DDoS Workshop

Brace Yourself: DDoS is Coming!

Polina Berman – Security Solutions Engineer
polina@incapsula.com

SANOG

Agenda

- Network and application layer attacks
- DDOS Background and Statistics
- Why DDOS?
- Example Botnet: Mirai
- Demo: DDOS Simulator and DNS Amplification attack
- DDOS Economy
- Attackers “Mode of Operation”
- Mitigation Techniques

What's DDoS in a nutshell

Cybercriminals and other threat actors MAIN GOAL is go after your data. PWC conducted a global survey that included responses from more than 10,000 IT security practitioners and found there was a 56% increase in data theft of intellectual property in 2015 compared to 2014.


4GIFs.com

A distinction between two main categories

Network Layer Attacks

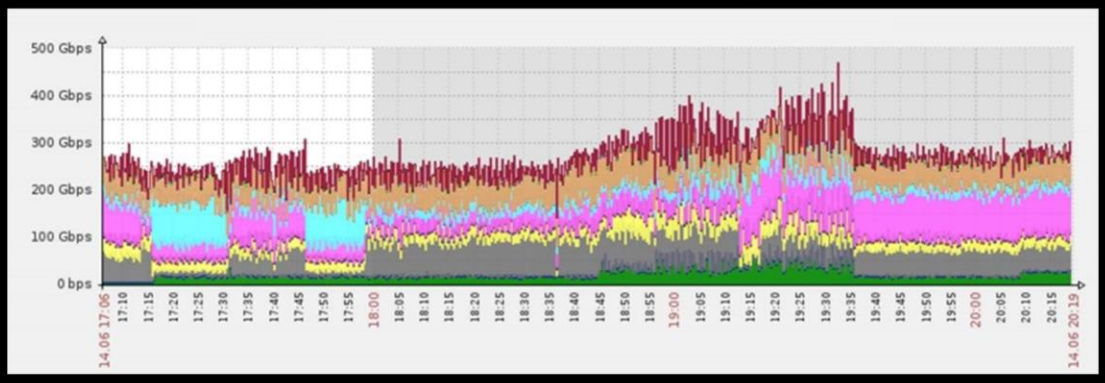
Application Layer Attacks

Network Layer Attacks

Generally referring to L3-4 attacks, but not only.

Network Layer Attack

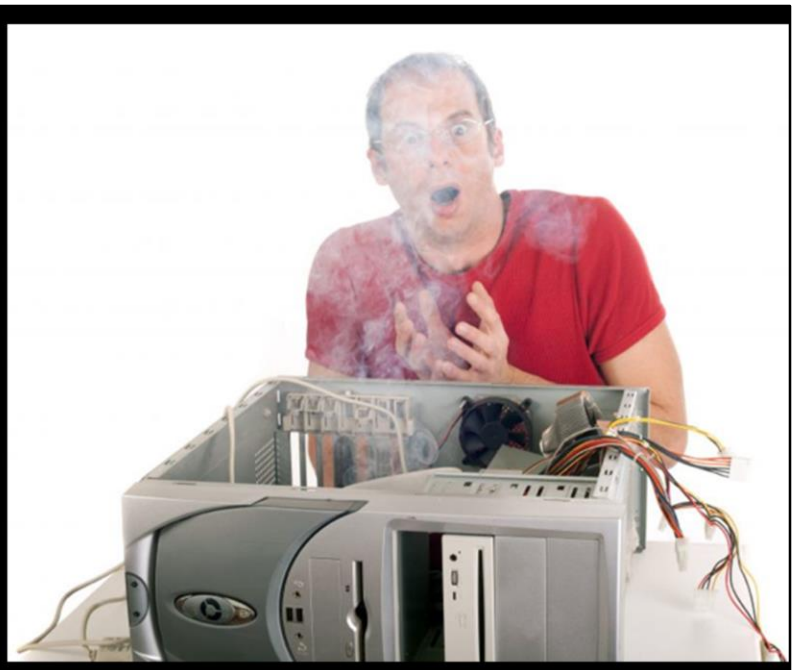
- From its first moment, this attack burst reached above 250 Gbps.
- It then slowly built up over the following hours, peaking at 470 Gbps at 19:32.
- After reaching this highpoint, attack traffic scaled back and completely resided within 30 min.



7

Source:
https://www.incapsula.com/blog/keep-calm-and-mitigate-470-gbps-ddos-attack.html

Layer 7 Attacks

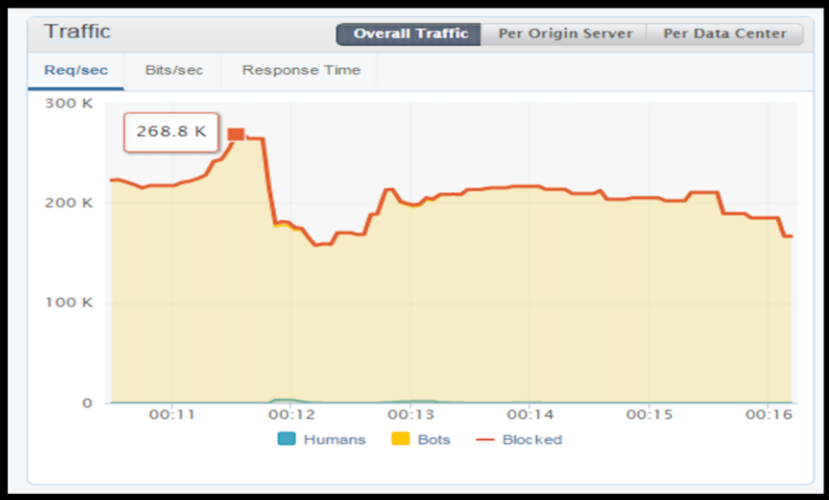


8

The goal in L7 attack is to dry your resources.
Usually focus on the web stack vulnerabilities or L7 known exploits.
Dynamic pages and API are the most vulnerable assets.

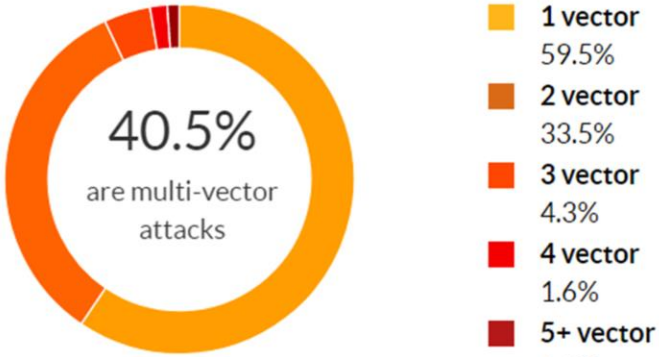
Like the guy who goes into CK shop and buy plenty of socks and pay in 10cents coins.

Layer 7 Attack Example



9

And this is how it looks like. Usually you'll see a spike in the number of request. Note that an average server can handle 20k at and even a powerful server will sweat hard when the 100k range is reached.



Distribution of network layer DDoS attacks, by number of vectors used

Source: Incapsula Global DDoS Threat Landscape Q1 2017
https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html

Distribution of application layer attacks, by frequency

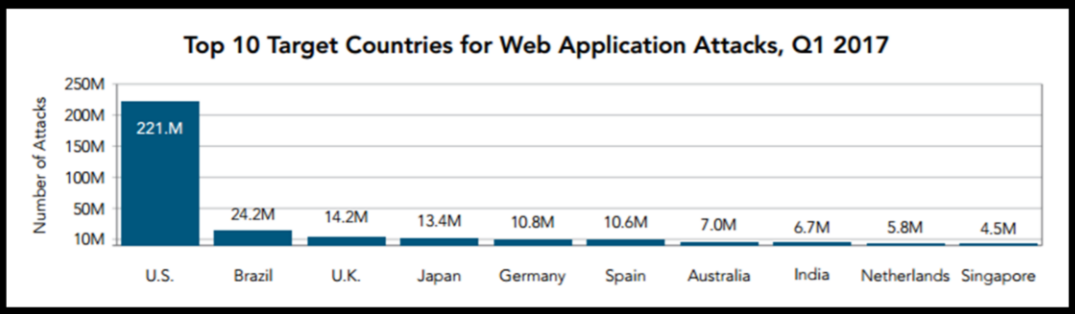
1
1

Source: Incapsula Global DDoS Threat Landscape Q1 2017
https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html

Source: Incapsula Global DDoS Threat Landscape Q4 2016

https://www.incapsula.com/ddos-report/ddos-report-q4-2016.html

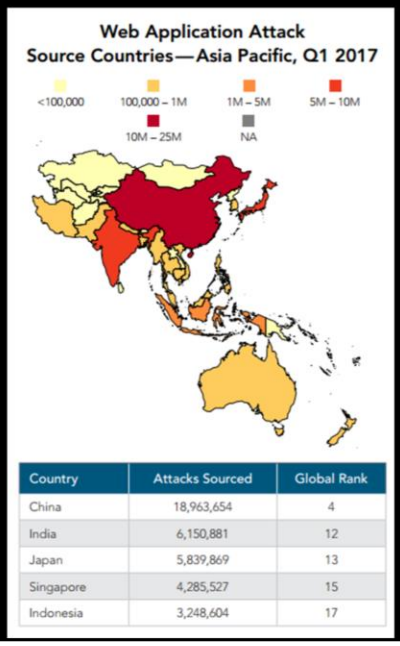
India among top 10 target countries: Akamai



Source: Akamai's state of the internet / security Q1 2017 report

https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-security-report.pdf

Web Application Attacks: India No.2 source country: Akamai



Country	Attacks Sourced	Global Rank
China	18,963,654	4
India	6,150,881	12
Japan	5,839,869	13
Singapore	4,285,527	15
Indonesia	3,248,604	17

Source: Akamai's state of the internet / security Q1 2017 report

https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-security-report.pdf

The longest attack recorded
More than 100 days

So if you still remember the question from before?!

Source: Incapsula SOC

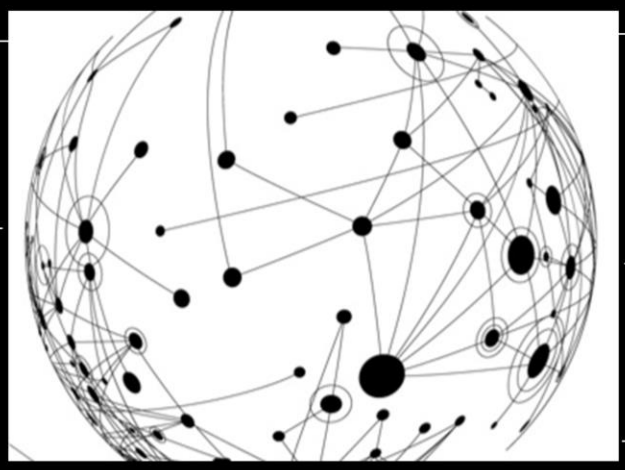
Catering service!

Rivalry of some sort. Or perhaps some Vegan hacktivists

Common pitfalls

I will use my FW/IPS

I have CDN in front



Increase Bandwidth

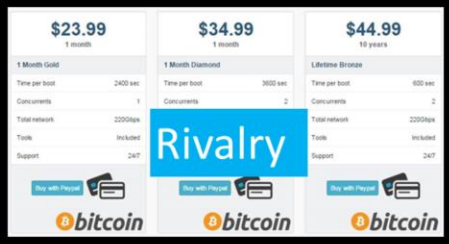
Other Responsibilities

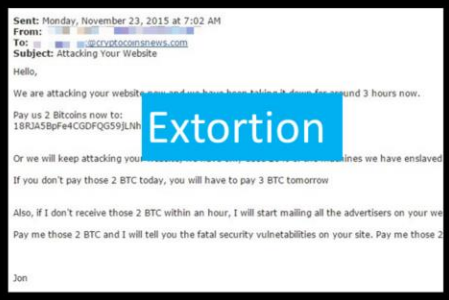
Default Password

17

Do you have password policy?

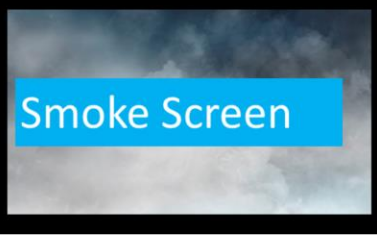
There are many reasons to djustify a DDoS act.
I've listed only few. In the next slides we going to cover each one


$23.99
1 month
1 Month Gold
Time per boot 2400 sec
Concurrents 1
Total network 220Gbps
Tools Included
Support 24/7
Buy with Paypal
bitcoin
$34.99
1 month
1 Month Diamond
Time per boot 3600 sec
Concurrents 2
Total network 220Gbps
Tools Included
Support 24/7
Buy with Paypal
bitcoin
$44.99
10 years
Lifetime Bronze
Time per boot 600 sec
Concurrents 2
Total network 220Gbps
Tools Included
Support 24/7
Buy with Paypal
bitcoin
Rivalry


Sent: Monday, November 23, 2015 at 7:02 AM
From:
To: @cryptocoinsnews.com
Subject: Attacking Your Website
Hello,
We are attacking your website
Pay us 2 Bitcoins now to:
18RJA5BpFe4CGDFQG59JLNh
Or we will keep attacking you
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
Extortion


Anonymous G
His Comment
Hacktivism


State Sponsored
YAHOO!


Smoke Screen

Rivlary

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

$23.99	$34.99	$44.99
1 month	1 month	10 years
1 Month Gold	1 Month Diamond	Lifetime Bronze
Time per boot 2400 sec	Time per boot 3600 sec	Time per boot 600 sec
Concurrents 1	Concurrents 2	Concurrents 2
Total network 220Gbps	Total network 220Gbps	Total network 220Gbps
Tools Included	Tools Included	Tools Included
Support 24/7	Support 24/7	Support 24/7
Buy with Paypal	Buy with Paypal	Buy with Paypal
bitcoin	bitcoin	bitcoin

2
0

Italian online poker – every time they had massive game they got attack. Choose our IP protection service to prevent it.

Extortion

Sent: Monday, November 23, 2015 at 7:02 AM
From:
To: @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#

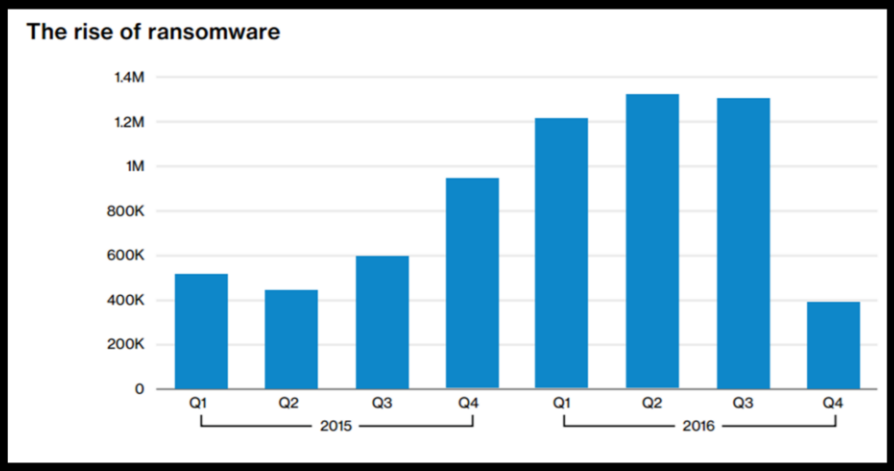
Or check this for best exchanger: http://howtobuybitcoins.info/

Current price of 1 BTC is about 220 USD.

avg is 15 Bitcoins (600$ each).
Extortion + Rivlary: If a certain industry sector is attacked, if you pay you both not get attacked, and your competition is attacked.

Example : Attack against emergency button for adults
The kid who wanted to buy Play Station he asked for $250

Ransom Notes are the Most Profitable Form of Writing: Verizon



22

Source: Verizon 2017 Data Breach Investigations Report

http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_execsummary_en_xg.pdf

“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

23

Monsanto – Energy sector, gets ongoing attack from Green activist

State-Sponsored / Cyber-Terrorism

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.*

24

The German newspaper who advertised Iran left wing and got attacked by Iran government

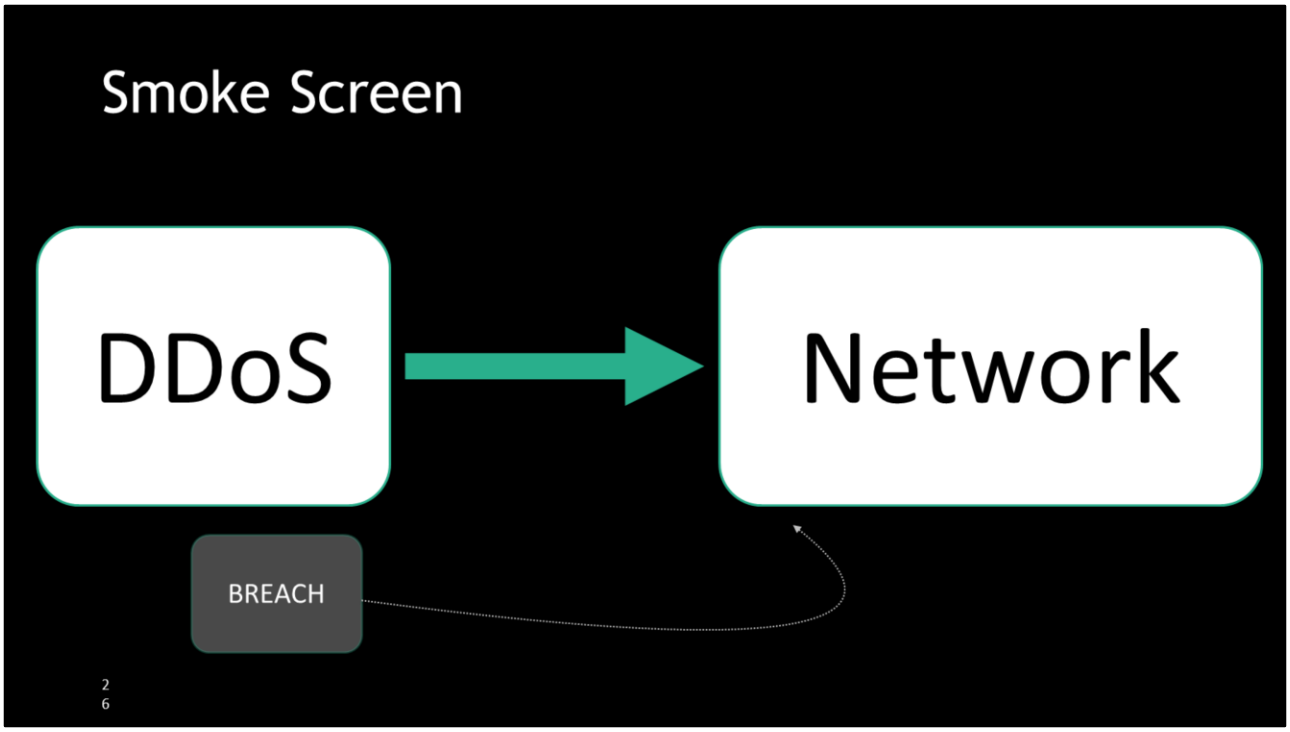
Revenge / Personal Vandetta

- 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…"

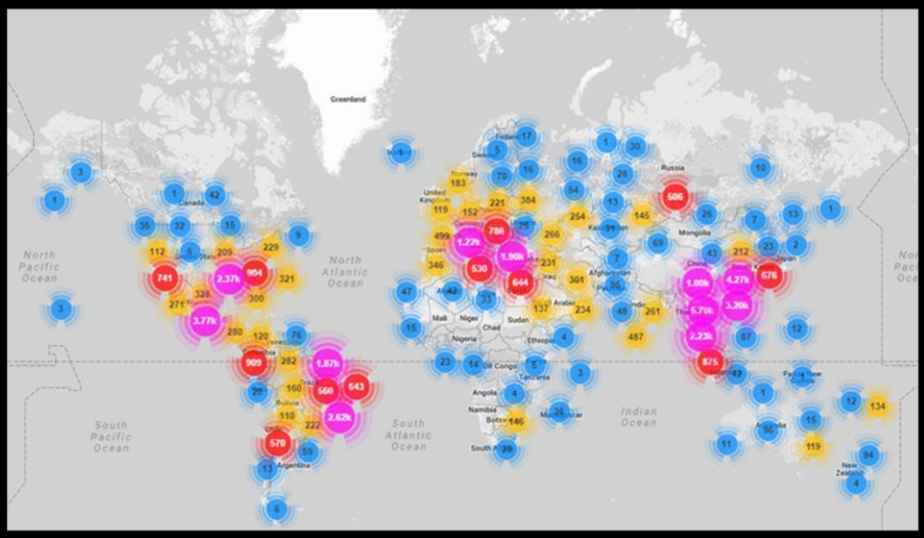
25

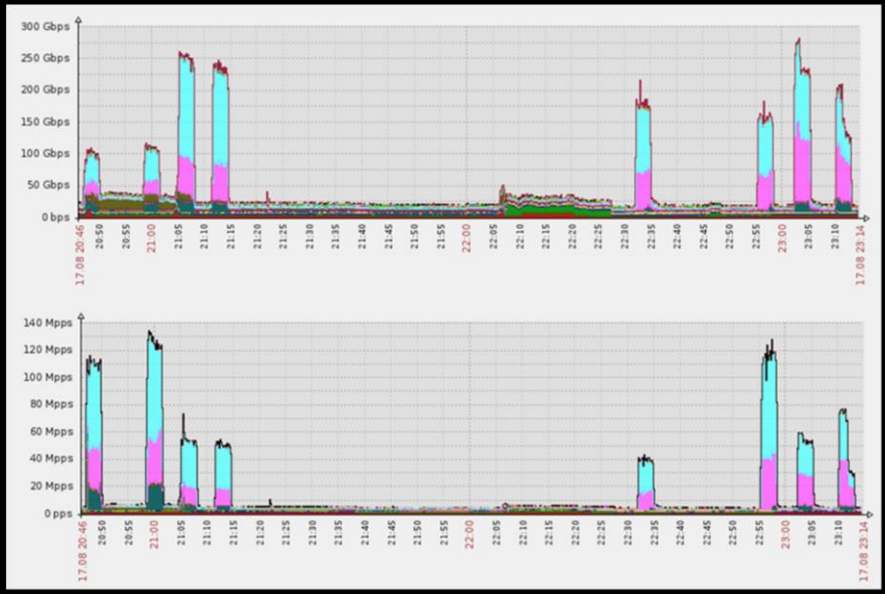
The UK person who launched an attack against British Airways



Possibly switching to a more vulnerable DR system

Mirai


Greenland
North Pacific Ocean
North Atlantic Ocean
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
Russia
Mongolia
Canada
Sudan
Chad
Nigeria
Angola
Namibia
Argentina
New Zealand


300 Gbps
250 Gbps
200 Gbps
150 Gbps
100 Gbps
50 Gbps
0 bps
140 Mpps
120 Mpps
100 Mpps
80 Mpps
60 Mpps
40 Mpps
20 Mpps
0 pps
17.08 20:46
20:50
20:55
21:00
21:05
21:10
21:15
21:20
21:25
21:30
21:35
21:40
21:45
21:50
21:55
22:00
22:05
22:10
22:15
22:20
22:25
22:30
22:35
22:40
22:45
22:50
22:55
23:00
23:05
23:10
17.08 23:14

```
root     realtek
root     00000000
admin    1111111
admin    1234
admin    12345
admin    54321
admin    123456
admin    7ujMko0admin
admin    1234
admin    pass
admin    meinsm
tech     tech
```

HTTP / GRE IP / GRE ETH / SYN ACK / STOMP / DNS / UDP

```
#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)) !=
                        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;
```

“Don’t mess with” list

```
127.0.0.0/8              - Loopback
0.0.0.0/8                - Invalid address space
3.0.0.0/8                - General Electric (GE)
15.0.0.0/7               - Hewlett-Packard (HP)
56.0.0.0/8               - US Postal Service
10.0.0.0/8               - Internal network
192.168.0.0/16           - Internal network
172.16.0.0/14            - Internal network
100.64.0.0/10            - IANA NAT reserved
169.254.0.0/16           - IANA NAT reserved
198.18.0.0/15            - IANA Special use
224.*.*.*+               - Multicast
6.0.0.0/7                - Department of Defense
11.0.0.0/8               - Department of Defense
21.0.0.0/8               - Department of Defense
22.0.0.0/8               - Department of Defense
26.0.0.0/8               - Department of Defense
28.0.0.0/7               - Department of Defense
30.0.0.0/8               - Department of Defense
33.0.0.0/8               - Department of Defense
55.0.0.0/8               - Department of Defense
214.0.0.0/7              - Department of Defense
```

A Territorial Predator

```
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
```

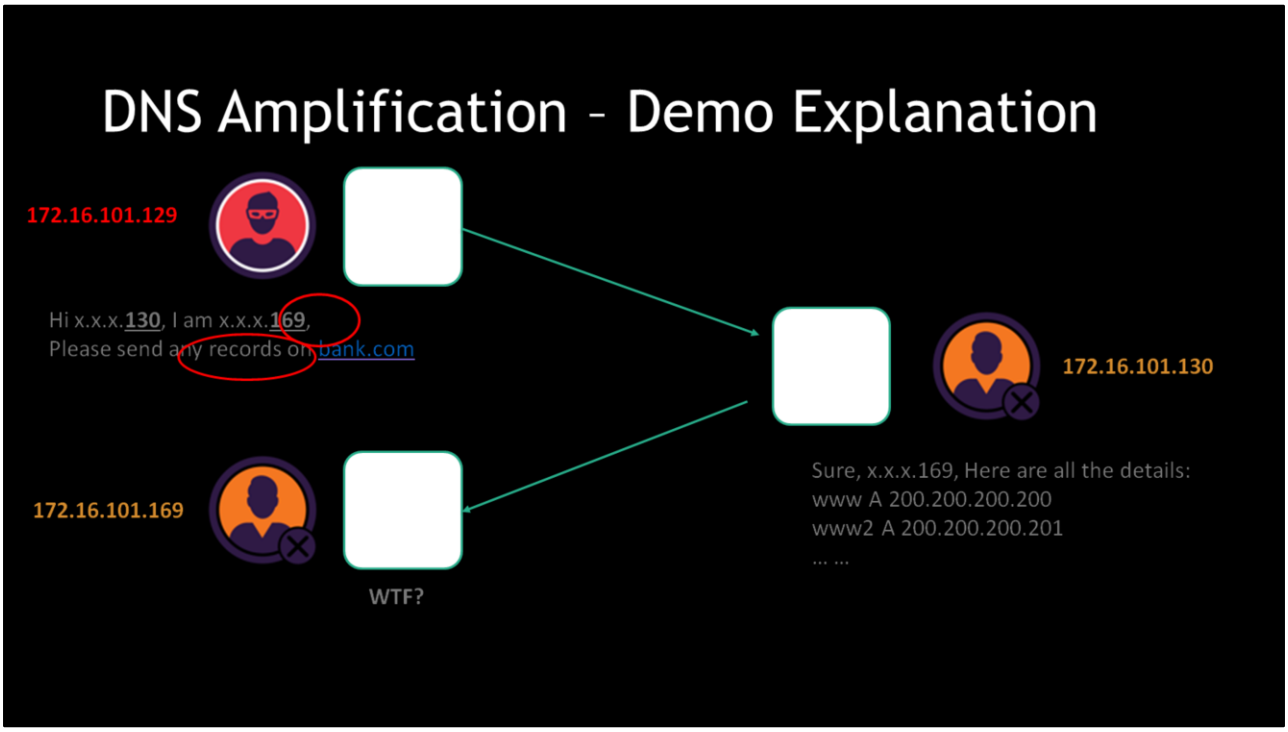
```
#DEFINE TABLE_MEM_QBOT            // REPORT %S:%S
#DEFINE TABLE_MEM_QBOT2           // HTTPFLOOD
#DEFINE TABLE_MEM_QBOT3           // LOLNOGTFO
#DEFINE TABLE_MEM_UPX             // \X58\X4D\X4E\X4E\X43\X50\X46\X22
#DEFINE TABLE_MEM_ZOLLARD         // ZOLLARD
```

Demo Time

Live Demo – placeholder to SANOG30 committee

- Part 1
  - Demonstration of DDOS simulator (tool developed internally at Incapsula)
  - Examples of various types of attacks and how it impacts internal network of an organization
  - ~30 minutes

- Part 2
  - DNS Amplification attack
  - ~30 minutes



create: IP() , UDP(), DNS(), DNSQR()

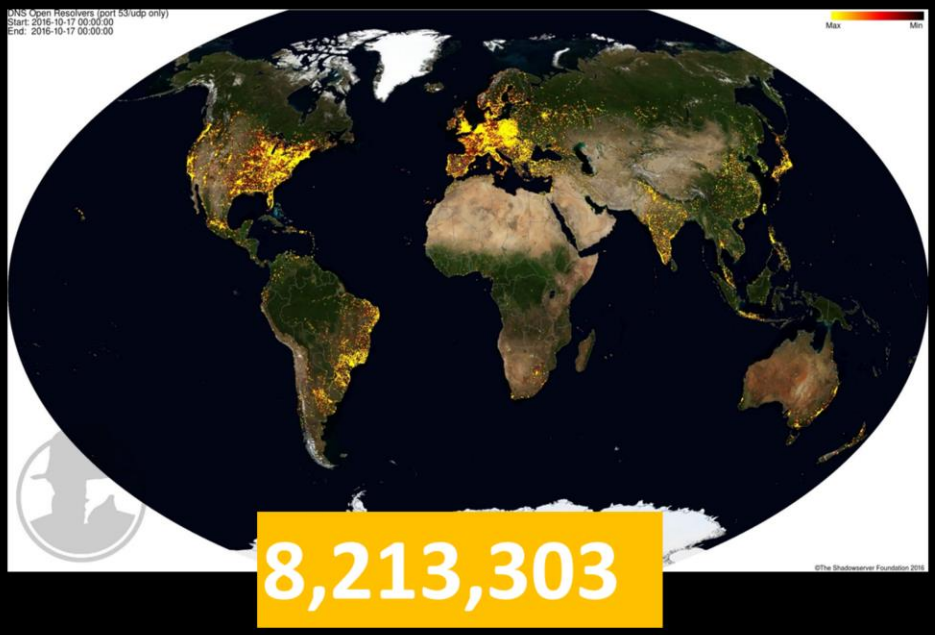
In DNS: rd = 1, qcount = 1, qd = the query desired
In DNSQR: qname = "domainname.com", qtype = 255 (ANY)
request = (i/u/d)
resp = sr1(request) to view
send(request) to send asynchronously

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
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
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request

Source: US Cert

Placeholder to SANOG30 committee

- The DNS amplification attack itself


DNS Open Resolvers (port 53/udp only)
Start: 2016-10-17 00:00:00
End: 2016-10-17 00:00:00
Max
Min
©The Shadowserver Foundation 2016
8,213,303

Questions

So, by now after hearing all of these talks today you must be very familiar with Denial of Service attacks. No need to explain what's a DDoS attack and why it's important to have a strong mitigation plan for your organization. So let's just have a 6 seconds summary of what a DDoS attack is.

DDoS Economy

Anyone knows what this is?
It’s a home made weapon used by the Hamas organization to create terror among IL civilians

Someone left a message for you, take a look under your chair…

From: Armada Collective
Subject: DDOS ATTACK!!!
Date: Wed, 9 Mar 2016 XX:XX:XX +0000

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.
http://www.govcert.admin.ch/blog/14/armada-collective-blackmails-swiss-hosting-providers

All your servers will be DDoS-ed starting Monday (March 14) if you
don't pay protection – 25 Bitcoins @
17j7onEtLgS2pd6qLekKQCteqTrnAFXZVS
If you don't pay by Monday, attack will start, price to stop will
increase to 50 BTC and will go up 20 BTC for every day of attack.

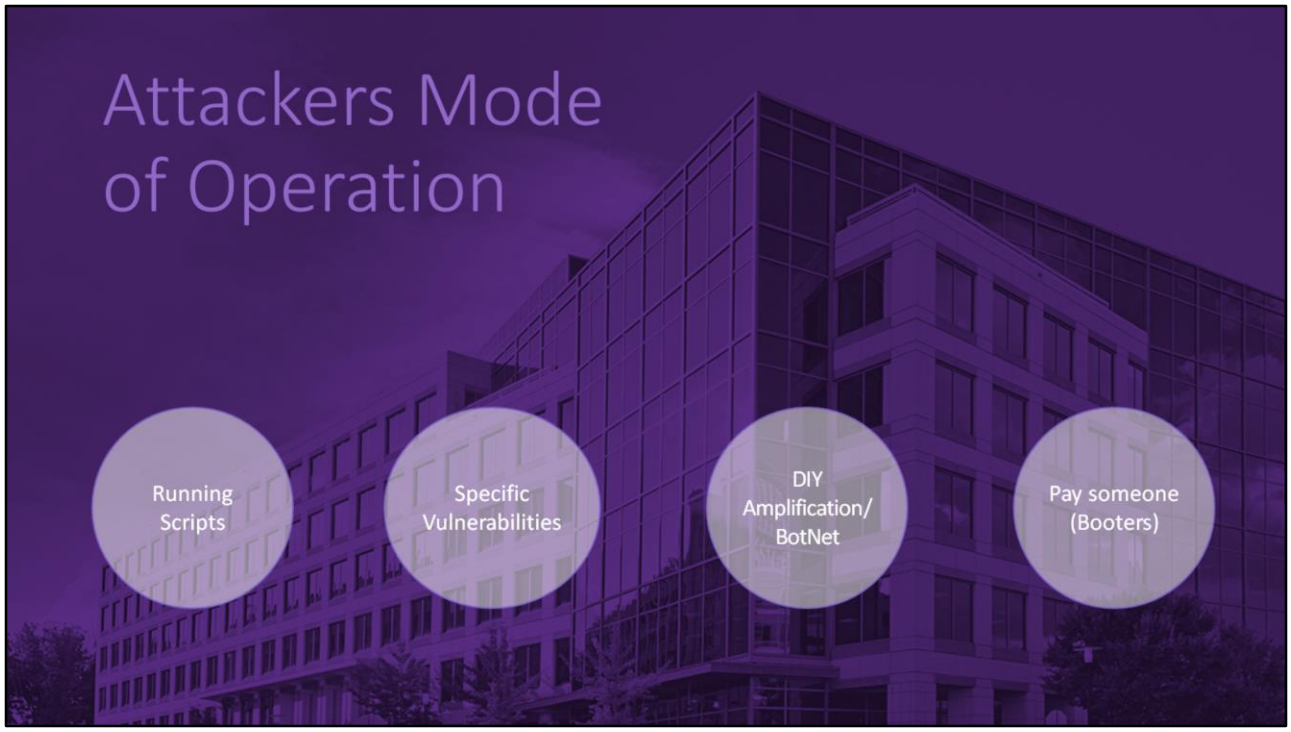
This is not a joke.
Our attacks are extremely powerful – sometimes over 1 Tbps per second.
So, no cheap protection will help.

Prevent it all with just 25 BTC @ 17j7onEtLgS2pd6qLekKQCteqTrnAFXZVS

Do not reply, we will not read. Pay and we will know its you. AND YOU
WILL NEVER AGAIN HEAR FROM US!
Bitcoin is anonymous, nobody will ever know you cooperated

Who is Armada? Is this the real one or a fake? Who know… are you willing to take the risk?

You have the date and sometime the exact time as well. Note how the price will grow if you don't pay know!
What will happen if you pay? In most cases they will still take you down just to get more… or they will go and try extort other companies from the same industry (we have seen that trend)

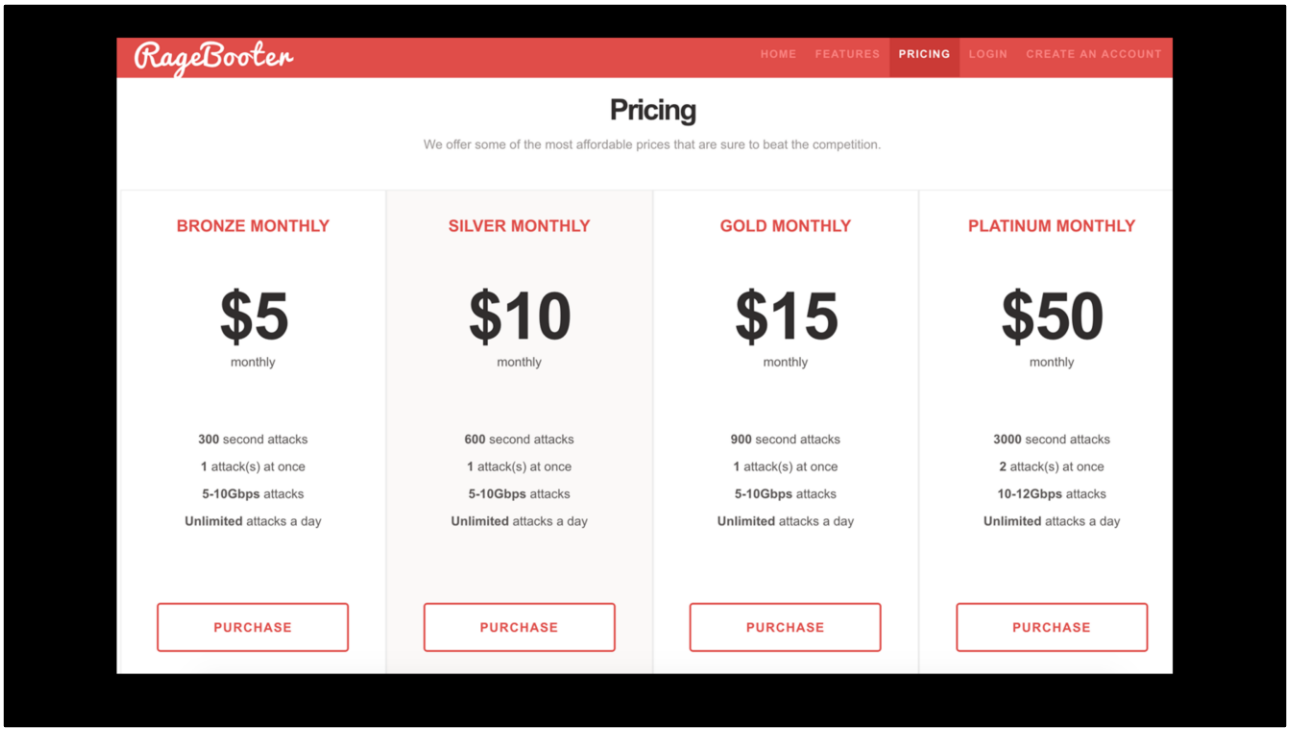


There are a few types/option to choose from and in the complexity can stretch between script kidz to advance vulnerabilities and setting up a BotNet. Yet the most common method that drive today industry is Booters/Stressers DDoS services

How booters work…

Establish botnet
Locate vulnerable reflective gateway
Dedicated servers in “grey” countries

Open DNS server or Open NTP server

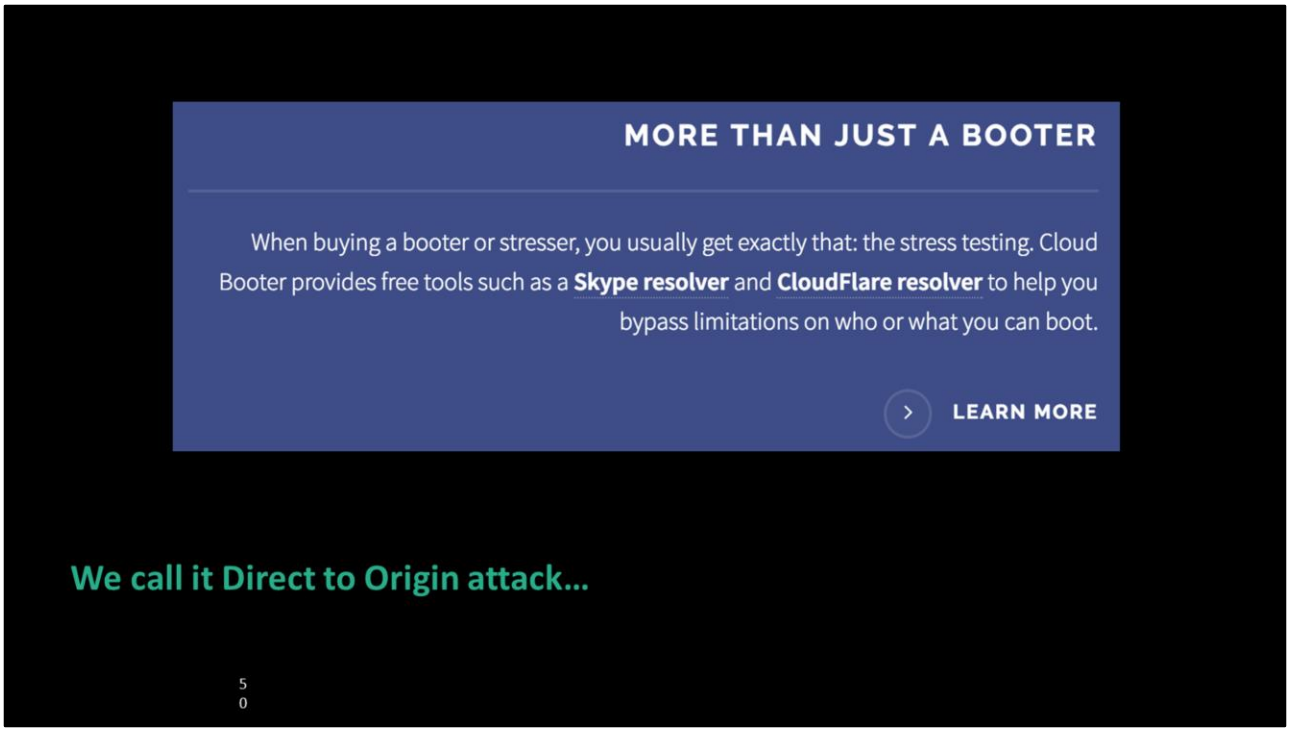


Source: https://ragebooter.net/

XyzBooter

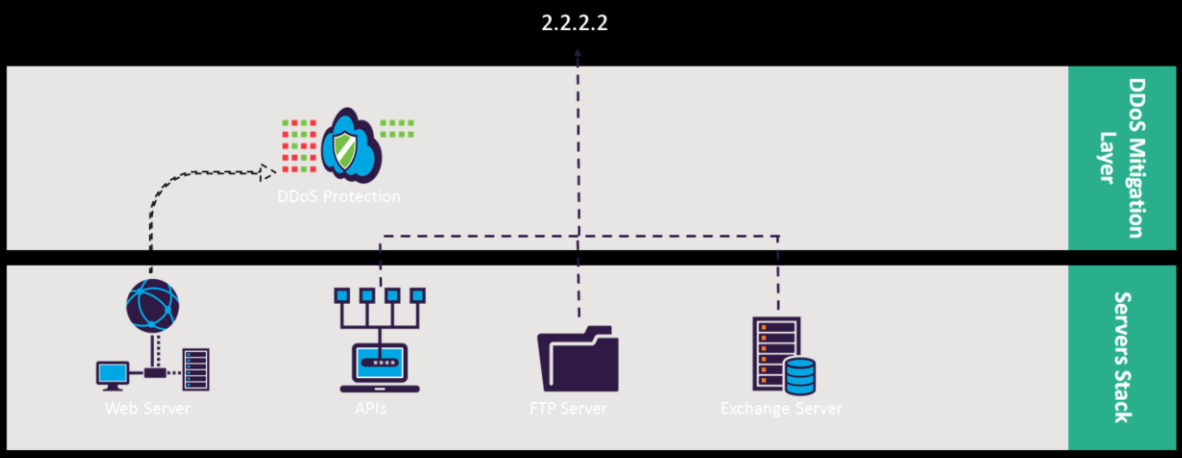
#	Method Name	Method Type	Target Type	Target Syntax
1	GET	Layer 7	Websites, WebServers, etc ..	URL: http://target.com
2	HEAD	Layer 7	Websites, WebServers, etc ..	URL: http://target.com
3	POST	Layer 7	Websites, WebServers, etc ..	URL: http://target.com
4	JSBYPASS	Layer 7	Websites, WebServers, etc ..	URL: http://target.com
5	JOOMLA	Layer 7	Websites, WebServers, etc ..	URL: http://target.com
6	XMLRPC	Layer 7	Websites, WebServers, etc ..	URL: http://target.com
7	SNMP	Layer 4	Home / Peoples, Servers, Custom IPs, etc ..	IP: 1.3.3.7
8	SSDP	Layer 4	Home / Peoples, Servers, Custom IPs, etc ..	IP: 1.3.3.7
9	DNS	Layer 4	Home / Peoples, Servers, Custom IPs, etc ..	IP: 1.3.3.7
10	CHARGEN	Layer 4	Home / Peoples, Servers, Custom IPs, etc ..	IP: 1.3.3.7
11	NTP	Layer 4	Home / Peoples, Servers, Custom IPs, etc ..	IP: 1.3.3.7
12	TS3	Layer 4	Home / Peoples, Servers, Custom IPs, etc ..	IP: 1.3.3.7
13	SSYN	Layer 4	Home / Peoples, Servers, Custom IPs, etc ..	IP: 1.3.3.7
14	DOMINATE	Layer 4	Home / Peoples, Servers, Custom IPs, etc ..	IP: 1.3.3.7


Welcome to Quez Stresser, an absolutely free booter that hits harder than 90% of paid booters.
Hours Booted
75827.6
Active Users
26
Floods Launched
1552369
Floods Running
13 / 15
FREE Booter
Target IP
1.3.3.7
Target Port
80
TLme
300
Attack Method
NTP
DDoS Da Skid

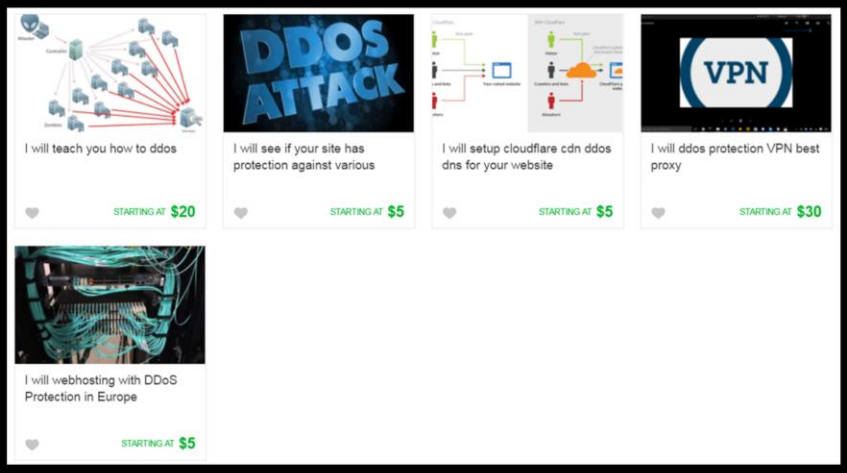


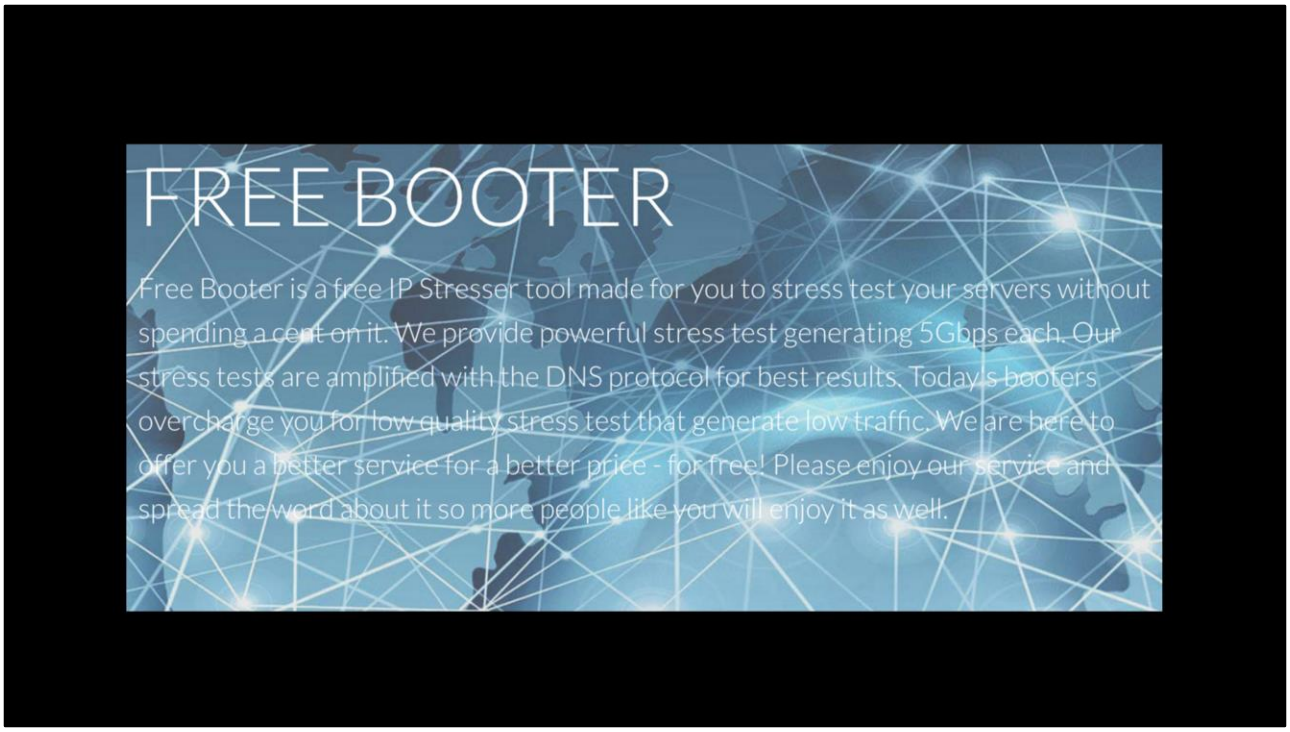
The “help you bypass limitations”… make no mistake they are bypassing the obviuse layers inorder to make direct to origin attacks.

Other services expose your IP to DDoS

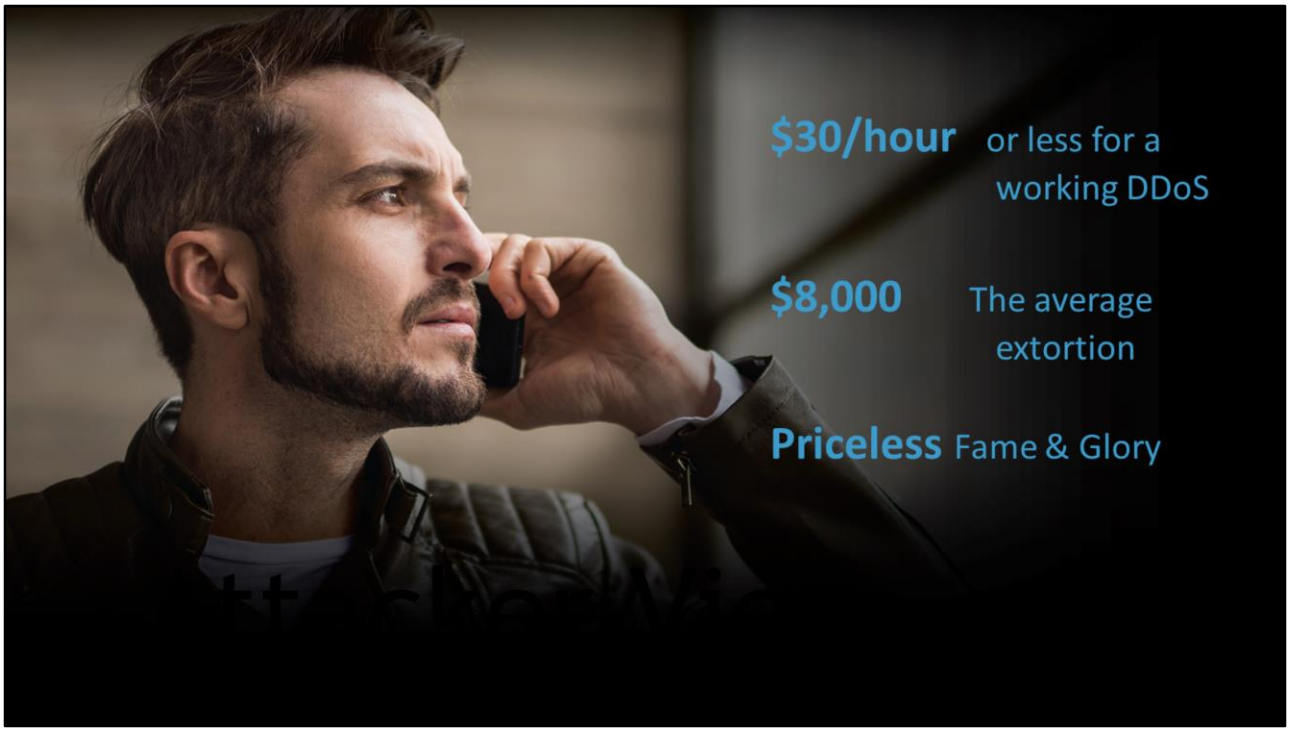


Fiverr ring a bell?



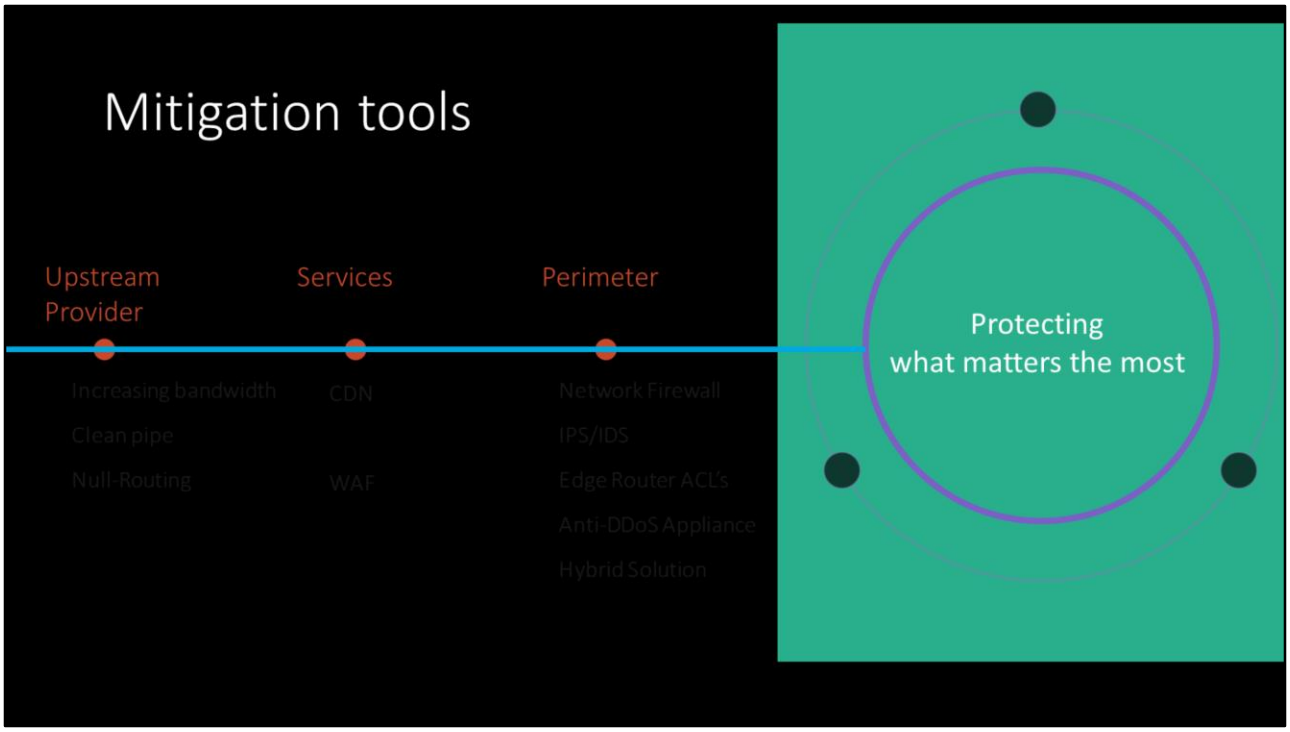


Probably: because when you attack you also become part of the bonnet
HOLA (Proxy anonymize) infested with bots

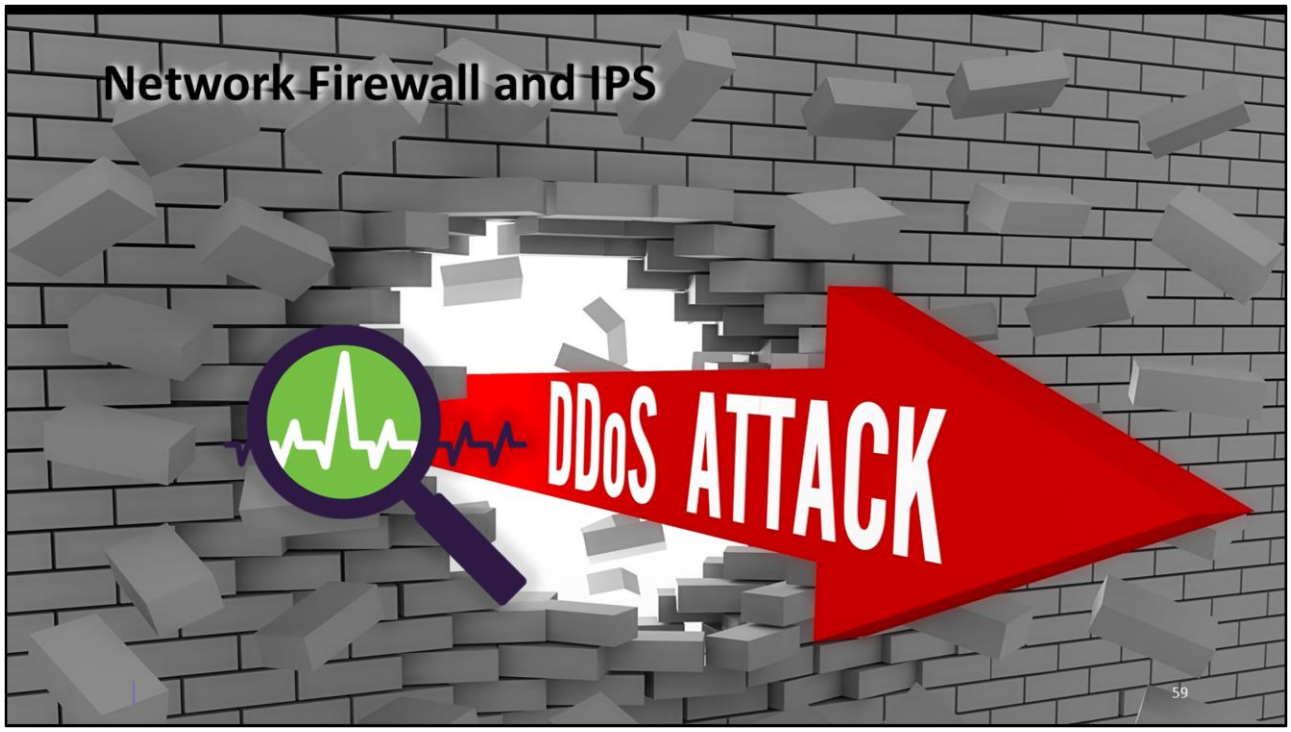

$30/hour or less for a working DDoS
$8,000 The average extortion
Priceless Fame & Glory

Source: Incapsula Survey: What DDoS attacks really cost business

Mitigation Options



The defense line start far away from your perimeter, at your up-stream provider. Here are the most common tools and defense layer one can use to handle DDoS.


Network Firewall and IPS
DDoS ATTACK
59

Network Firewall and IPS

Close to the target

- **DDoS protection** required at the **first line of defense** – far away from the target
- A volumetric attack is an attack that is aimed at flooding the network controls and **clogging the bandwidth**.

60

Network Firewall and IPS

- Every minute counts
- IPS and stateful FW relies on signatures
- Signatures takes time to config

Correlation Between Millions of Legit Requests

GET / HTTP/1.0 Accept: text/plain
Accept: text/html
Session-Id: SID:ANON:w3.org:j6oAOxCWZh/CD723LGeXlf-01:034
User-Agent: libwww/4.1

GET / HTTP/1.0 Accept: text/plain
Accept: text/html
Session-Id: SID:ANON:w3.org:j6oAOxCWZh/CD723LGeXlf-01:034
User-Agent: libwww/4.1

GET / HTTP/1.0 Accept: text/plain
Accept: text/html
Session-Id: SID:ANON:w3.org:j6oAOxCWZh/CD723LGeXlf-01:034
User-Agent: FF/12.227

62

As you can see the last request is very similar except of one thing the user agent is a fake.
In such case your FW can’t correlate between all other requests. Even a basic WAF may fail detecting such behavior.
You’ll need a session aware tool, one that can correlate between events and detect header manipulation even when they are camouflaged

ACL at your edge router

- Not everything is legit traffic, use **five tuples** to prevent none legit
  - E.g. on a webserve accept TCP on port 80, 443 block/drop everything else
- When using a switch in a tandem mode, make sure it doesn't reduce your **performance** once the ACL is used to block type of traffic

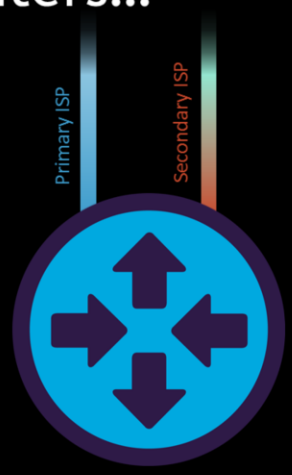
Pros:
- Already exists in organization
- Helps decrease attack surface

Cons:
- Not useful against sophisticated attacks
- Not granular and hard to manage

ACL and performance….

While speaking about edge routers…

- At the ISP level
  - Always have a **backup line**, at least dual ISPs
- At the equipment level
  - Separate between edge devices
  - Connect to same ISPs in each device
  - Your routers should **handle high packet rates** (reduce the router bottleneck)



Separate between edge devices?

Upstream provider - Increase Bandwidth

- Either as a permanent addition or when there are volumetric spikes

Pros:
- Extra bandwidth can help coping with volumetric attacks
- If the increase is low-cost, it might be a good addition

Cons:
- Larger bandwidth is cheaper for the attackers
- For some attacks, increasing incoming attack traffic may actually cause **more** damage
- In most cases not cost effective

Increasing the BW can bring even larger attack to the gates of your edge device. It can kill the device…

Upstream provider - ACL/Other Solutions

- Upstream provider creates certain rules to block attack traffic before reaching the organization

Pros:

- Stops attacks before they're clogging your bandwidth

Cons:

- Not always an option - it makes bandwidth more expensive for ISP's
- Not granular, may have high % of False Positives
- Hard to maintain
- Not effective against most L7 attacks

Upstream provider - Null Route (a.k.a RTBH)

- An effective null route is when your provider tells its up-streams (using bgp) to not send traffic to an IP
- It its an easy solution to stop strong attacks that are just too much to handle locally
- The attack itself wont stop, but no packets destined to that IP will reach the provider and will be dropped by the border routers of its transit providers

Upstream provider - Null Route (a.k.a RTBH)

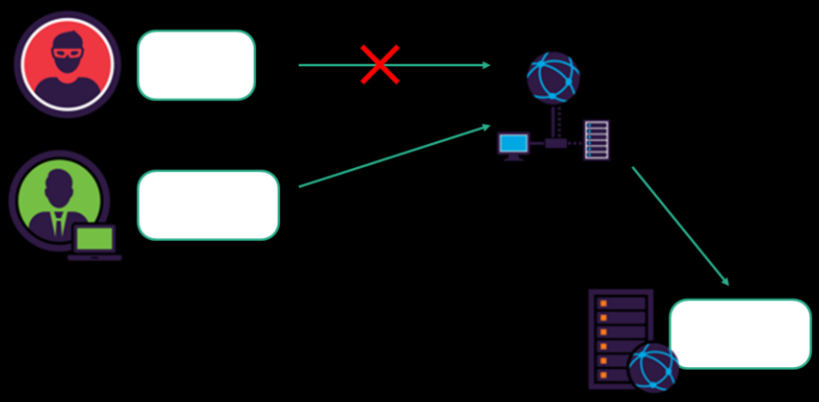
Pros:

- Sometimes you have no other choice

Cons:

- Lots of False Positives by design
- Resources are sacrificed

CDN



CDN

Pros:

* A proxy doesn’t transfer anything else “by-design”

Cons:

- Only effective for protecting web applications
- Not effective against big / persistent attacks
- Not always effective against all L7 attacks

70

A proxy doesn't’t transfer anything else?... There are many kind of proxies why assume web proxy

WAF

- Most DDoS attack vectors cannot be mitigated by network capacity alone
- Successful mitigation of Layer 7 DDoS attacks relies on the ability to accurately profile incoming traffic – to distinguish between humans, human-like bots and hijacked web browsers
- Protect applications from Layer 7 DDoS by deploying a WAF solution that can classify between bad bots and good bots, rely on visitor reputation, protect against OWASP top 10, utilize progressive challenge techniques, detect anomaly

WAF

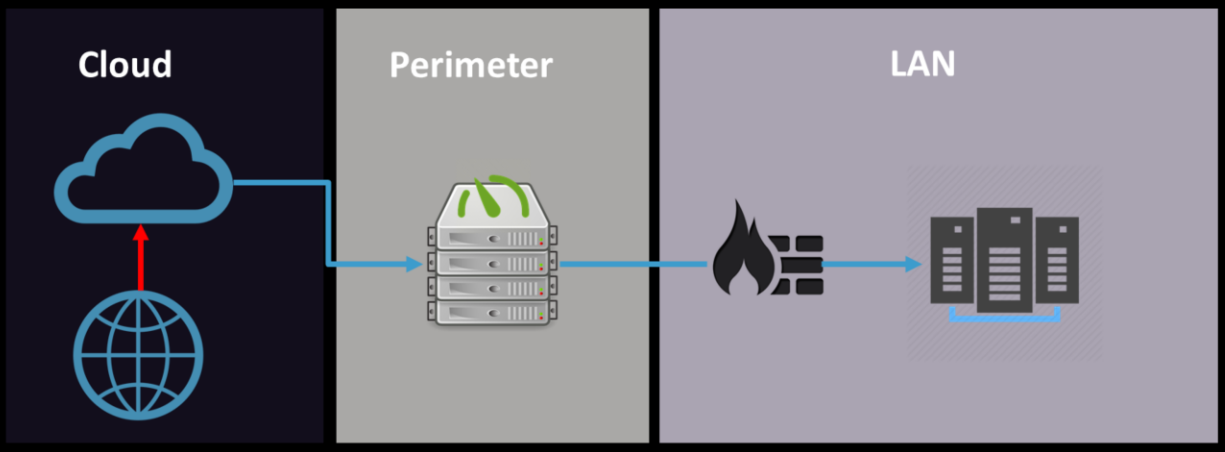
Pros:

- Effective against L7 attacks (Not all solutions)
- Can be very granular (Not all solutions)

Cons:

- Ineffective against volumetric attacks

Hybrid Solution



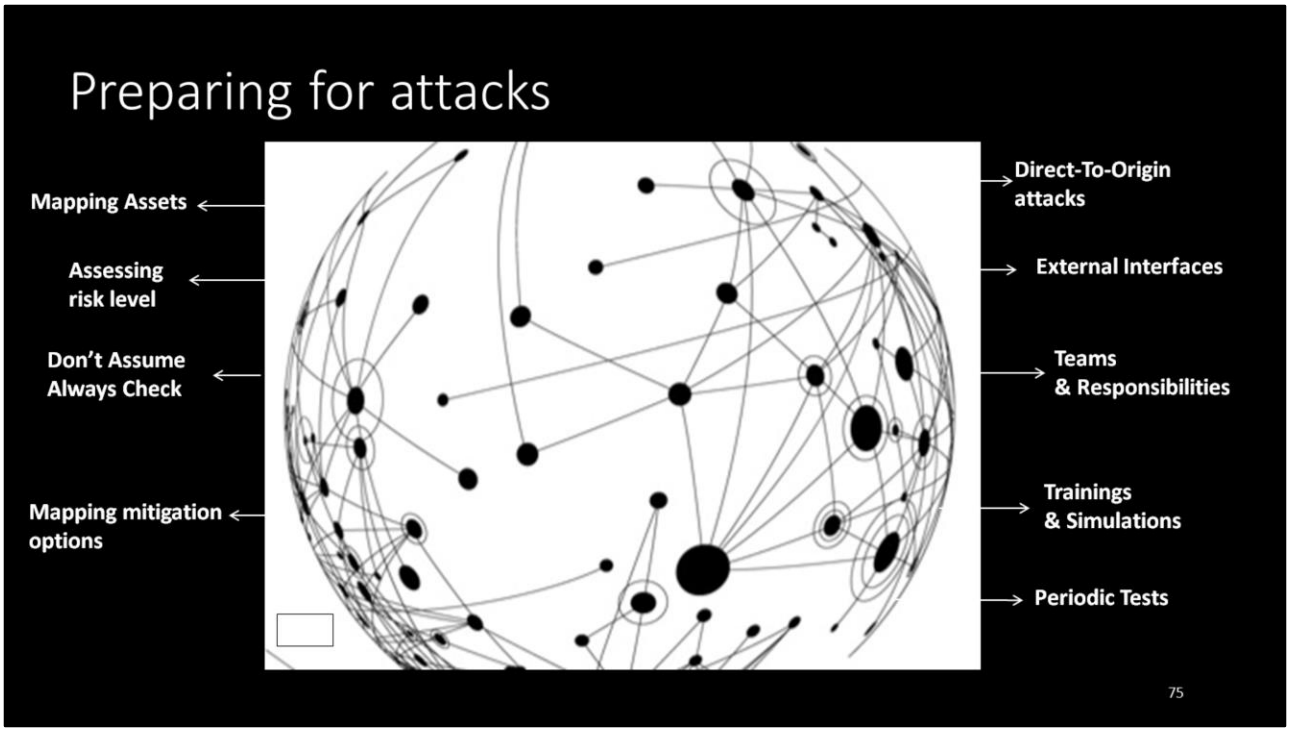
Hybrid Solution

Pros:

- Hybrid sounds good
- Provides coverage both against L7 and against volumetric attacks

Cons:

- Ineffective against large L7 attacks



We talked about tools and ways to mitigate but you always need to be prepare for the dooms day.
Make sure that all of the buzz words that you see on the screen right now, make sense to you and cover in your "What to do when ddos come" notebook.

DDOS Bootcamp

www.ddosbootcamp.com

Created for the benefit of Internet Community by:

Imperva Incapsula

Nimbus DDOS

76

polina@incapsula.com

SANOG