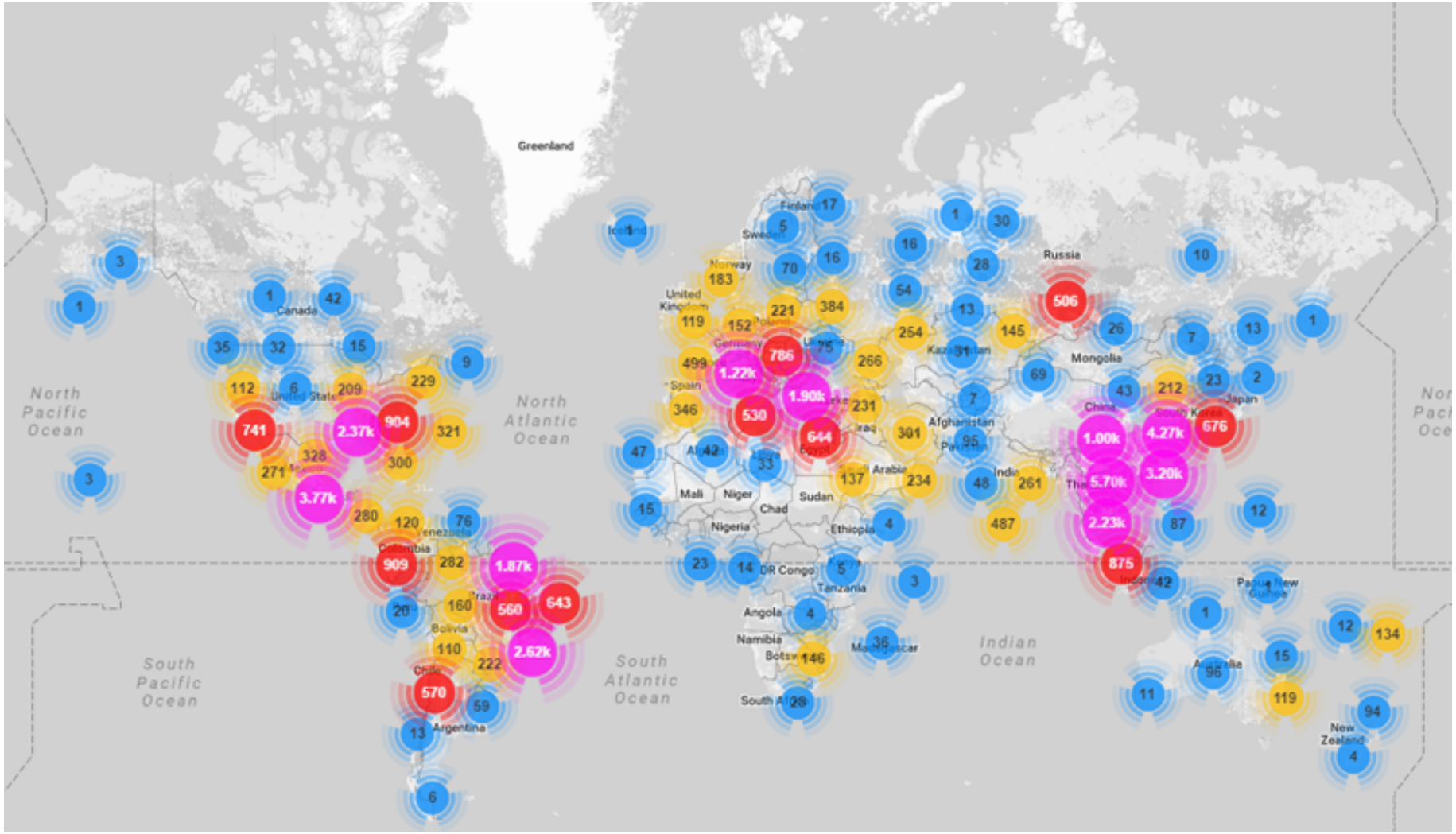
‘Mirai’ an IoT BotNet

- On September 30 user by the name of ‘Anna-senpai’ leaked the source code for Mirai bot

‘Mirai’ an IoT BotNet

- Infects IoT devices and is used as a launch platform for DDoS attacks.
- Performs wide-ranging scans of IP addresses to locate under-secured IoT devices that could be remotely accessed via easily guessable login credentials
- Implement DDoS for hire business model

Spread of ‘Mirai’ bot



‘Mirai’ attack types

```
void attack_tcp_syn(uint8_t targs_len, struct attack_target *targs,…)
void attack_tcp_ack(uint8_t targs_len, struct attack_target *targs,…)
void attack_tcp_stomp(uint8_t targs_len, struct attack_target *targs,…)

void attack_udp_generic(uint8_t targs_len, struct attack_target *targs,…)
void attack_udp_plain(uint8_t targs_len, struct attack_target *targs,…)
void attack_udp_dns(uint8_t targs_len, struct attack_target *targs,…)

void attack_gre_ip(uint8_t targs_len, struct attack_target *targs,…)
void attack_gre_eth(uint8_t targs_len, struct attack_target *targs,…)

void attack_app_http(uint8_t targs_len, struct attack_target *targs,…)
```

Anti-anti DDoS techniques

```
# define TABLE_ATK_DOSARREST              45  // "server: dosarrest"
# define TABLE_ATK_CLOUDFLARE_NGINX       46  // "server: cloudflare-nginx"

if (util_stristr(generic_memes, ret,
table_retrieve_val(TABLE_ATK_CLOUDFLARE_NGINX, NULL)) != -1)
    conn->protection_type = HTTP_PROT_CLOUDFLARE;

if (util_stristr(generic_memes, ret,
table_retrieve_val(TABLE_ATK_DOSARREST, NULL)) != -1)
    conn->protection_type = HTTP_PROT_DOSARREST;
```

Territory predator

- Eradicate other worms and Trojans on infected machine

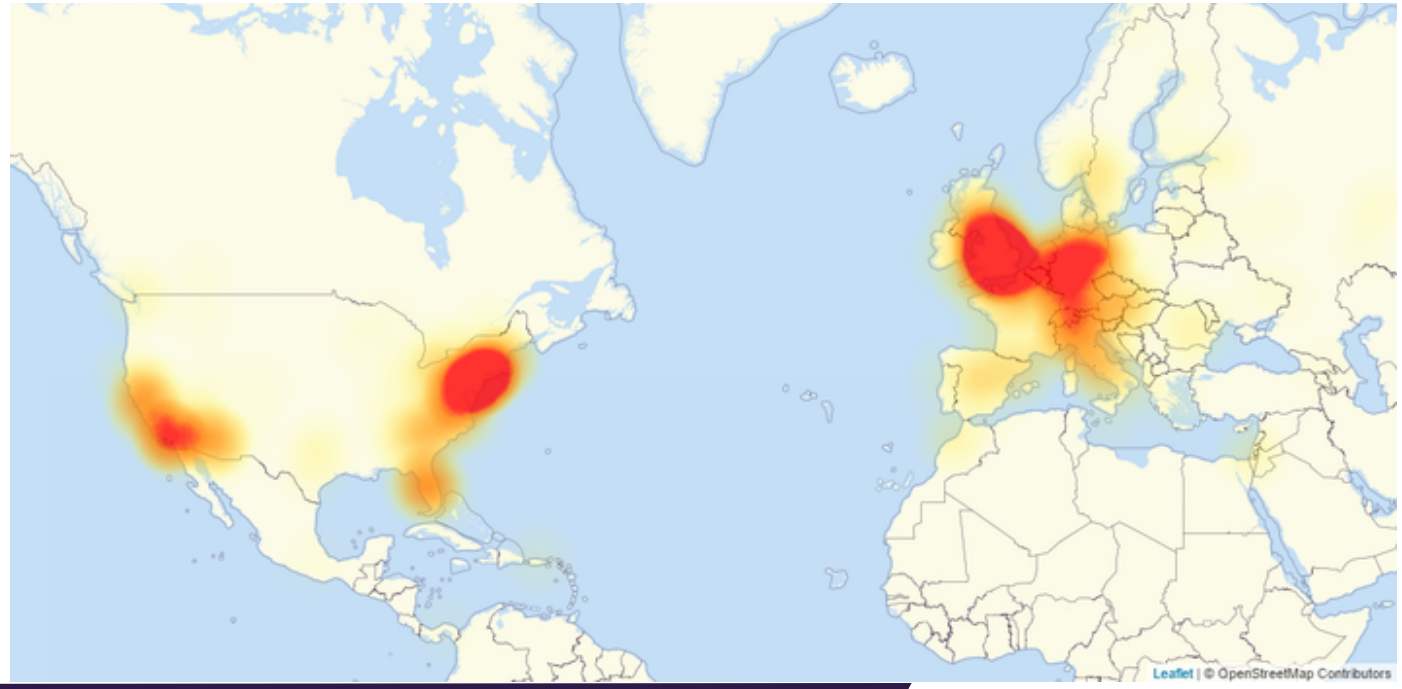
```
#DEFINE TABLE_MEM_QBOT              // REPORT %S:%S
#DEFINE TABLE_MEM_QBOT2             // HTTPFLOOD
#DEFINE TABLE_MEM_QBOT3             // LOLNOGTFO
#DEFINE TABLE_MEM_UPX               // \X58\X4D\X4E\X4E\X43\X50\X46\X22
#DEFINE TABLE_MEM_ZOLLARD           // ZOLLARD
#DEFINE TABLE_KILLER_ANIME          // .anime

killer_kill_by_port(htons(23))  // Kill telnet service
killer_kill_by_port(htons(22))  // Kill SSH service
killer_kill_by_port(htons(80))  // Kill HTTP service
```

DDoS for hire business model

```
func (this *Database) CreateUser(username string, password string, max_bots
    int, duration int, cooldown int)
    bool {
    ...
    this.db.Exec("INSERT INTO users (username, password, max_bots, admin, "
                 "last_paid, cooldown, duration_limit)"
                 "VALUES (?, ?, ?, 0, UNIX_TIMESTAMP(), ?, ?)",
                 username, password, max_bots, cooldown, duration)
    return true
}
```

Attack on Dyn

- Dyn confirms Mirai botnet as primary source of malicious attack traffic.
- TCP and UDP traffic over port 53.
- Packet flow bursts 40 to 50 times higher than normal



HOW?

IMPERVA®

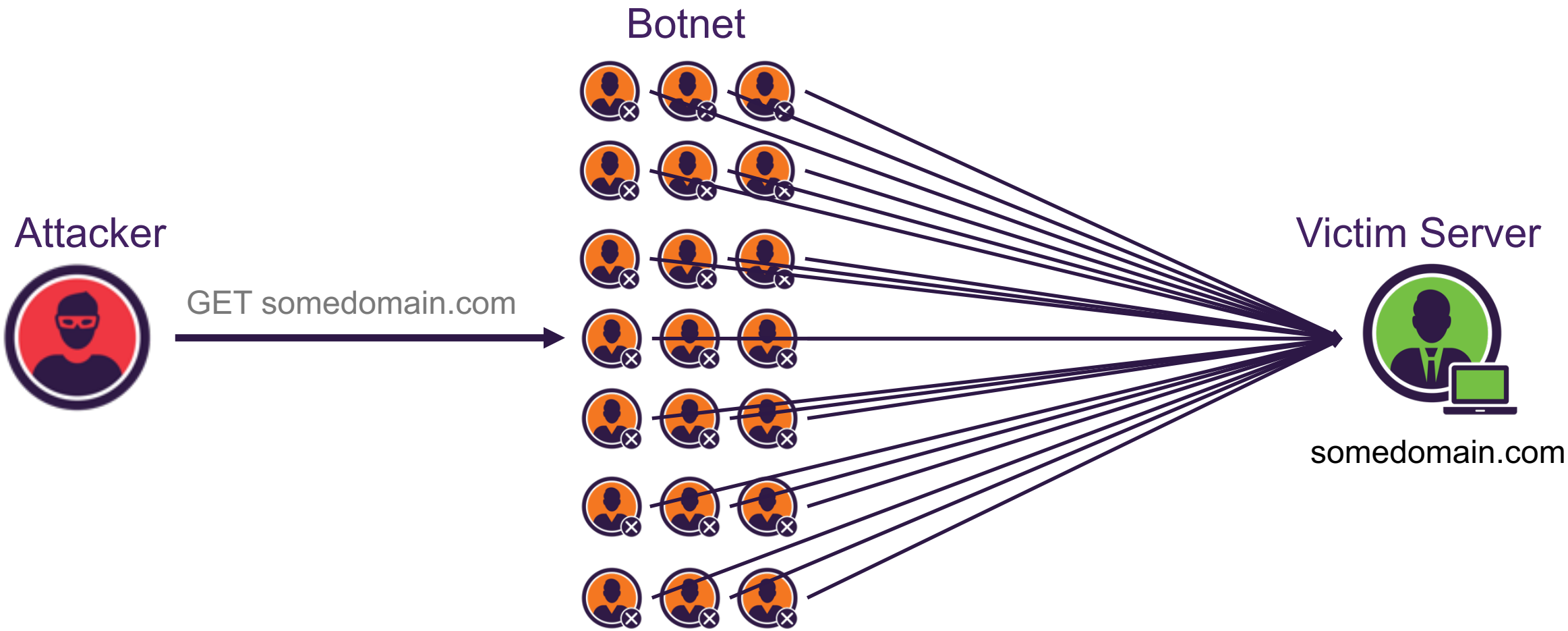
Application

IMPERVA®

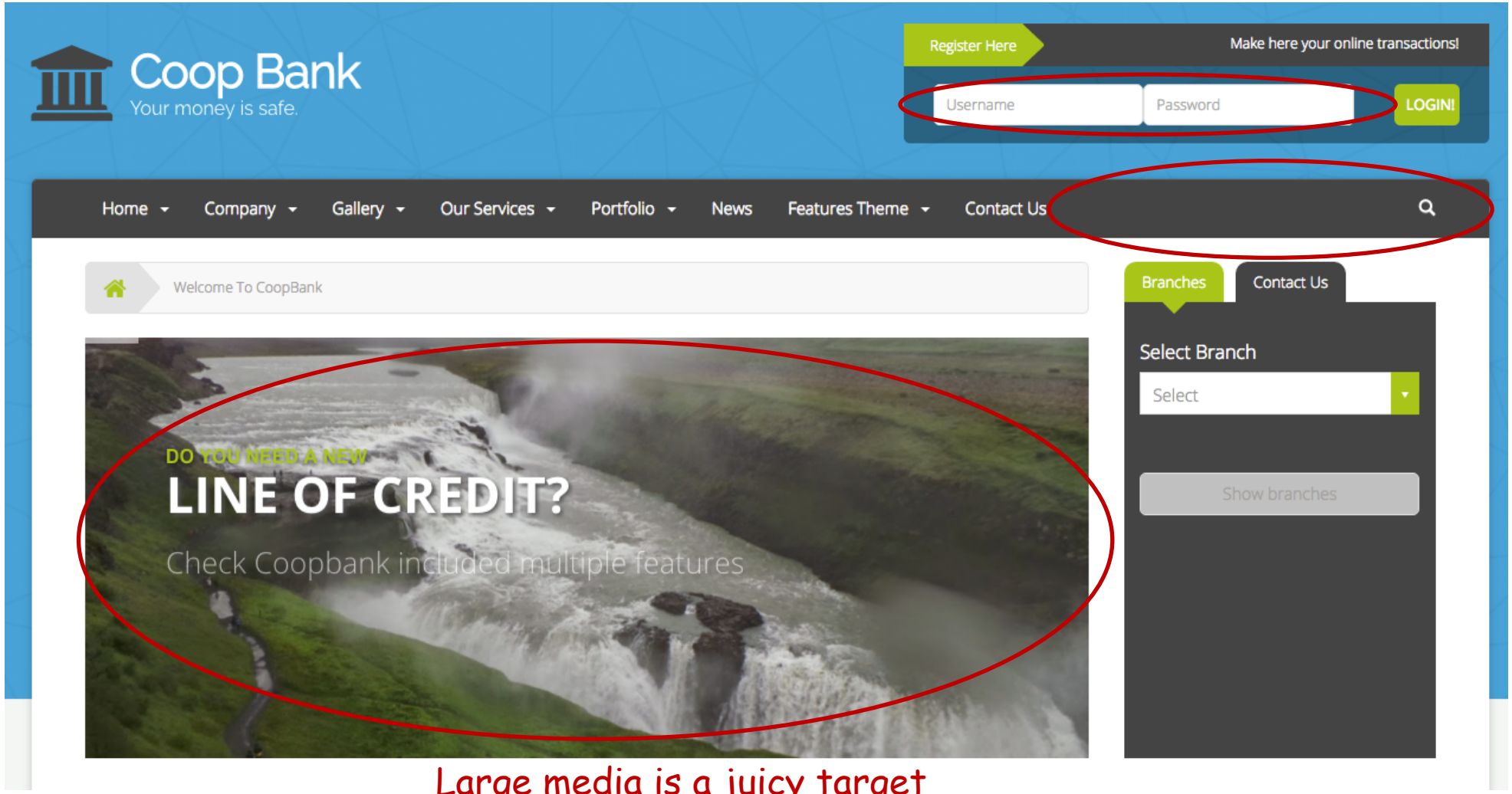
Web Application “Basic Schema” Quick Recap

```
POST /account/DoSomething HTTP/1.1
Host: test.domain.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:47.0)
Gecko/20100101 Firefox/47.0
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.google.com
Cookie: SESSION=1bc89e09d45b15eeba713c0ced4dcc9a6d42eccf01-%000;
Connection: keep-alive
Cache-Control: max-age=0

someParam=aaaaaaa
```

The Power of Bots



Finding the Attack Vectors



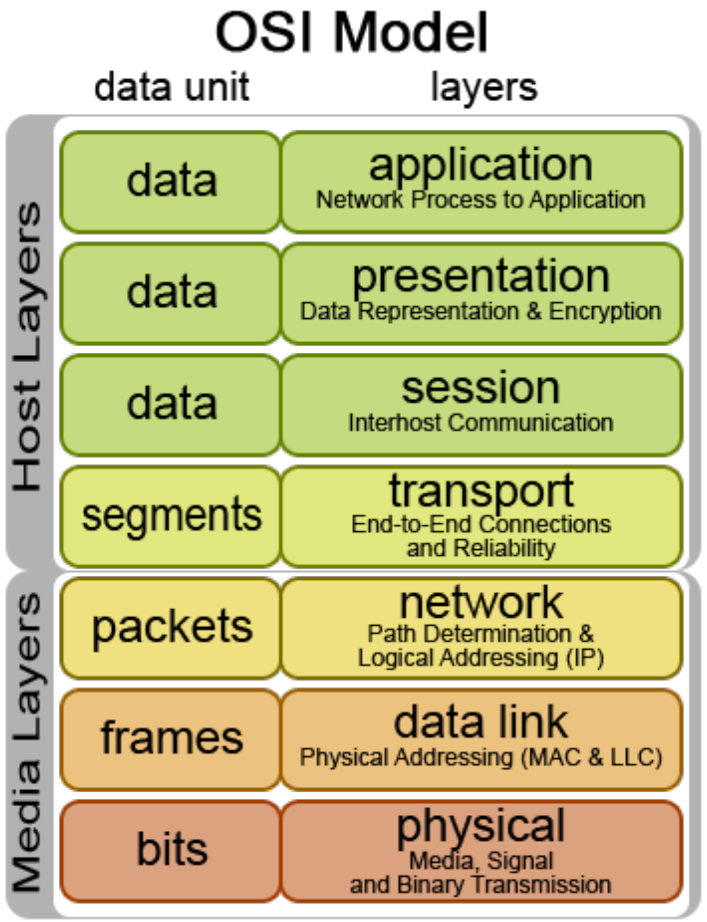
Search and Log-in hits DB and uses lots of CPU

Large media is a juicy target

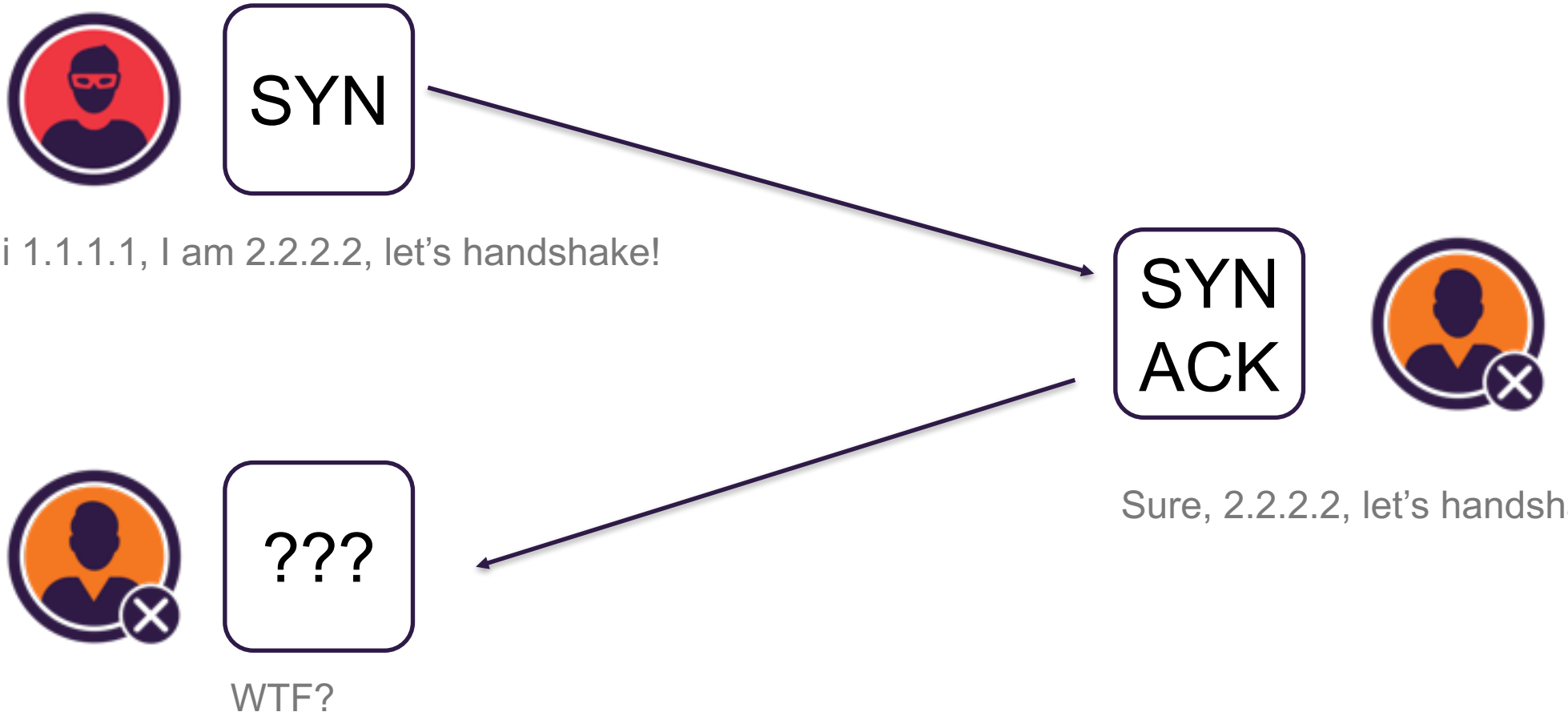
Volumetric

IMPERVA®

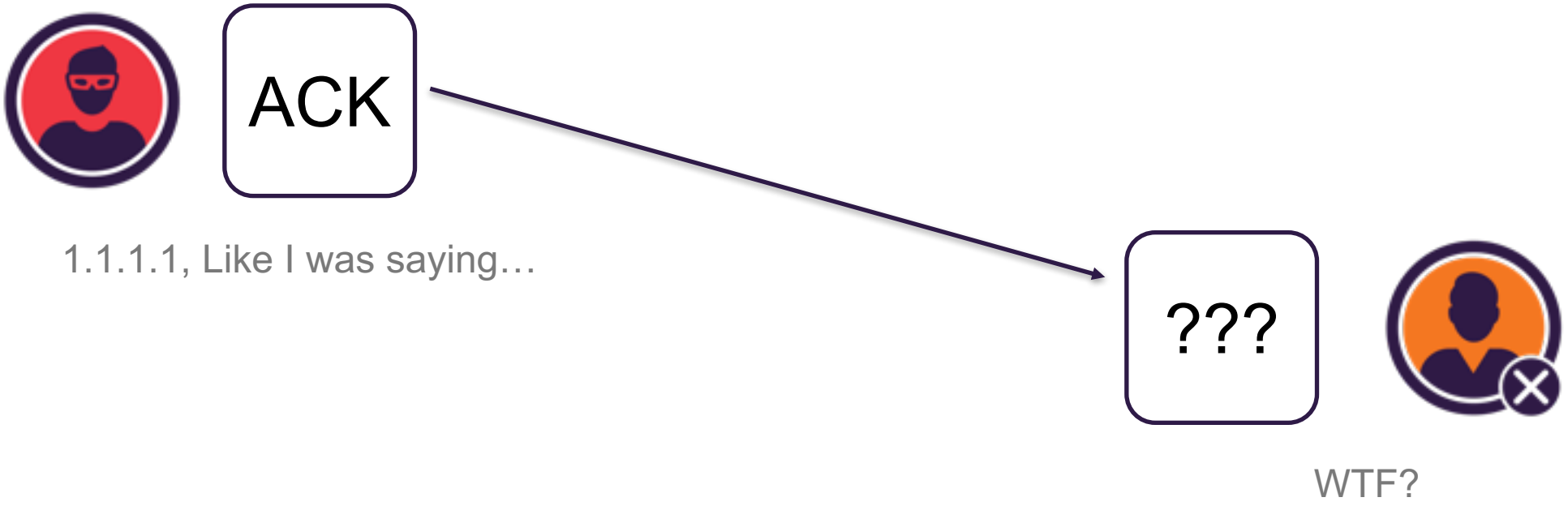
OSI Model Quick Recap



SYN Flood



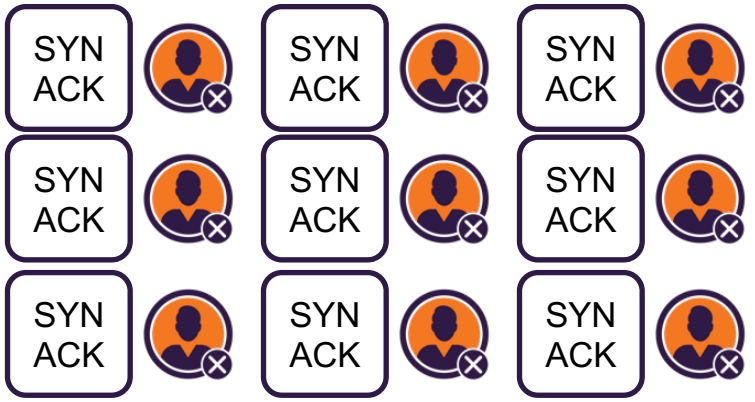
ACK Flood - Spoofed



ACK Flood - Reflected

SYN

Hi x.x.x.x, I am 2.2.2.2, let's handshake!



Sure, 2.2.2.2, let's handshake!

???

WTF?

DNS Amplification

DNS QR

Hi 1.1.1.1, I am 2.2.2.2, Please send any records on somedomain.com

DNS RES

???

WTF?

Sure, 2.2.2.2, Here are all the details:
www A 200.200.200.200
www2 A 200.200.200.201
… …

Demo Time

Tools Introduction - WireShark

Tools Introduction - Scapy @ Python

Obrigado!

THANK YOU!


@unxmaster


Dima Bekerman


dima@incapsula.com

IMPERVA®