DDoS Mitigation

EPIC FAIL

collection

TL;DR: DDOS STRATEGISTS DO DRUGS

Agenda

- Intro
- Methodology of work
- DDoS tactics in-the-wild and how to improve
- Ready, set, FACEPALM!
- Q&A

~$ whoami_

- Moshe Zioni, Head of Research, Comsec
- 3 years (and counting) of designing & providing full-blown an on-demand DDoS attack service.
- 2nd time at hack-in-paris, 1st time as speaker (thanks!)
- .///. END OF SHAMELESS PROMOTION SLIDE .///.

Method

DDoS for Everyone!

Run-of-the-Mill DDoS attacks nowadays

- **Rely heavily on bandwidth consumption**
- **53% of attacks are < 2Gbps (SANS)**
- **Most attacks does not require brains**
- **Amplification and Reflection relies on 3rd party domains (DNS, NTP etc.)**

Strike harder! (!=bigger)

- There is more to a web site then a front-end (!!)
- Overload the backend by making the system work for you
- Keep it stealthy, they are looking for you
- Generalized term for Amplification

Generalized Amplification - “4 Pillars”

- Amplification factors
  - **Network** – The usual suspect
  - **CPU** – Very limited on some mediators and web application servers
  - **Memory** – Volatile, everything uses it
  - **Storage** – Can be filled up or exhausting I/O buffer

Just before we start

- **NO SHAMING POLICY - Client identity will remain anonymous**
- **Meet - “SuperBank”**
- **10 common-practices and the appropriate bypass/attack**

Ready?
Set.
FACEPALM!

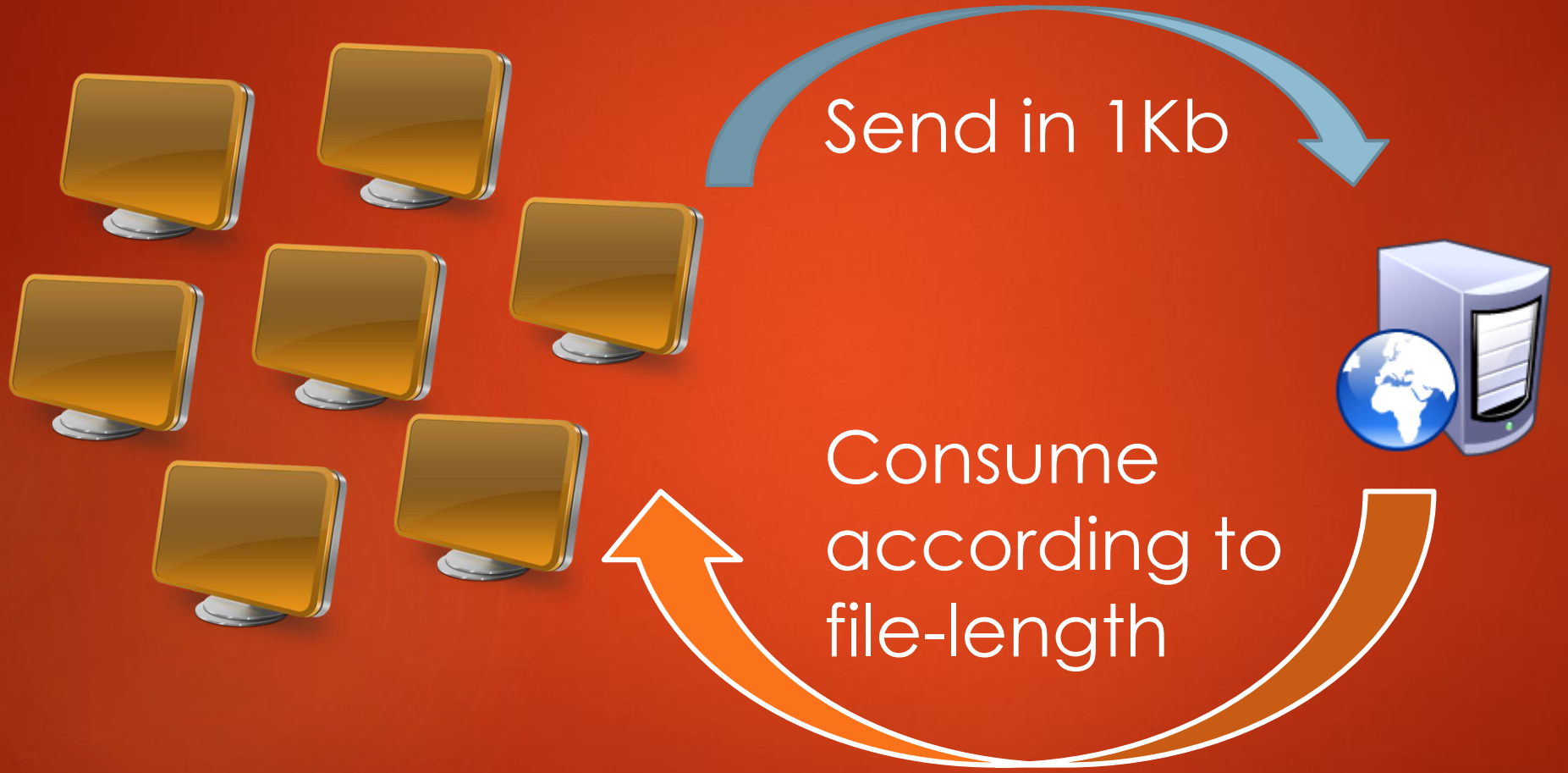
10

“Limit the rate of incoming packets”

- The bank has been hit by a DDoS attack that consumed ALL BANDWIDTH

- To rectify the situation the ISP suggested limiting incoming packet rate to ensure availability

Reflection to the rescue!



Consumption by reflection

9

“It’s OK now, monitoring shows everything is back to normal”

- MegaCommonPractive now went on to buy a Anti-DDoS solution

- A known Anti-DDoS cloud-based protection solution approached the client and offered a very solid looking solution including 24/7 third party monitoring

ACTUALLY TRY TO ACCESS THE WEB SITE!!!!

8

“Backend servers are not important to protect against DDoS”

Mapping the backend for DDoS

- Databases are very susceptible to DDoS attacks and provide good grounds for intra-amplification
- How can we find DBs?
  - You can always guess, pentersters do that all the time…
  - Takes more time == talk more with BE !!! PROFIT!!!

7


PROTECT
ALL THE DOMAINS
memegenerator.net

Really??!?! ALL OF THE DOMAINS?!?

- What is the strategy of mitigation? Do you understand it?

6

“We don’t trust the vendor, we don’t give them certificates”

Talk to me in layer 7…

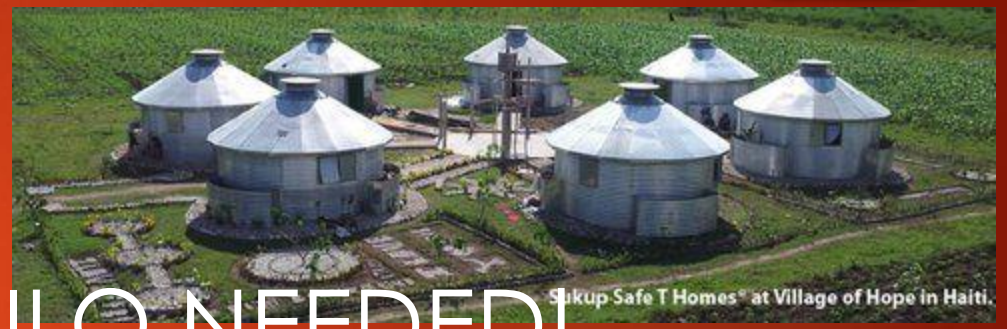
- Defense have chosen not to monitor layer 7 – HTTPS attacks..

- SSL re/negotiation
- Full blown HTTPS GET/POST/… no one can see you now

5

“We need Big Data, collect all the logs”

Logs need to be handled



SILO NEEDED!

- Storage Boom
- Result in a complete lock-down, including not be able to manage the overflowed device
- It was the IPS, so no traffic allowed to anything

4

“We are under attack – enforce the on-demand Scrubbing Service”

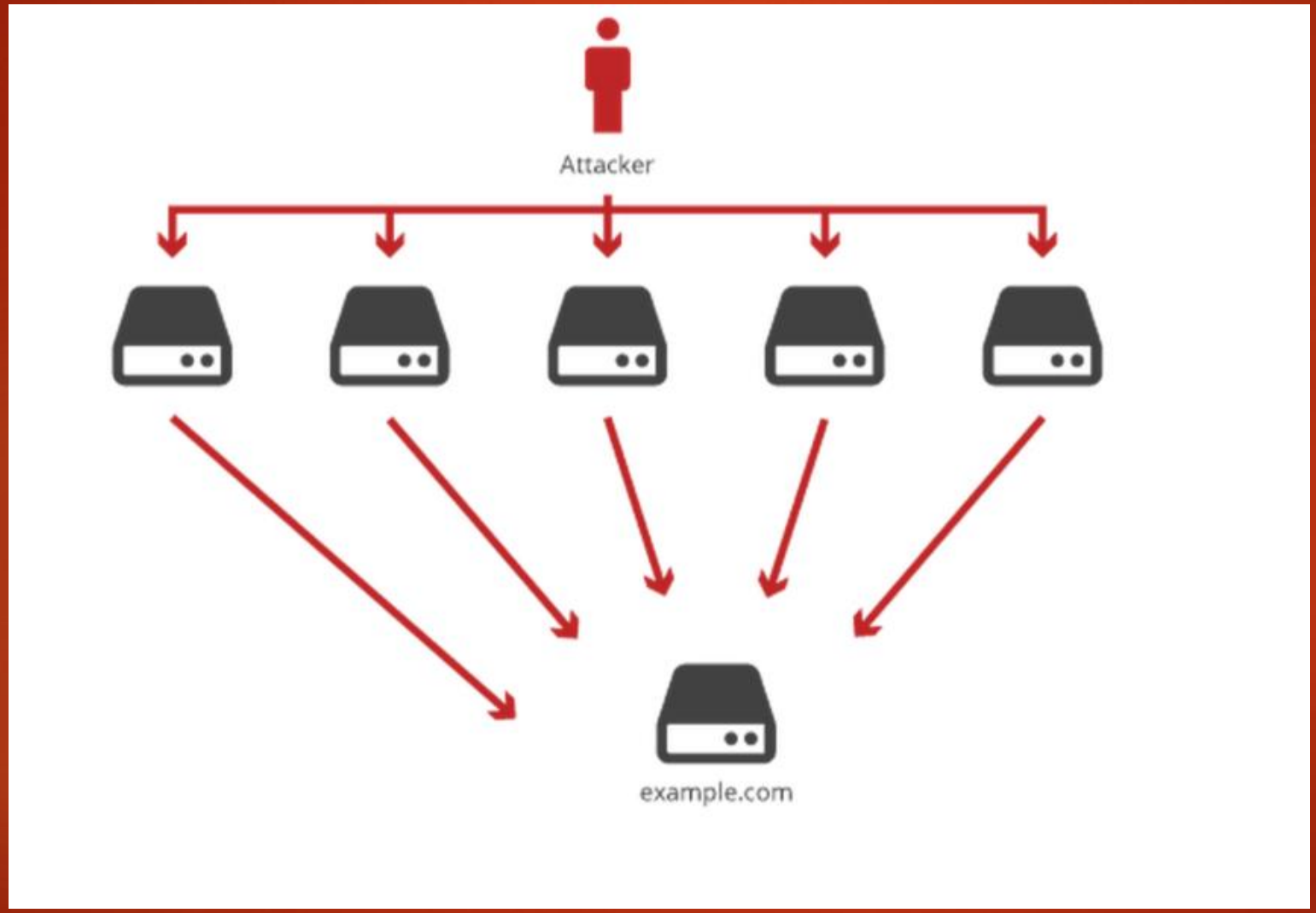
Learning mode – did you do it?

- All is learned
- Attack considered legitimate traffic

3

“So what CDN is not dynamic? Let’s enable it”

NOT IN CACHE? ASK THE ORIGIN!



2

CDN Planet Content Delivery Networks CDN blog

How to protect your CDN origin server

Published on **March 18, 2013** by **Aaron**

<snip>

Whitelisting

Another possible method for allowing only requests from your CDN is to whitelist the CDN. This should work well in theory, but in practice it is difficult to do effectively. You can whitelist

Option B: unguessable origin hostname

This is a simple trick and it is also the best solution. Create some random, long set of alphanumeric characters and use that as the subdomain. Example: `205ck07023nckhfsh92485.example.com`. This hostname will then be only known to the CDN, the owner of the origin and the origin's DNS provider(s). Can it be guessed? Yes, but highly unlikely. Can it leak? Yes, but again: highly unlikely.

`205ck07023nckhfsh92485.example.com`. This hostname will then be only known to the CDN, the owner of the origin and the origin's DNS provider(s). Can it be guessed? Yes, but highly unlikely. Can it leak? Yes, but again: highly unlikely.

How to find an ‘invisible’ origin?

- Find other known subdomain -> translate to IP -> scan the /24 or /16 -> good chance it’s there.
- AND….. WHOIS never forgets
- http://viewdns.info FTW!

ViewDNS.info

IP history results for bing.com.
==========

IP Address	Location	IP Address Owner	Last seen on this IP
204.79.197.200	United States	Microsoft Corporation	2015-06-15
131.253.33.200	Ottawa - Canada	Microsoft Corp	2013-09-17
204.79.197.200	United States	Microsoft Corporation	2013-04-12
131.253.13.32	Ottawa - Canada	Microsoft Corp	2013-02-24
65.52.107.149	United States	Microsoft Corporation	2012-06-04
65.55.175.254	United States	Microsoft Corporation	2012-02-17

1

“Block ‘em!, now them, now them, now them, now them, now them, now them, now them, now them, now them, now them, now them, now them, now them, now them. “

Total IPs in FR: ~82 M

About 1,200 class B ranges

Now think of a monkey blocking every incoming alert.

10 MINUTES TO SELF INFLECTED DDOS

Collected misconceptions

- There is no magic pill or best cocktail mix of technologies/appliances/services, never was
- DDoS is a subset of DoS, not the other way around
- You can have all the toys and money in the world – you have to be prepared and have trained people in mitigation because of those reasons
- If you won't do that – you can be evaluated for this presentation in the future

Questions?

Thank you!

Moshe Zioni
zimoshe@gmail.com, @dalmoz_
corp:moshez@comsecglobal.com