DDoS Workshop
Brace Yourself: DDoS is Coming!

Polina Berman – Security Solutions Engineer
polina@incapsula.com
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
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.
A distinction between two main categories

Network Layer Attacks

Application 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.

Source:
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.
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.
40.5% are multi-vector attacks

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

Source: Incapsula Global DDoS Threat Landscape Q1 2017
74% are attacked more than once

Distribution of application layer attacks, by frequency

Source: Incapsula Global DDoS Threat Landscape Q1 2017
Source: Incapsula Global DDoS Threat Landscape Q4 2016

India among top 10 target countries: Akamai

Top 10 Target Countries for Web Application Attacks, Q1 2017

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

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

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

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

Increase Bandwidth

I have CDN in front

Other Responsibilities

Default Password

Do you have password policy?
There are many reasons to justify a DDoS act. I’ve listed only few. In the next slides we going to cover each one
Rivalry

Extortion

Hacktivism

State Sponsored

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

Source: Verizon 2017 Data Breach Investigations Report

“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

Monsanto – Energy sector, gets ongoing attack from Green activist
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...”

The UK person who launched an attack against British Airways
Possibly switching to a more vulnerable DR system
Mirai
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)) != -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;
### “Don’t mess with” list

<table>
<thead>
<tr>
<th>Address Block</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>127.0.0.0/8</td>
<td>Loopback</td>
</tr>
<tr>
<td>0.0.0.0/8</td>
<td>Invalid address space</td>
</tr>
<tr>
<td>3.0.0.0/8</td>
<td>General Electric (GE)</td>
</tr>
<tr>
<td>15.0.0.0/7</td>
<td>Hewlett-Packard (HP)</td>
</tr>
<tr>
<td>56.0.0.0/8</td>
<td>US Postal Service</td>
</tr>
<tr>
<td>10.0.0.0/8</td>
<td>Internal network</td>
</tr>
<tr>
<td>192.168.0.0/16</td>
<td>Internal network</td>
</tr>
<tr>
<td>172.16.0.0/14</td>
<td>Internal network</td>
</tr>
<tr>
<td>190.64.0.0/10</td>
<td>IANA NAT reserved</td>
</tr>
<tr>
<td>169.254.0.0/16</td>
<td>IANA NAT reserved</td>
</tr>
<tr>
<td>198.18.0.0/15</td>
<td>IANA Special use</td>
</tr>
<tr>
<td>224.<em>.</em>.*</td>
<td>Multicast</td>
</tr>
<tr>
<td>0.0.0.0/7</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>11.0.0.0/8</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>21.0.0.0/8</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>22.0.0.0/8</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>26.0.0.0/8</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>28.0.0.0/7</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>30.0.0.0/8</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>33.0.0.0/8</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>55.0.0.0/8</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>214.0.0.0/7</td>
<td>Department of Defense</td>
</tr>
</tbody>
</table>
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         // LOLNOGF0
#define TABLE_MEM_UPX           // \x58\x4d\x4e\x43\x50\x46\x22
#define TABLE_MEM_ZOLLARD       // ZOLLARD
```
Demo Time
Live Demo – placeholder to SANOG30 committee

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

• Part 2
  o DNS Amplification attack
  o ~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
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Bandwidth Amplification Factor</th>
<th>Vulnerable Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv2</td>
<td>6.3</td>
<td>GetBulk request</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>3.8</td>
<td>Name resolution</td>
</tr>
<tr>
<td>SSDP</td>
<td>30.8</td>
<td>SEARCH request</td>
</tr>
<tr>
<td>CharGEN</td>
<td>358.8</td>
<td>Character generation request</td>
</tr>
<tr>
<td>QOTD</td>
<td>140.3</td>
<td>Quote request</td>
</tr>
<tr>
<td>BitTorrent</td>
<td>3.8</td>
<td>File search</td>
</tr>
<tr>
<td>Kad</td>
<td>16.3</td>
<td>Peer list exchange</td>
</tr>
<tr>
<td>Quake Network Protocol</td>
<td>63.9</td>
<td>Server info exchange</td>
</tr>
<tr>
<td>Steam Protocol</td>
<td>5.5</td>
<td>Server info exchange</td>
</tr>
<tr>
<td>Multicast DNS (mDNS)</td>
<td>2 to 10</td>
<td>Unicast query</td>
</tr>
<tr>
<td>RIPv1</td>
<td>131.24</td>
<td>Malformed request</td>
</tr>
<tr>
<td>Portmap (RPCbind)</td>
<td>7 to 28</td>
<td>Malformed request</td>
</tr>
</tbody>
</table>

Source: US Cert
Placeholder to SANOG30 committee

• The DNS amplification attack itself
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 @ 17j7onEtLgS2pd6qLeKQCTeqTrnAFXZV5
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 @ 17j7onEtLgS2pd6qLeKQCTeqTrnAFXZV5
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
<table>
<thead>
<tr>
<th>Plan</th>
<th>Monthly Price</th>
<th>Included Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>BRONZE</td>
<td>$5</td>
<td>300 second attacks, 1 attack(s) at once, 5-10Gbps attacks, Unlimited attacks a day</td>
</tr>
<tr>
<td>SILVER</td>
<td>$10</td>
<td>600 second attacks, 1 attack(s) at once, 5-10Gbps attacks, Unlimited attacks a day</td>
</tr>
<tr>
<td>GOLD</td>
<td>$15</td>
<td>900 second attacks, 1 attack(s) at once, 5-10Gbps attacks, Unlimited attacks a day</td>
</tr>
<tr>
<td>PLATINUM</td>
<td>$50</td>
<td>3000 second attacks, 2 attack(s) at once, 10-12Gbps attacks, Unlimited attacks a day</td>
</tr>
</tbody>
</table>

Source: https://ragebooter.net/
<table>
<thead>
<tr>
<th>#</th>
<th>Method Name</th>
<th>Method Type</th>
<th>Target Type</th>
<th>Target Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GET</td>
<td>Layer 7</td>
<td>Websites, WebServers, etc ..</td>
<td>URL: <a href="http://target.com">http://target.com</a></td>
</tr>
<tr>
<td>2</td>
<td>HEAD</td>
<td>Layer 7</td>
<td>Websites, WebServers, etc ..</td>
<td>URL: <a href="http://target.com">http://target.com</a></td>
</tr>
<tr>
<td>3</td>
<td>POST</td>
<td>Layer 7</td>
<td>Websites, WebServers, etc ..</td>
<td>URL: <a href="http://target.com">http://target.com</a></td>
</tr>
<tr>
<td>4</td>
<td>JSBYPASS</td>
<td>Layer 7</td>
<td>Websites, WebServers, etc ..</td>
<td>URL: <a href="http://target.com">http://target.com</a></td>
</tr>
<tr>
<td>5</td>
<td>JOOMLA</td>
<td>Layer 7</td>
<td>Websites, WebServers, etc ..</td>
<td>URL: <a href="http://target.com">http://target.com</a></td>
</tr>
<tr>
<td>6</td>
<td>XMLRPC</td>
<td>Layer 7</td>
<td>Websites, WebServers, etc ..</td>
<td>URL: <a href="http://target.com">http://target.com</a></td>
</tr>
<tr>
<td>7</td>
<td>SNMP</td>
<td>Layer 4</td>
<td>Home / Peoples, Servers, Custom IPs, etc ..</td>
<td>IP: 1.3.3.7</td>
</tr>
<tr>
<td>8</td>
<td>SSDP</td>
<td>Layer 4</td>
<td>Home / Peoples, Servers, Custom IPs, etc ..</td>
<td>IP: 1.3.3.7</td>
</tr>
<tr>
<td>9</td>
<td>DNS</td>
<td>Layer 4</td>
<td>Home / Peoples, Servers, Custom IPs, etc ..</td>
<td>IP: 1.3.3.7</td>
</tr>
<tr>
<td>10</td>
<td>CHARGEN</td>
<td>Layer 4</td>
<td>Home / Peoples, Servers, Custom IPs, etc ..</td>
<td>IP: 1.3.3.7</td>
</tr>
<tr>
<td>11</td>
<td>NTP</td>
<td>Layer 4</td>
<td>Home / Peoples, Servers, Custom IPs, etc ..</td>
<td>IP: 1.3.3.7</td>
</tr>
<tr>
<td>12</td>
<td>TS3</td>
<td>Layer 4</td>
<td>Home / Peoples, Servers, Custom IPs, etc ..</td>
<td>IP: 1.3.3.7</td>
</tr>
<tr>
<td>13</td>
<td>SSYN</td>
<td>Layer 4</td>
<td>Home / Peoples, Servers, Custom IPs, etc ..</td>
<td>IP: 1.3.3.7</td>
</tr>
<tr>
<td>14</td>
<td>DOMINATE</td>
<td>Layer 4</td>
<td>Home / Peoples, Servers, Custom IPs, etc ..</td>
<td>IP: 1.3.3.7</td>
</tr>
</tbody>
</table>
The "help you bypass limitations"... make no mistake they are bypassing the obvious layers inorder to make direct to origin attacks.
Other services expose your IP to DDoS
Fiverr ring a bell?

- I will teach you how to ddos
  - STARTING AT $20

- I will see if your site has protection against various ddos
  - STARTING AT $5

- I will setup cloudflare cdn ddos dns for your website
  - STARTING AT $5

- I will ddos protection VPN best proxy
  - STARTING AT $30

- I will webhosting with DDoS Protection in Europe
  - STARTING AT $5
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
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
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**.
Network Firewall and IPS

- Every minute counts
- IPS and stateful FW relies on signatures
- Signatures takes time to config
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 webserver 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?
Increasing the BW can bring even larger attack to the gates of your edge device. It can kill the device...

**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
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's an easy solution to stop strong attacks that are just too much to handle locally

- The attack itself won't 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
A proxy doesn'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

Cloud

Perimeter

LAN
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 prepared 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