DDoS Attacks: Solutions and Pitfalls

Thomas Vissers

SecAppDev, Leuven (Mar 3, 2017)

ABOUT ME

Thomas Vissers

PhD Researcher at Distrinet, KU Leuven

thomas.vissers@cs.kuleuven.be

AGENDA

●●●

DDoS ATTACKS

CLOUD SECURITY

PITFALLS

PREVENTION

DDoS ATTACKS

WHAT IS A DDOS ATTACK?

- DDoS attacks attempt to take online services down

- Neustar claims

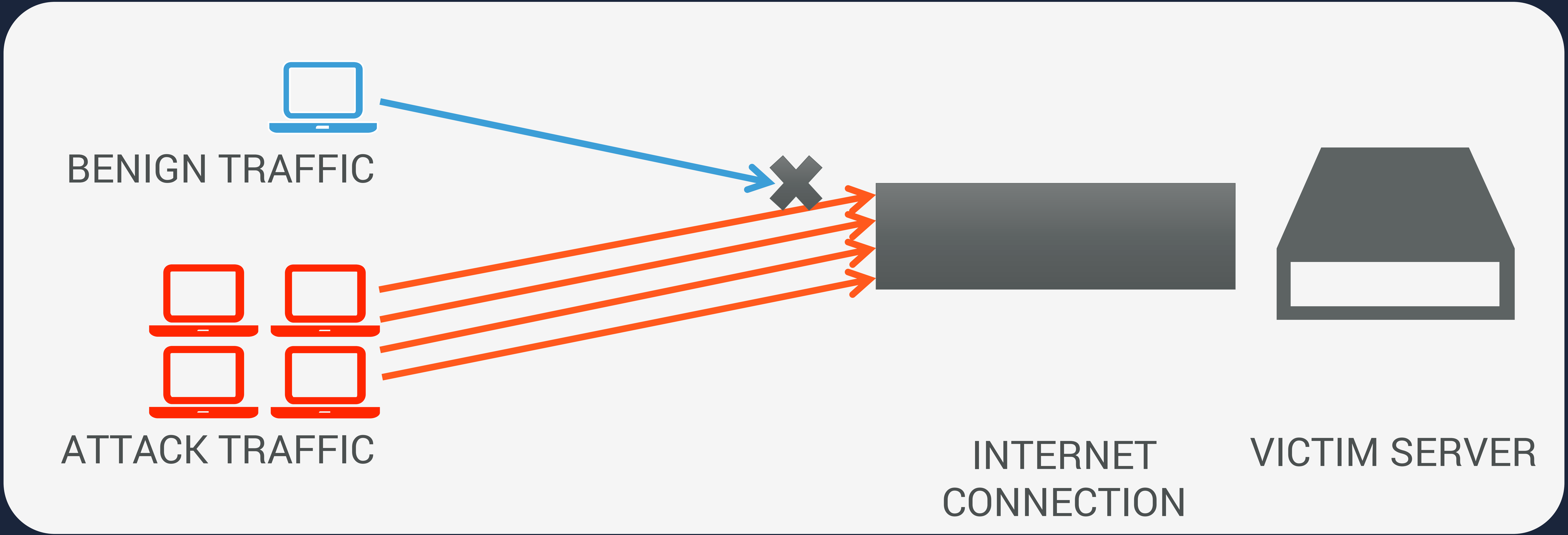
  "73% of companies suffered from a DDoS attack in 2015"

- Attacker motives
  - Extortion, hacktivism, hindering competitors, harm reputation, cyber-warfare, smokescreen, "f0r th3 lulz", …

WHAT IS A DDOS ATTACK?

Volumetric attack

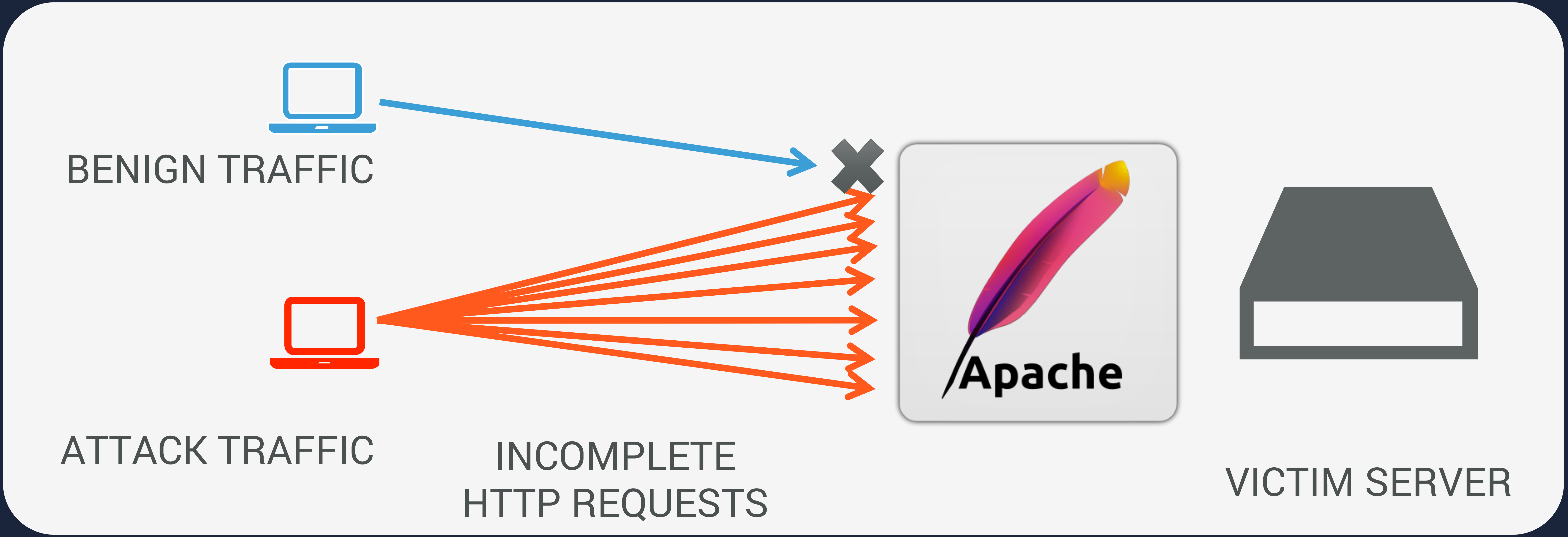
- Saturate the victim’s connection by flooding with network packets
- Coordinated botnet attack
- ”Amplify” traffic by abusing other services (e.g. open DNS resolvers)



WHAT IS A DDOS ATTACK?

Layer-7 attacks

- Rely on cleverly crafted requests, aimed at specific applications
- Saturate the resources of the server
  - CPU, Memory, specific limitations, ….
- Popular example: ``Slowloris” attack



EVER LARGER ATTACKS

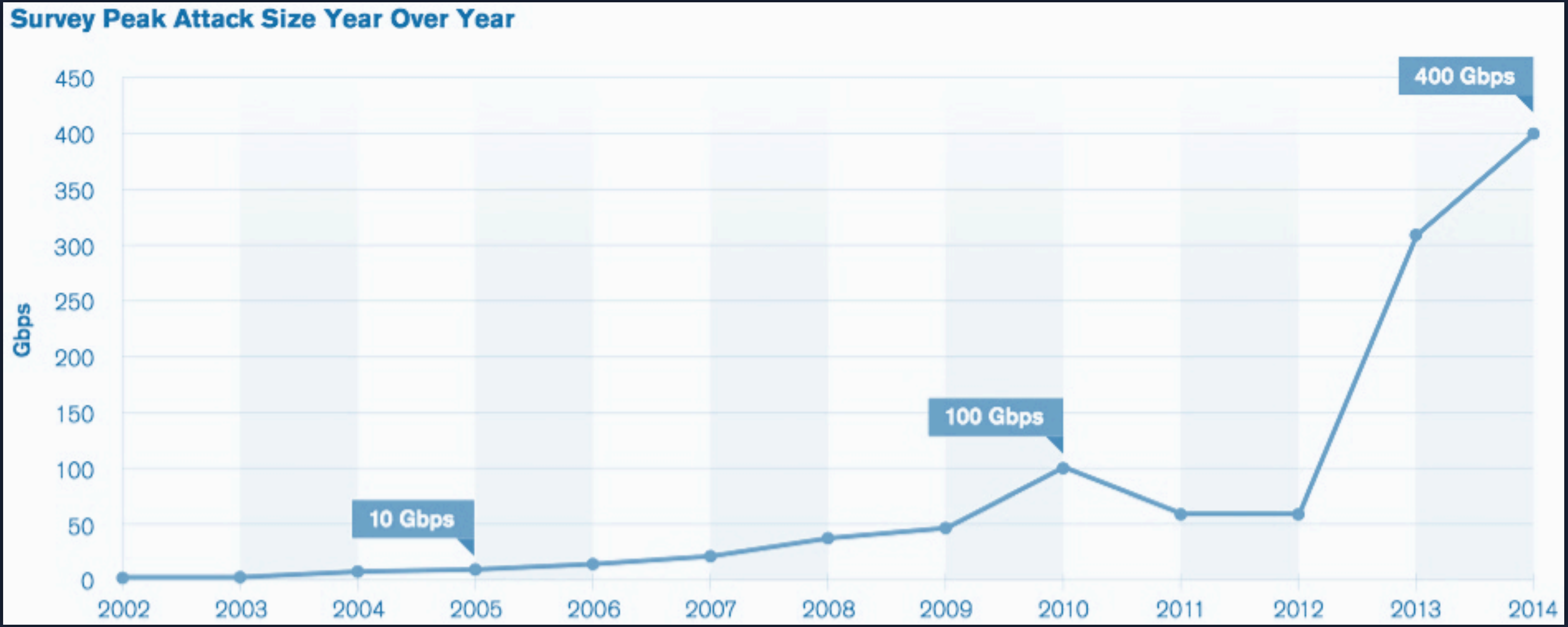


Image from Arbor Networks

EVER LARGER ATTACKS

300 Gbps – Spamhaus (Mar, 2013)

- One of the first heavily documented attacks
- World’s largest anti-spam organization
- Launched by spammers and bullet-proof hosting proviers

https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/
https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet
https://krebsonsecurity.com/2016/08/inside-the-attack-that-almost-broke-the-internet/#more-35925

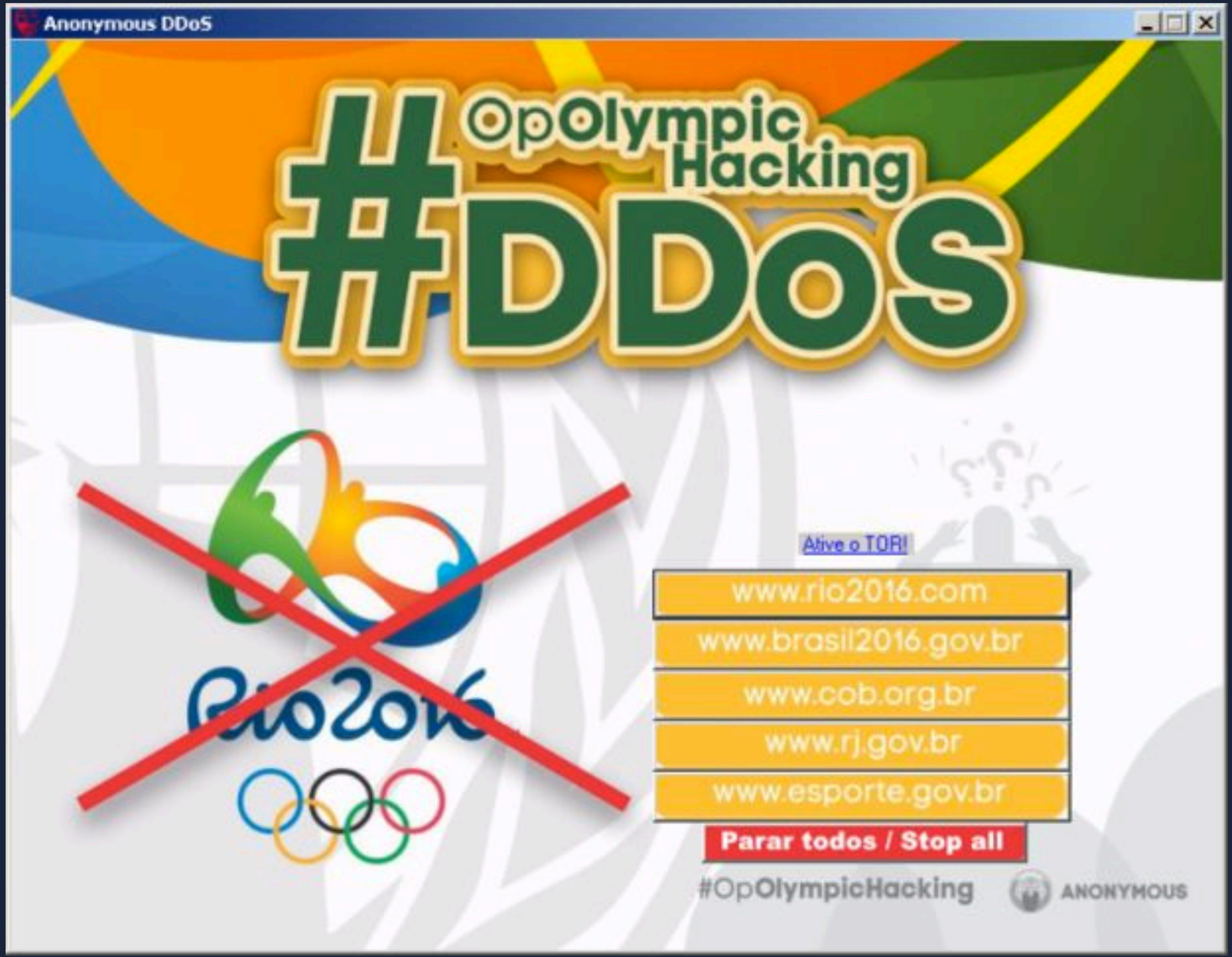
EVER LARGER ATTACKS

579 Gbps – Rio Olympics (August, 2016)

- Brazilian Olympic and governmental websites
- Sustained attacks
- Hacktivists (ANONYMOUS)
  - Windows application
  - Layer-7 attack over TOR

EVER LARGER ATTACKS

579 Gbps – Rio Olympics (August, 2016)



http://news.softpedia.com/news/anonymous-created-special-ddos-tool-just-for-the-opolympichacking-attacks-507500.shtml

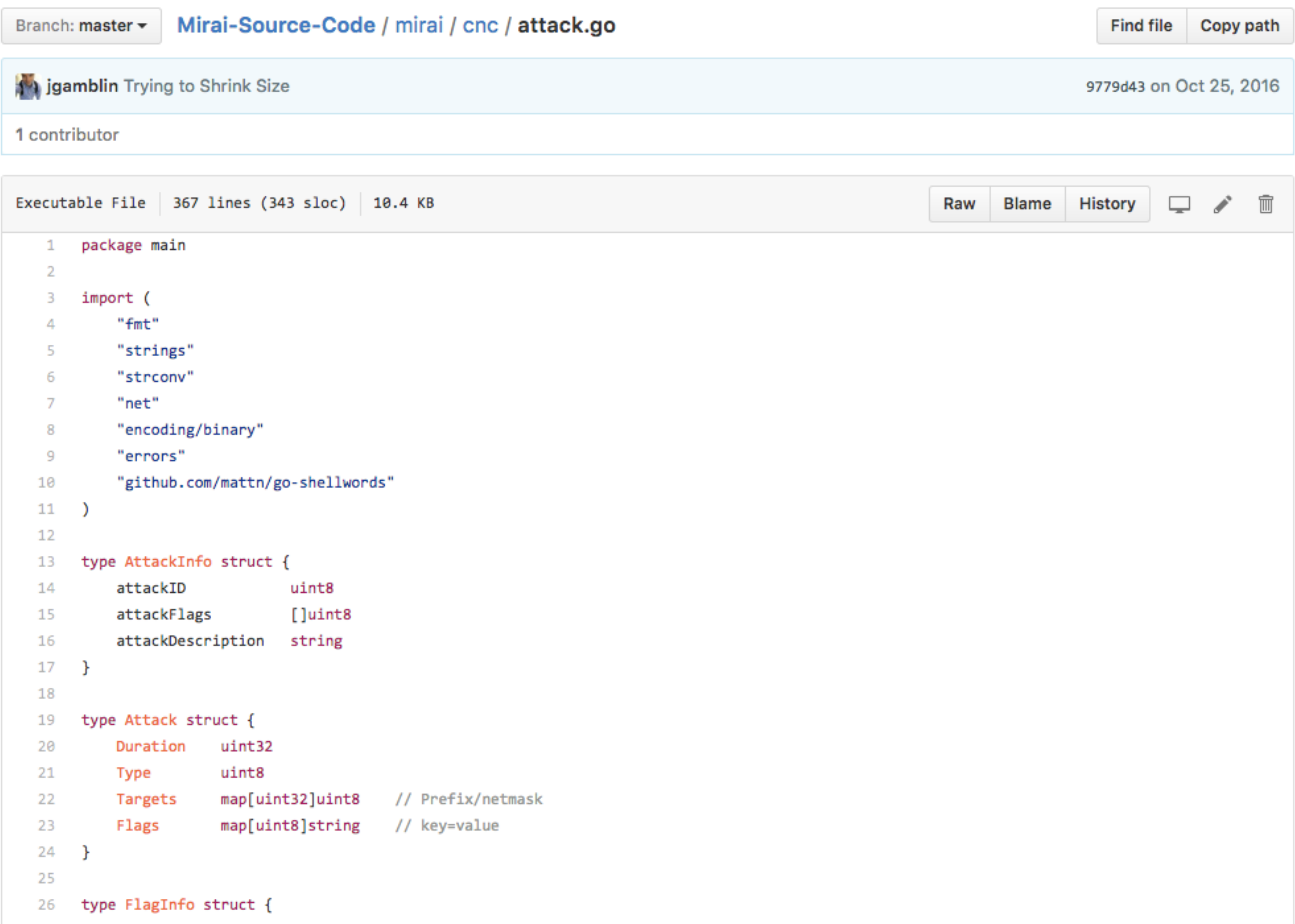
The advent of the IoT botnets

When printers and camera’s attack

EVER LARGER ATTACKS

Mirai – IoT Botnet

- telnet login attempts
- 60 factory default usernames and passwords
- Spreads like a worm
- Different DDoS attack methods
  - Network-layer and application-layer



Mirai-Source-Code / mirai / cnc / attack.go

jgamblin Trying to Shrink Size 9779d43 on Oct 25, 2016

1 contributor

Executable File | 367 lines (343 sloc) | 10.4 KB

```go
package main

import (
    "fmt"
    "strings"
    "strconv"
    "net"
    "encoding/binary"
    "errors"
    "github.com/mattn/go-shellwords"
)

type AttackInfo struct {
    attackID            uint8
    attackFlags         []uint8
    attackDescription   string
}

type Attack struct {
    Duration    uint32
    Type        uint8
    Targets     map[uint32]uint8    // Prefix/netmask
    Flags       map[uint8]string    // key=value
}

type FlagInfo struct {
```

EVER LARGER ATTACKS

620 Gbps – KrebsOnSecurity.com (Sep 20, 2016)

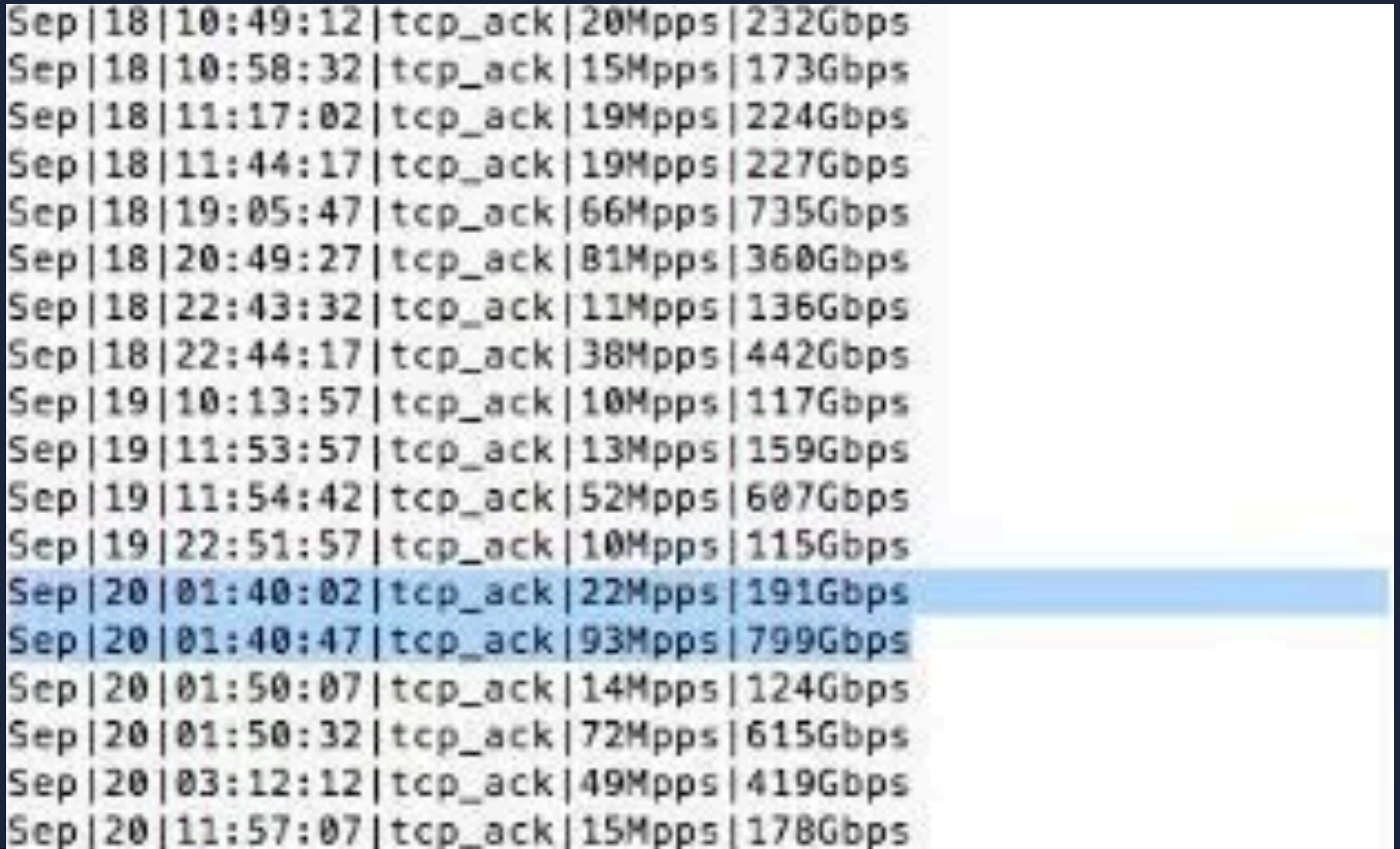
- Security Journalist/Researcher
- Abandoned by his pro-bono DDoS mitigation provider
- Mirai + BASHLITE

https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

EVER LARGER ATTACKS

799+ Gbps – OVH (Sep 18-22, 2016)

- Webhosting company
- Mirai
- Same actors as KrebsOnSecurity.com



```
Sep|18|10:49:12|tcp_ack|20Mpps|232Gbps
Sep|18|10:58:32|tcp_ack|15Mpps|173Gbps
Sep|18|11:17:02|tcp_ack|19Mpps|224Gbps
Sep|18|11:44:17|tcp_ack|19Mpps|227Gbps
Sep|18|19:05:47|tcp_ack|66Mpps|735Gbps
Sep|18|20:49:27|tcp_ack|81Mpps|360Gbps
Sep|18|22:43:32|tcp_ack|11Mpps|136Gbps
Sep|18|22:44:17|tcp_ack|38Mpps|442Gbps
Sep|19|10:13:57|tcp_ack|10Mpps|117Gbps
Sep|19|11:53:57|tcp_ack|13Mpps|159Gbps
Sep|19|11:54:42|tcp_ack|52Mpps|607Gbps
Sep|19|22:51:57|tcp_ack|10Mpps|115Gbps
Sep|20|01:40:02|tcp_ack|22Mpps|191Gbps
Sep|20|01:40:47|tcp_ack|93Mpps|799Gbps
Sep|20|01:50:07|tcp_ack|14Mpps|124Gbps
Sep|20|01:50:32|tcp_ack|72Mpps|615Gbps
Sep|20|03:12:12|tcp_ack|49Mpps|419Gbps
Sep|20|11:57:07|tcp_ack|15Mpps|178Gbps
```

http://securityaffairs.co/wordpress/51640/cyber-crime/tbps-ddos-attack.html

EVER LARGER ATTACKS

1.2 Tbps – Dyn (Oct 21, 2016)

- Managed DNS provider
- Many high-profile customers’ websites down
- Mirai
- Perpetrators and motives remain unclear

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

EVER LARGER ATTACKS

1.2 Tbps – Dyn (Oct 21, 2016)

Airbnb
Amazon.com
Ancestry.com
The A.V. Club
BBC
The Boston Globe
Box
Business Insider
CNN
Comcast
CrunchBase
DirecTV
Elder Scrolls Online
Electronic Arts
Etsy

EQAO
FiveThirtyEight
Fox News
The Guardian
GitHub
Grubhub
HBO
Heroku
HostGator
iHeartRadio
Imgur
Indiegogo
Mashable
NHL
Netflix

New York Times
Overstock.com
PayPal
Pinterest
Pixlr
PlayStation
Qualtrics
Quora
Reddit
Roblox
Ruby Lane
RuneScape
SaneBox
Seamless
Second Life

Shopify
Slack
SoundCloud
Squarespace
Spotify
Starbucks
Storify
Swedish Civil
Contingencies Agency
Swedish Government
Tumblr
Twilio
Twitter
Verizon Communications
Visa

Vox Media
Walgreens
Wall Street Journal
Wikia
Wired
Wix.com
WWE Network
Xbox Live
Yammer
Yelp
Zillow

EVER LARGER ATTACKS

1.2 Tbps – Dyn (Oct 21, 2016)

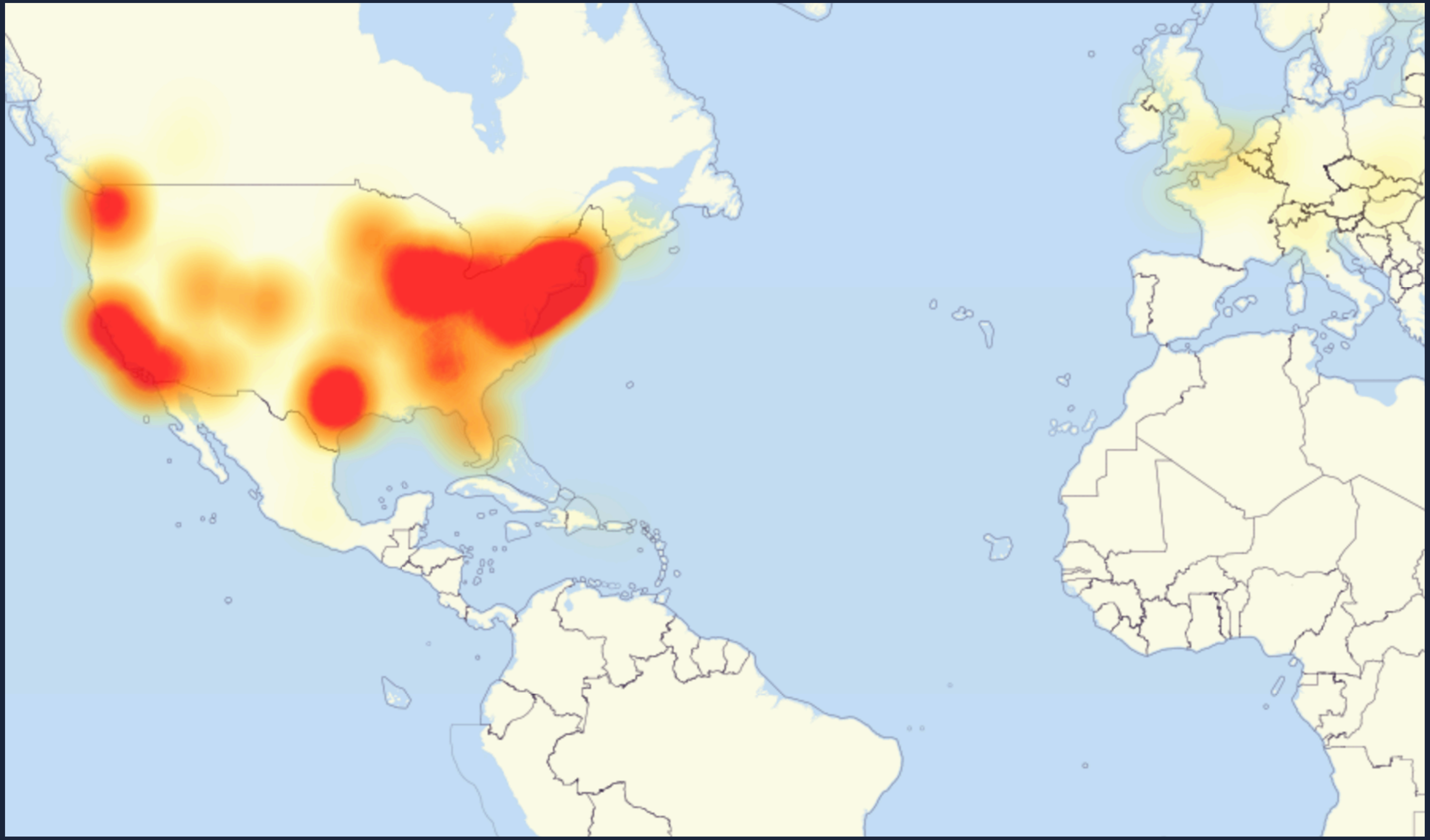
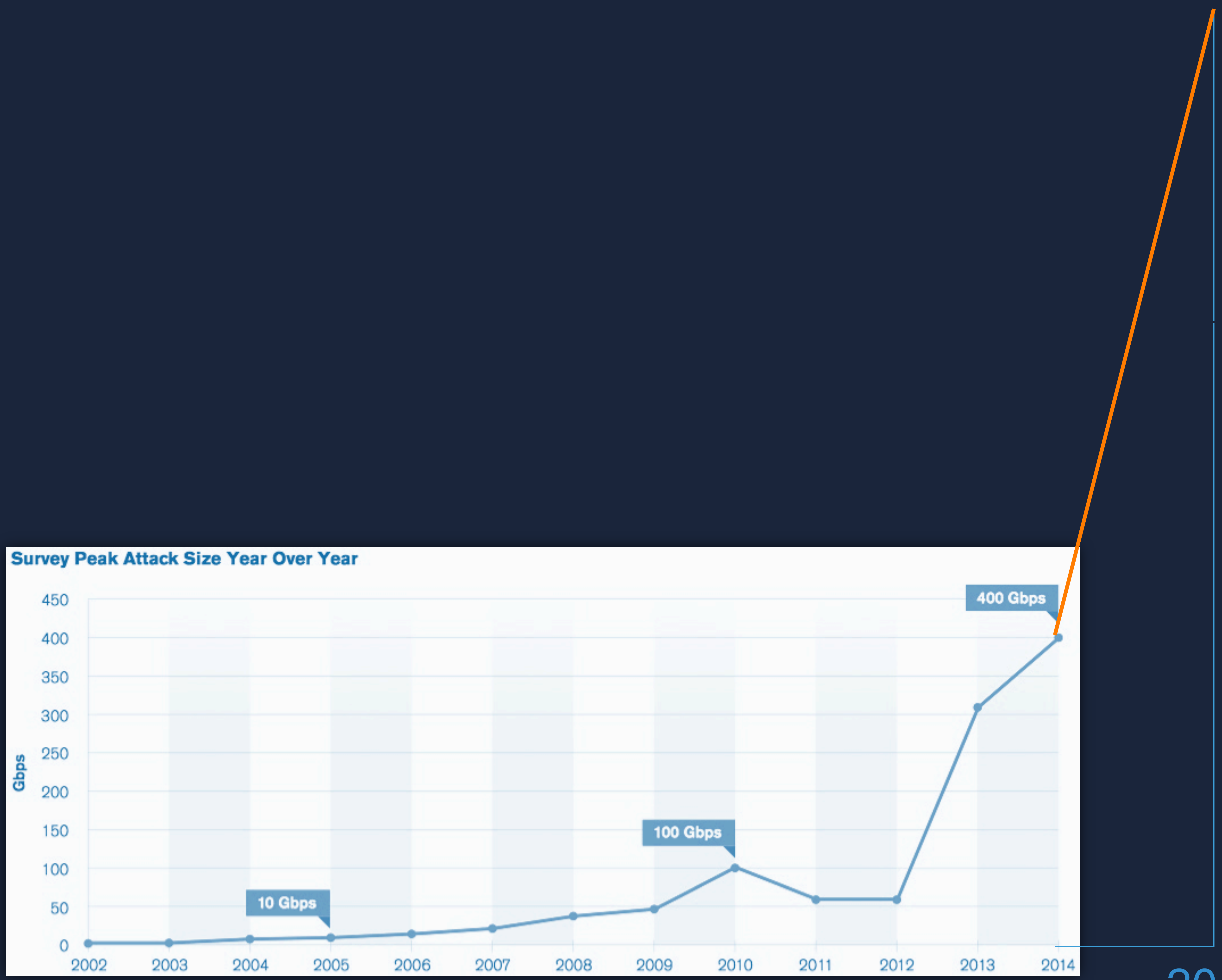


Image from Level3

EVER LARGER ATTACKS



1200 Gbps

2017

Image from Arbor Networks

MORE COMMON ATTACKS

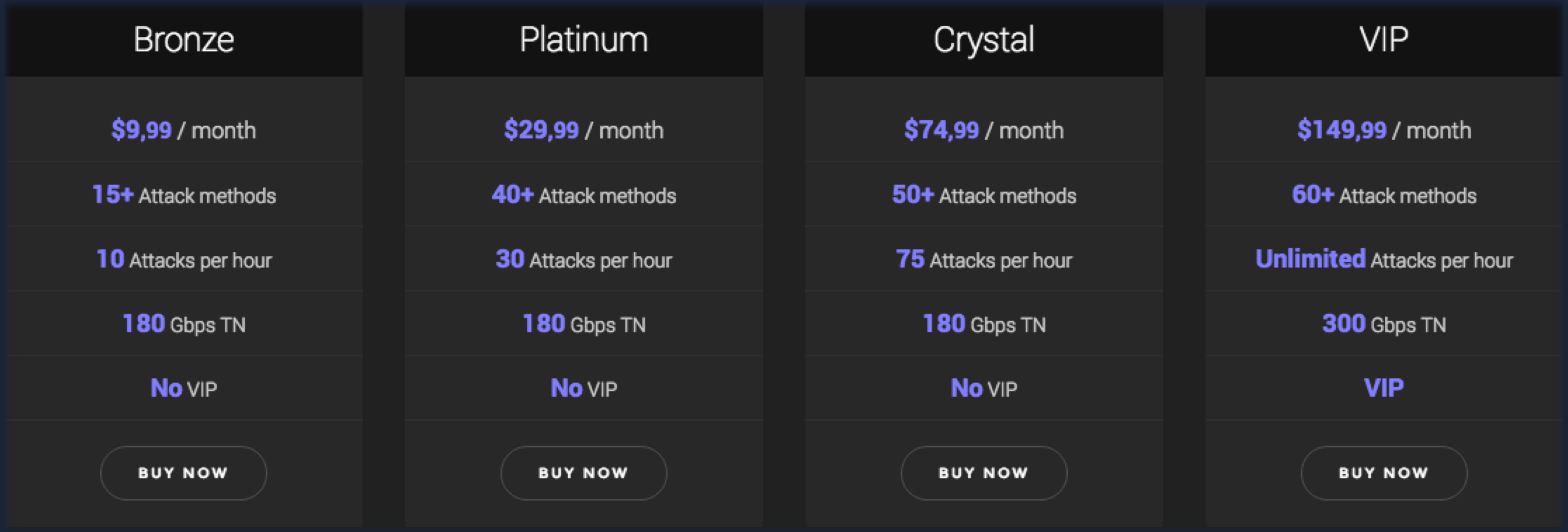
DDoS attacks – *more common*

- A plethora of DDoS-as-a-service providers (“*stressers*” or “*booters*”)

  DDoS attack at the click of a button

  Very cheap (in line with their quality)

  http://str3ssed.me



Bronze	Platinum	Crystal	VIP
$9,99 / month	**$29,99** / month	**$74,99** / month	**$149,99** / month
15+ Attack methods	**40+** Attack methods	**50+** Attack methods	**60+** Attack methods
10 Attacks per hour	**30** Attacks per hour	**75** Attacks per hour	**Unlimited** Attacks per hour
180 Gbps TN	**180** Gbps TN	**180** Gbps TN	**300** Gbps TN
No VIP	**No** VIP	**No** VIP	**VIP**
BUY NOW	BUY NOW	BUY NOW	BUY NOW

CLOUD-BASED SECURITY

CLOUD-BASED SECURITY

Quick recap

- Flooding web servers with loads of traffic to take it down

    Volumetric attacks

    Application-level attacks

- Attacks become ever larger and more common

- Classic on-premises security devices are usually ineffective

    Network connections saturate

CLOUD-BASED SECURITY

Quick recap

- Flooding web servers with loads of traffic to take it down

  Volumetric attacks

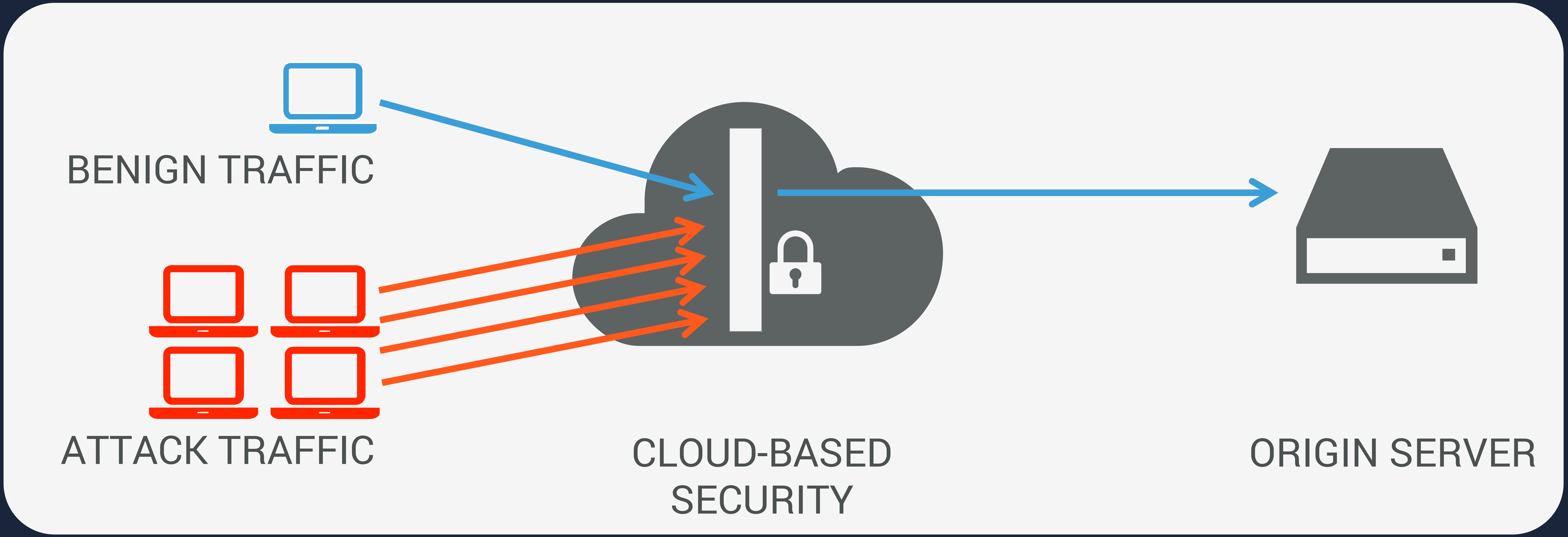
  Application-level attacks

- Attacks become ever larger and more common

- Classic on-premises security devices are usually ineffective

  Network connections saturate

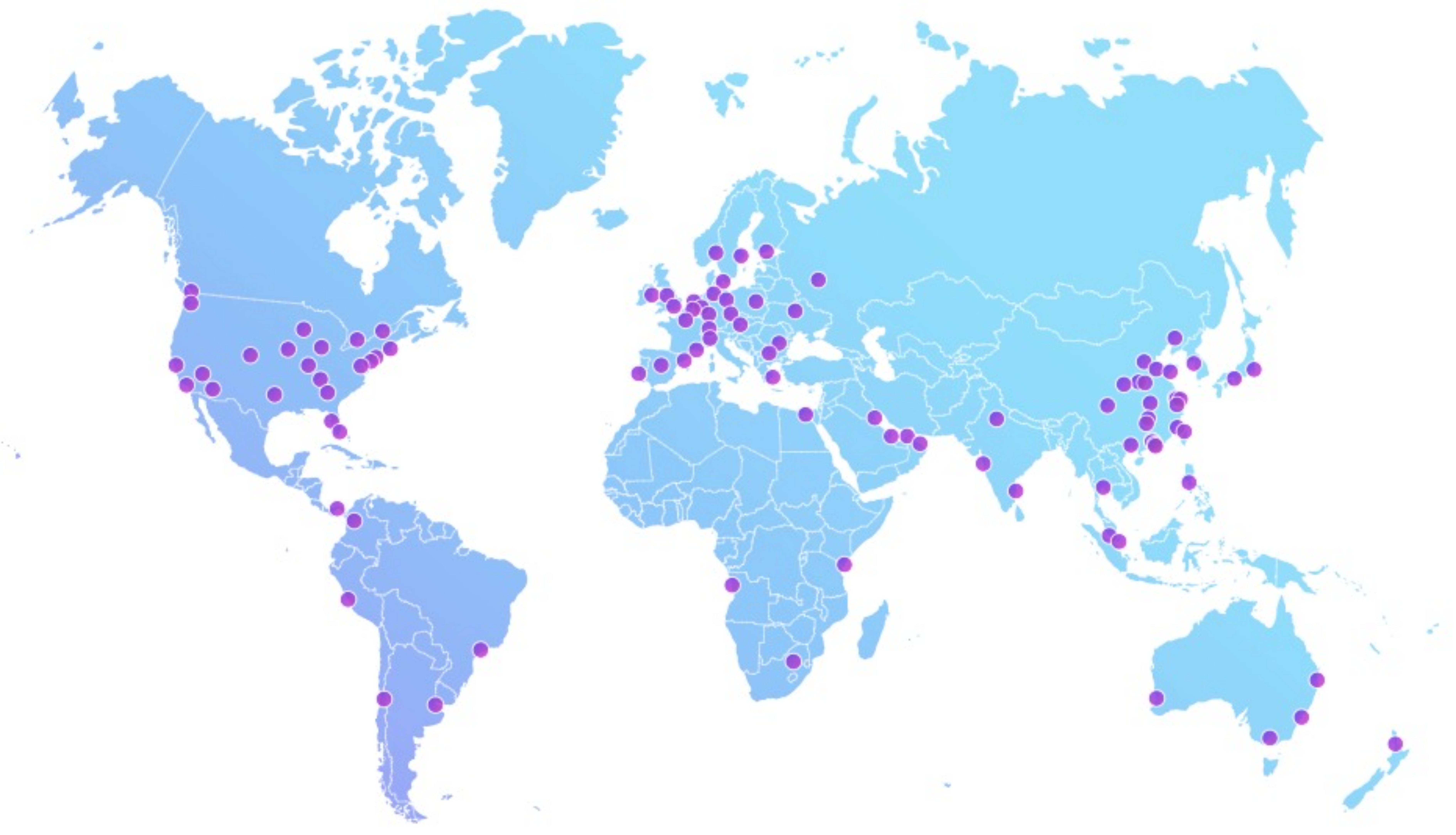
CLOUD-BASED SECURITY



CBSPs reroute and filter the customers’ traffic through their cloud

> CBSP forwards clean traffic to customer’s server

CLOUD-BASED SECURITY



Source: cloudflare.com/network

CLOUD-BASED SECURITY

Side note: This is also about…
Web application attacks

Cloud-based security usually filter several Layer-7 attacks with their web application firewall (WAF)

> SQL injections, XSS, …

CLOUD-BASED SECURITY

Cloud-based security: several flavors

- DNS vs. BGP rerouting to scrubbing centers
- On-demand vs. always-on

  On-demand requires in-house expertise or CPE to decide when to flick the switch
- Other types

  On-premises, hybrid protection, DDoS protection by ISPs (Clean Pipes), …

CLOUD-BASED SECURITY

BGP rerouting

- Requires a Class C network infrastructure (/24 IP range)
- AS of CBSP will announce your IP ranges
- Reroutes packets on the “IP level” to scrubbing center
- CBSP tunnels packets back to you (GRE)

Images on next two slides from neustar.biz and thousandeyes.com

SITEPROTECT

1) After BGP announcement, all traffic is drawn to Neustar SiteProtect scrubbing cloud.

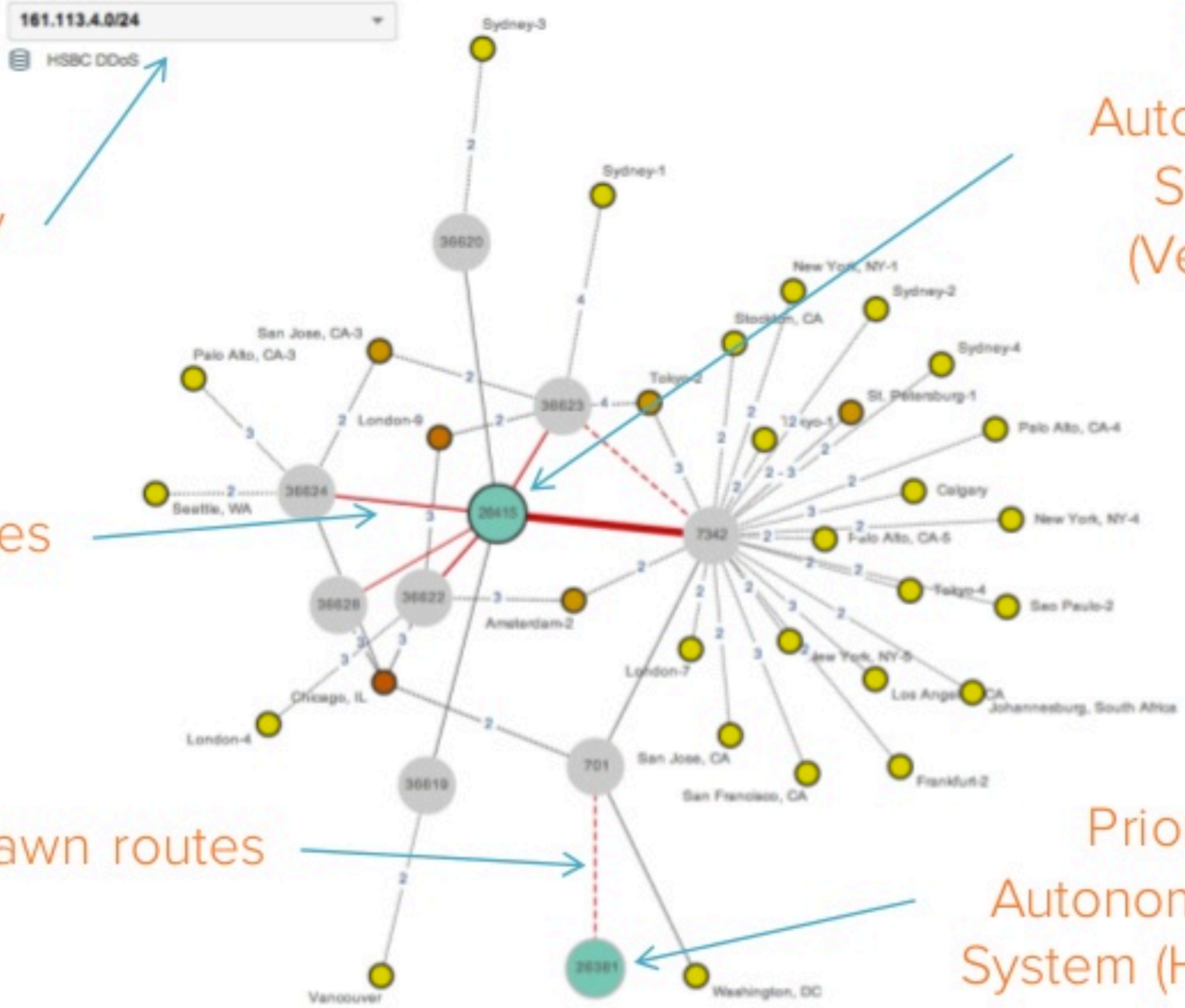
2) Our Scrubbing centers clean your traffic in the cloud, allowing legitimage traffic to proceed to your infrastructure.

3) Cleaned traffic is sent to you via GRE tunnels

4) Final response sent back to legitimate visitor. Good to go!

Source: Neustar

DDoS Attack: Mitigation Handoff Using BGP



Prefixes automatically identified

New Autonomous System (VeriSign)

New routes

Withdrawn routes

Prior Autonomous System (HSBC)

CLOUD-BASED SECURITY

DNS rerouting

- Redirects traffic on the "domain level"
  - i.e. domain name resolves to IP of CBSP
  - CBSP forwards traffic to IP of client (~reverse proxy)

    > Rely on HTTP Host header to forward to correct customer

- Unprotected:

```
example.com → 11.22.11.22
```

- Protected:

```
example.com → 33.44.33.44 [ → 11.22.11.22 ]
```

Cloud-based security: several flavors

- DNS vs. BGP rerouting to scrubbing centers

  BGP requires a Class C network infrastructure (/24 IP range)

- On-demand vs. always-on

  On-demand requires in-house expertise or CPE to decide when to flick the switch

Popular solution

10% of top 10,000 websites use DNS-rerouting, always-on cloud security services

CLOUD-BASED SECURITY

Always-on + DNS…? What are these services?

- Often a combination of CDN + Security services

  The geographically distributed nature of CDNs is ideal for high-absorbing scrubbing centers

- “DDoS protection for the masses”

  > No infrastructural requirements

  > No expertise needed

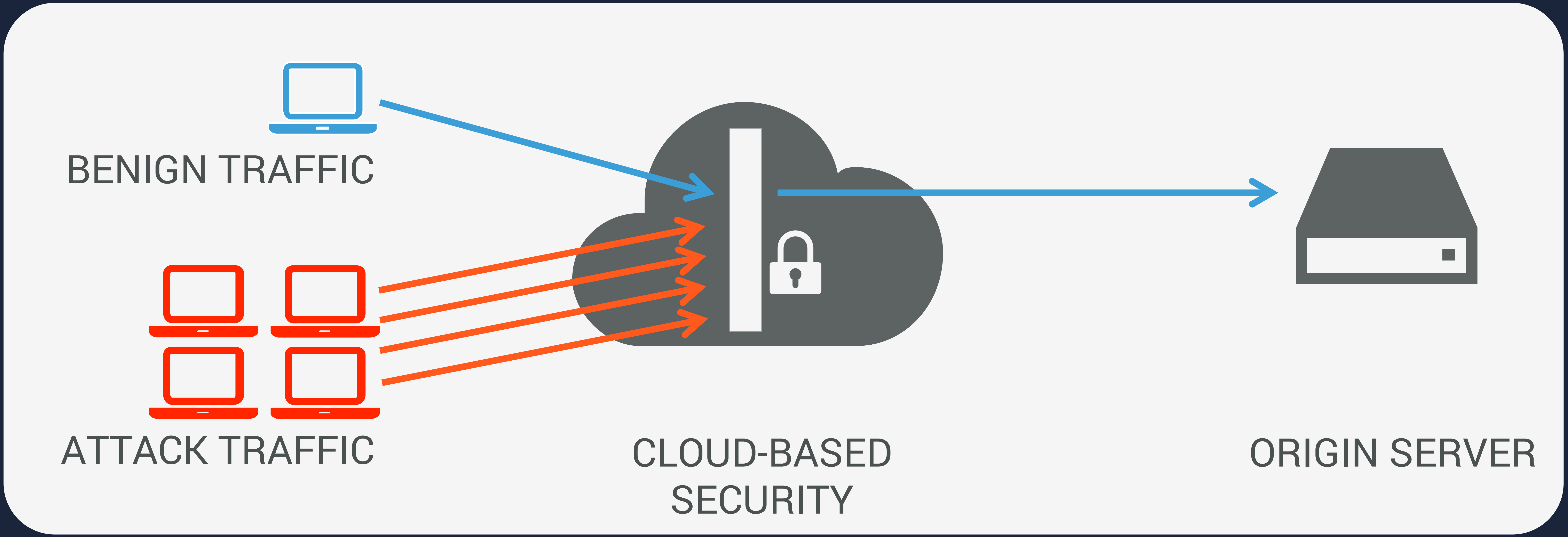
  > Quick and easy installation (change DNS records)

  > Low cost (sometimes free)

CLOUDFLARE
DOS arrest Internet security
sucuri
Incapsula
Akamai

PITFALLS

CLOUD-BASED SECURITY PITFALL

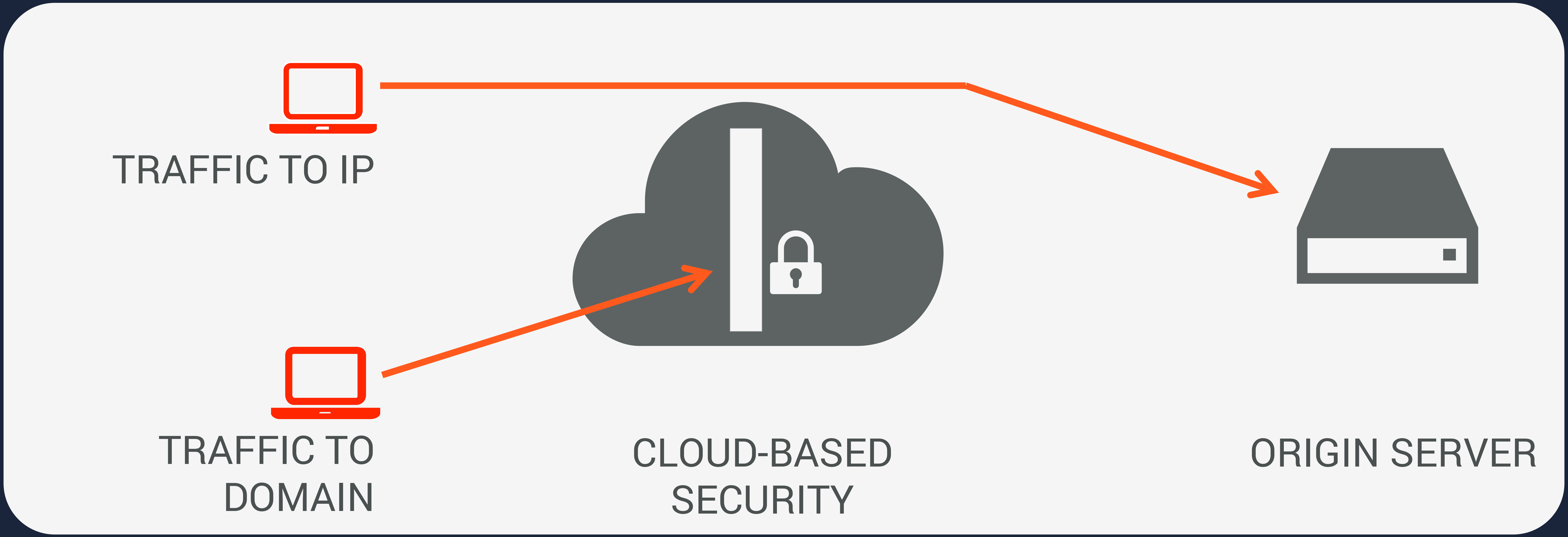


CBSPs reroute and filter the customers' traffic through their cloud

> *Customer's domain name resolves to CBSP's infrastructure*

> *CBSP forwards clean traffic to customer's server (=origin's IP address)*

CLOUD-BASED SECURITY PITFALL



“DIRECT-TO-IP ATTACKS”

> Origin’s IP address should be kept secret
> Exposure of the IP address jeopardizes the entire security mechanism

LARGE-SCALE ANALYSIS

- 1. Sampled ~18,000 domains using always-on DNS-based cloud security
- 2. Tested for 8 potential origin IP leaks on each of them
- 3. Subjected all candidate origin IP addresses to a verification test

  > Filtered out IP addresses belonging to CBSPs

  > Retrieve home page via CBSP

  > Retrieve home page via candidate IP address

  > If both return the same page, the candidate IP address is an origin

LARGE-SCALE ANALYSIS

our large-scale evaluation of 18,000 CBSP protected domains reveals that

7 of 10

websites are exposed through at least one vulnerability

VISSERS, T., VAN GOETHEM, T., JOOSEN, W., AND NIKIFORAKIS, N.
Maneuvering Around Clouds: Bypassing Cloud-based Security Providers.
In CCS (2015), ACM.

COVERAGE

Cloudpiercer Discovery Tool

By Akamai SIRT Alerts October 9, 2015 12:37 PM
0 Comments

Researchers have released details of a tool that allows users to discover orig
Cloudpiercer, which uses a number of techniques to locate origin servers' IP a

The Cloudpiercer tool bundles several previously known methods with some
reconnaissance against targets. It's a reconnaissance tool, not an attack tool.
methods to search for a customer's datacenter IP addresses or netblock(s) bu
technologies to perform an actual DDoS or web application attack.

Akamai's Security Intelligence Research Team (SIRT) has analyzed the meth
following observations.

Cloudpiercer requires verification of ownership of a site for it to be tested. Thi

The Incapsula Blog

12 Oct 2015

How to Prevent "Origin Exposing" Attacks (CloudPiercer Study)

By Igal Zeifman

Share Tweet Share Share

eleased an interesting paper on the topic c
circumvent cloud-based security solution
ased DDoS mitigation, such as Incapsula W

Strengthen Your Cloud-Based DDoS Protection

October 10, 2015 by Scott Altman 87

article ddos security silverline

Reduce your risk from CloudPiercer and other discovery tools

Companies build out public-facing web presences for a variety of reasons, but most often their goal is to boost brand awareness or provide a transaction point for the exchange of services, information, money, etc. These websites are, by nature, publicly accessible, which means that organizations must build defenses to protect them from various threats. One of the most dangerous threats in today's security ecosystem is that of Distributed Denial of Service (DDoS) attacks.

The CloudPiercer Problem: 70 percent of cloud-based DDoS mitigation systems can be bypassed by attackers

Posted on 6th January 2016 by Max Pritchard in Opinion Technology.

CloudPiercer: Is your cloud-protected w

In October 2015, an academic study paper relating to th
("Maneuvering Around Clouds: Bypassing Cloud-based Se
that rely on cloud-based DDoS mitigation are often still v

TechRepublic. CXO Innovation Cloud Security Big Data

SECURITY

DDoS mitigation
site vulnerable

DNS rerouting does not eliminate the possib
way to reduce your site's risk is to use this IP address scanning tool.

By Michael Kassner | December 27, 2015, 7:36 AM PST

FORTINET Home Categories Archive

Fear of a Filled Pipe - The Origin Exposed

by Hemant Jain | Oct 12, 2015 | Filed in: Industry Trends & News

Volumetric attacks were the reason for the birth and growth of cloud based DDoS attack mitigation service providers. With the recent research rela
flaw in the current solutions has been uncovered. The paper linked here exposes critical weaknesses in the mechanisms for cloud-based DDoS att
weaknesses of the vendors in the space.

Premise of a Cloud Based Security Provider

Cloud based security providers base their value around a few key points:

1. Attacks should be blocked closer to the source via a globally distributed network of mitigation nodes.

PITFALL 1: SUBDOMAINS

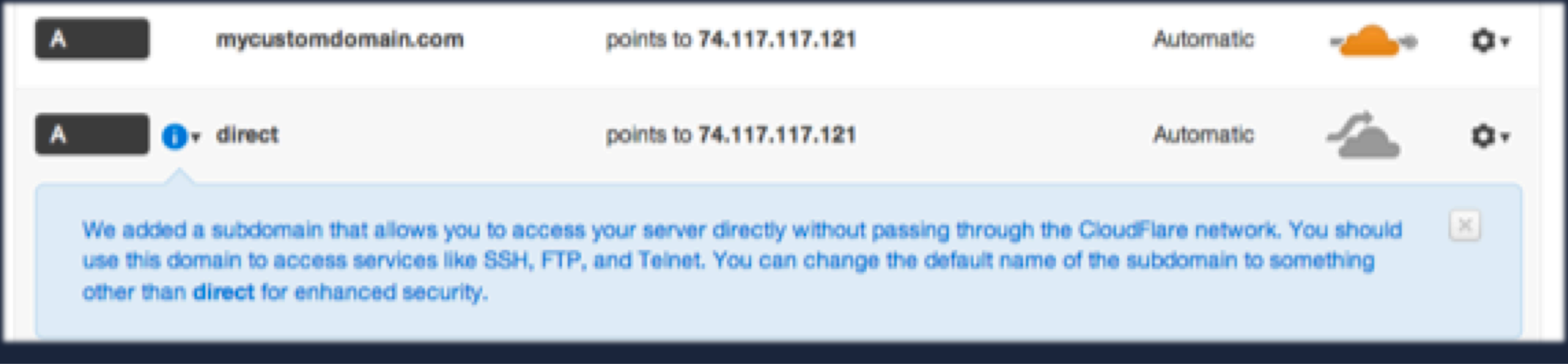
- CBSPs rely on HTTP "*Host*" header to forward requests

  Breaks non-host header protocols (FTP, SSH, …)

  `ssh root@domain.com` *now connects to the CBSP without any notion of the domain*

  `ssh root@104.131.120.106` *must be used*

- "Let's just use a direct-to-origin subdomain for SSH!"



A	mycustomdomain.com	points to **74.117.117.121**	Automatic	
A	direct	points to **74.117.117.121**	Automatic	

We added a subdomain that allows you to access your server directly without passing through the CloudFlare network. You should use this domain to access services like SSH, FTP, and Telnet. You can change the default name of the subdomain to something other than **direct** for enhanced security.

PITFALL 1: SUBDOMAINS

Our findings

- Scanned 5,000 subdomains per domain

  Verified each IP address to which they resolved

- 43% of domains had a direct-to-origin “backdoor”

ftp.example.com	(3,952 domains)
direct.example.com	(3,583 domains)
mail.example.com	(3,203 domains)
…	

PITFALL 2: DNS RECORDS

- Other DNS records might still reveal your origin

- Example – SPF records

```
"v=spf1  ip4:104.237.146.167 -all”
```

TXT record that allows you to publish IPs authorized to send email on your domain’s behalf.
Removing your origin from this record will result in those emails being classified as spam.

- Example – MX records

CBSPs don’t process or forward your emails.

PITFALL 2: DNS RECORDS

Our findings

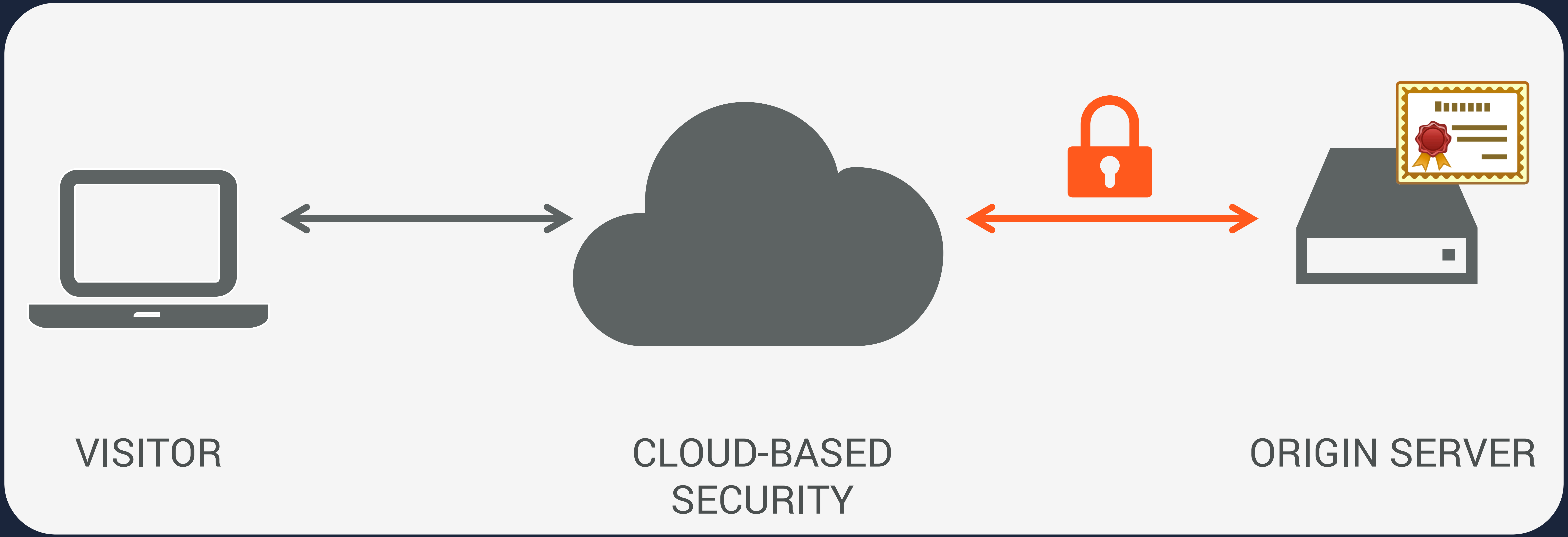
- Queried all DNS RR types for every domain

  We extracted and verified each IP address that we found.

- 28% of domains are vulnerable

MX records	(4,390 domains)
TXT records	(1,134 domains)
Sometimes even A or AAAA records	

PITFALL 3: SSL CERTIFICATES



- HTTPS connection between CBSP and origin

  Origin server has to present certificate.
  This certificate contains the domain name.

PITFALL 3: SSL CERTIFICATES

Our findings

- Harvest certificates from all IP addresses

  Data from Project Sonar. (https://scans.io/study/sonar.ssl)

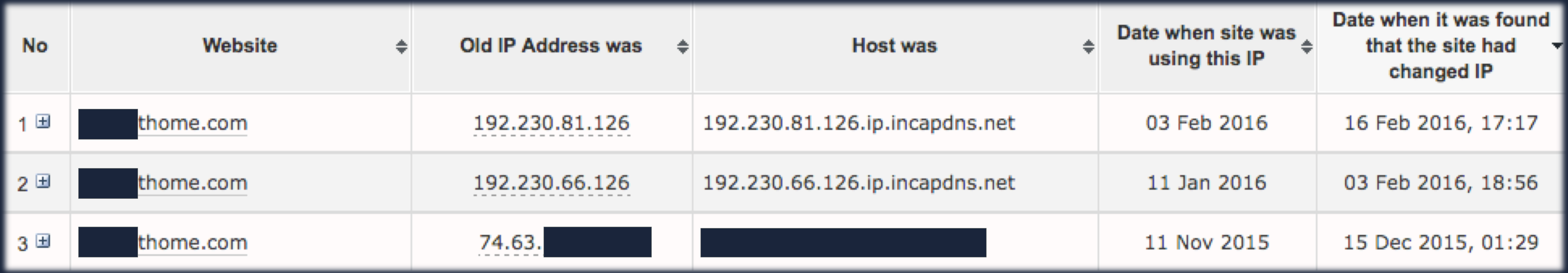
  Censys.io: a new search engine for this data.

- 9% of domains are revealing their origin by publicly presenting the domain’s certificate

PITFALL 4: IP HISTORY

- "The Internet never forgets": companies constantly track DNS changes

  Historical databases of previously used IP addresses (e.g. domaintools.com, myip.ms, …).
  Your origin IP address might be listed.



No	Website	Old IP Address was	Host was	Date when site was using this IP	Date when it was found that the site had changed IP
1 ⊞	[redacted]thome.com	192.230.81.126	192.230.81.126.ip.incapdns.net	03 Feb 2016	16 Feb 2016, 17:17
2 ⊞	[redacted]thome.com	192.230.66.126	192.230.66.126.ip.incapdns.net	11 Jan 2016	03 Feb 2016, 18:56
3 ⊞	[redacted]thome.com	74.63.[redacted]	[redacted]	11 Nov 2015	15 Dec 2015, 01:29

- Best practice: new IP address after adopting cloud protection

PITFALL 4: IP HISTORY

Our findings

- We queried these IP History databases

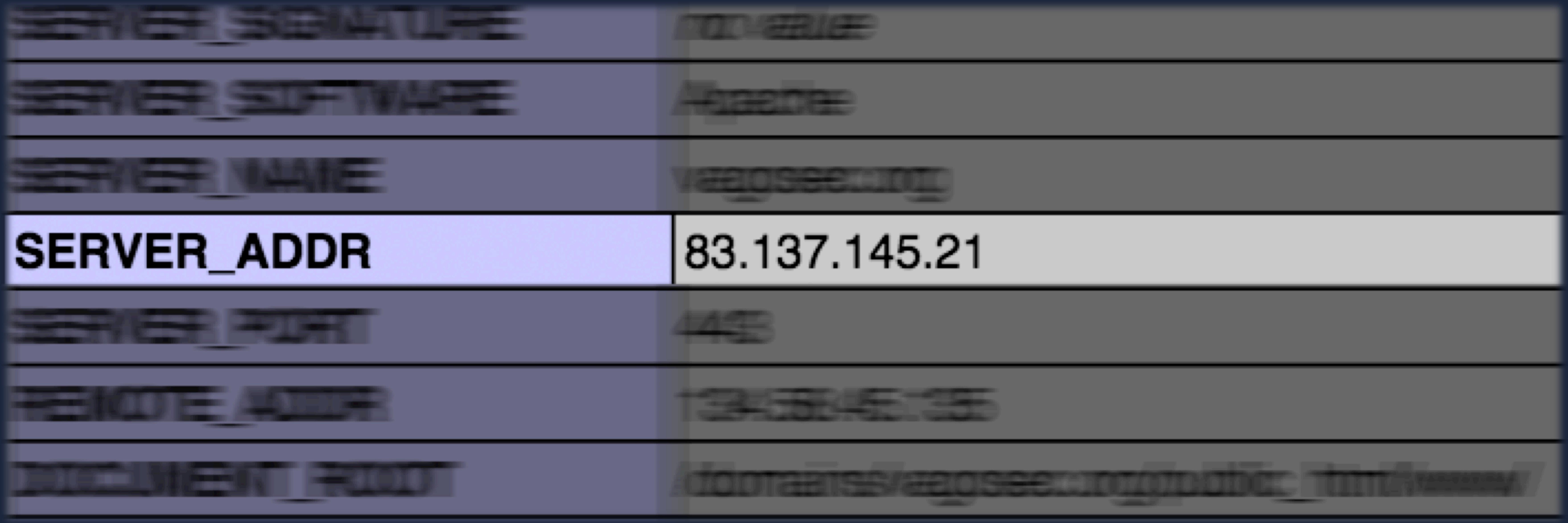
We verified each listed historic IP address for all domains.

- 40% of domains have their origin listed in these databases

PITFALL 5: SENSITIVE FILES

- Publicly accessible sensitive files can expose the origin

    Verbose error messages, log files, configuration files, …



[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
SERVER_ADDR	83.137.145.21
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

PITFALL 5: SENSITIVE FILES

Our findings

- We searched for files that called *phpinfo()* in 4 fixed locations

  /info.php

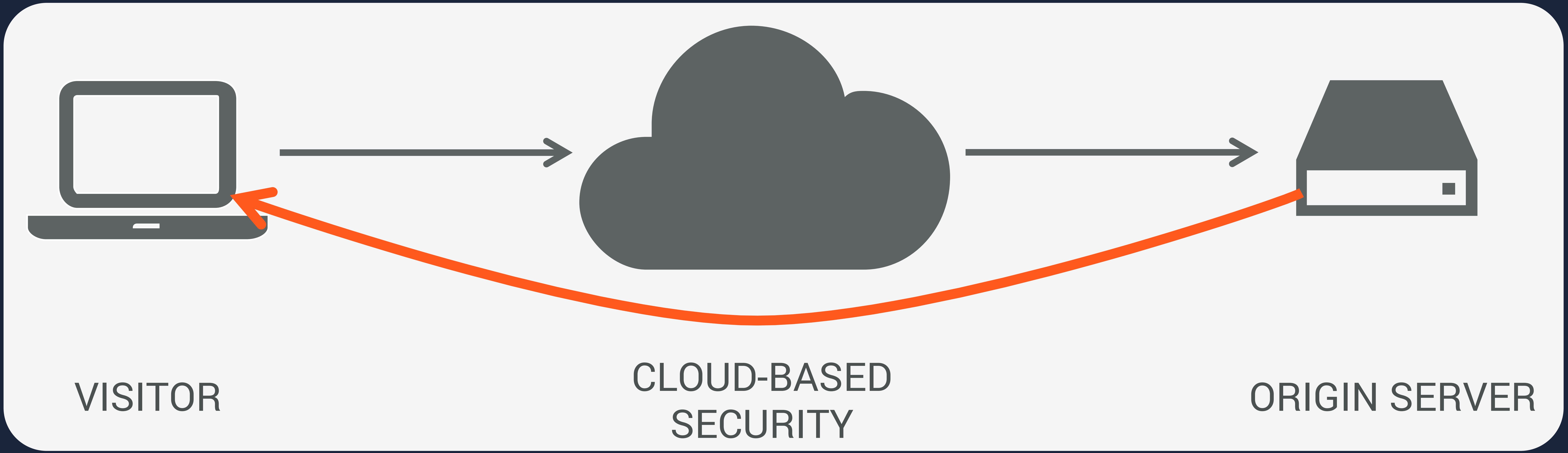
  /phpinfo.php

  /test.php

  /phpMyAdmin/phpinfo.php

- 5% of domains have such files and expose their origin in this fashion

PITFALL 6: OUTBOUND CONNECTIONS



- Triggering an origin to connect to you

  Outbound connections don't pass through CBSP.
  IP address of the origin will be directly visible to destination.
  Usually application specific vulnerabilities.

PITFALL 6: OUTBOUND CONNECTIONS

Our findings

- Triggered a PingBack verification on each web server

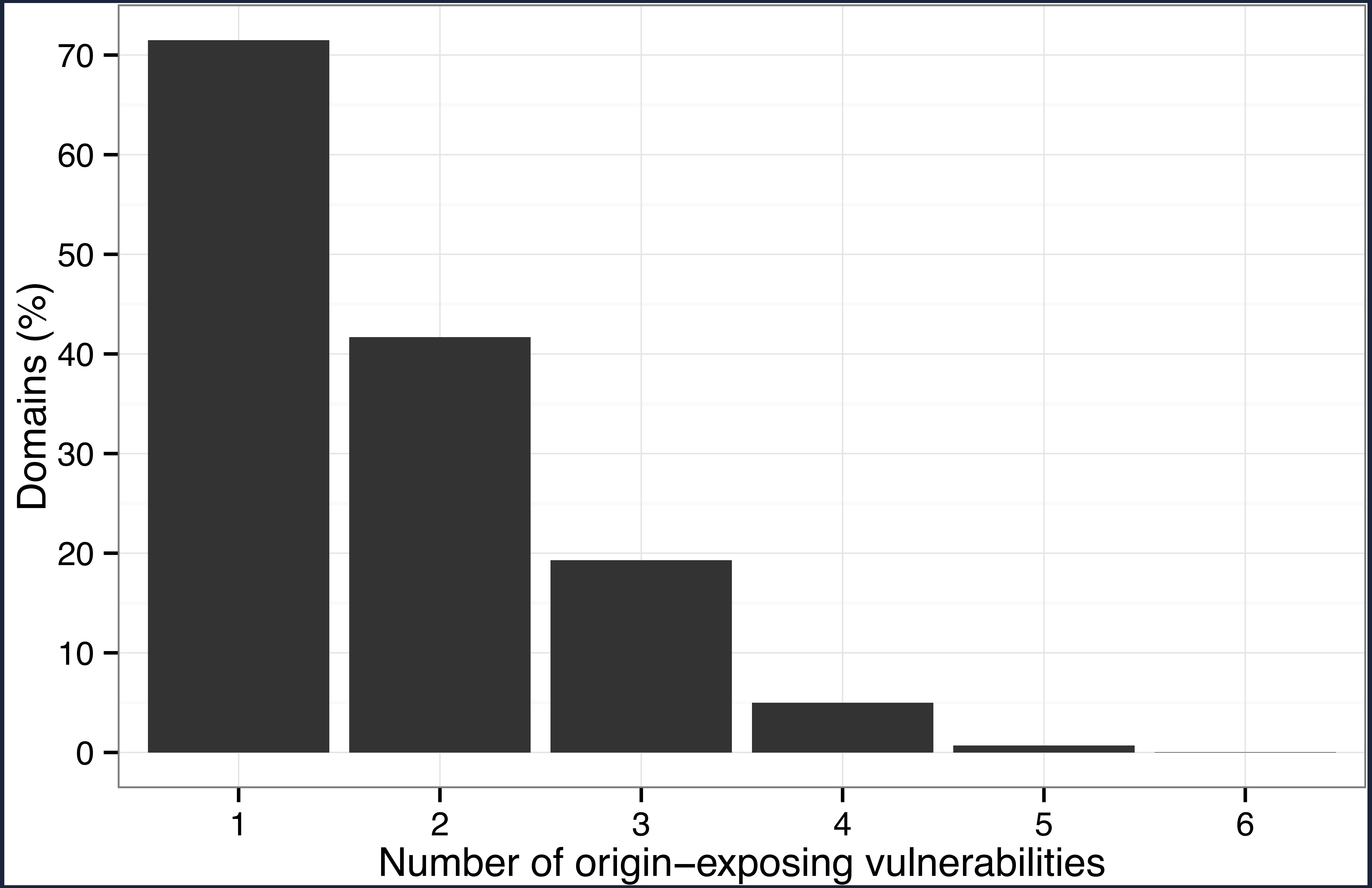
  Web application retrieves the link in the PingBack notification

  Mostly WordPress installations

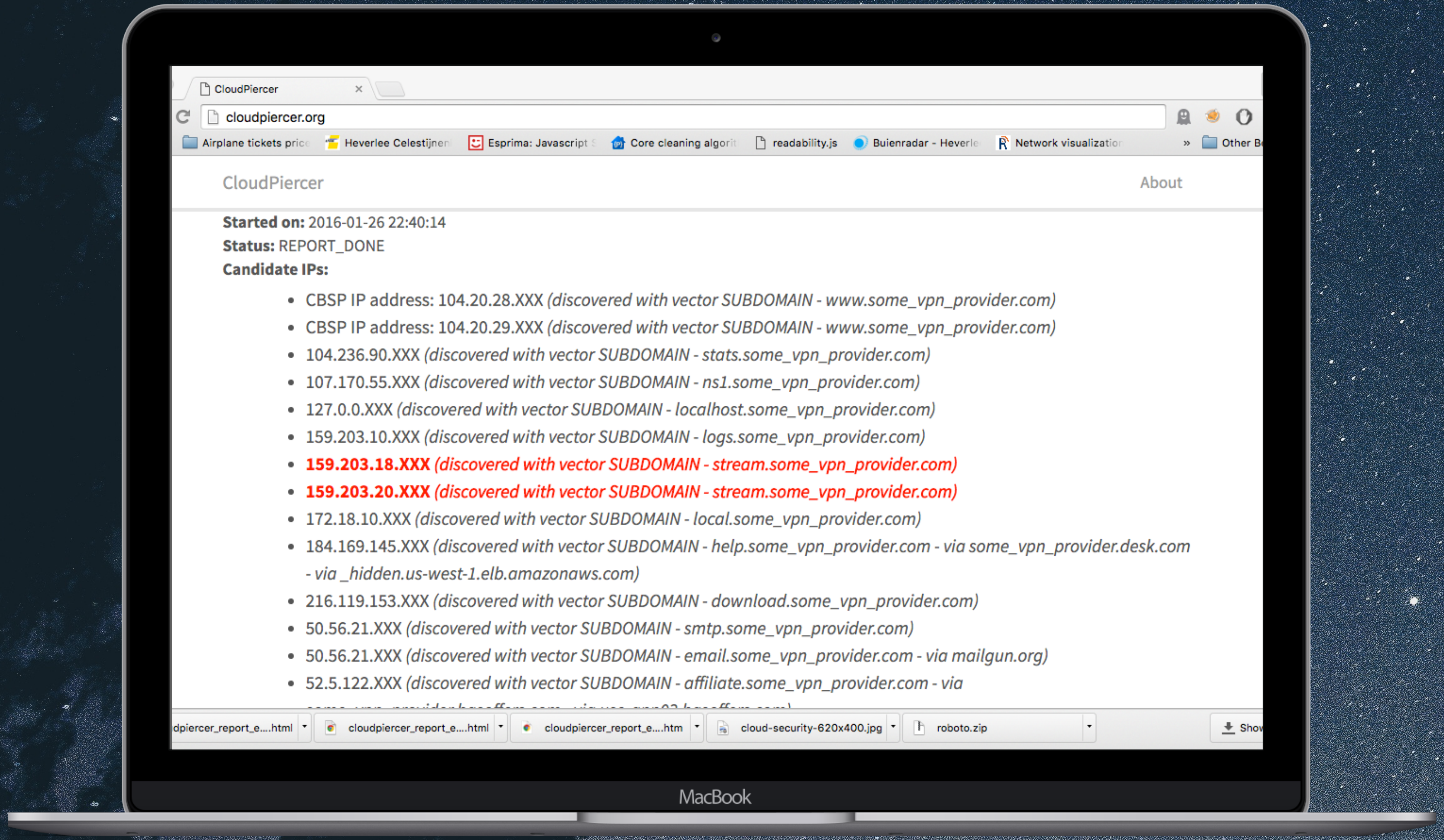
- Our own web server tracked incoming connections

- 7% of domains connected to us using their origin IP address

GOTTA CATCH 'EM ALL



ONLINE TOOL



Started on: 2016-01-26 22:40:14
Status: REPORT_DONE
Candidate IPs:

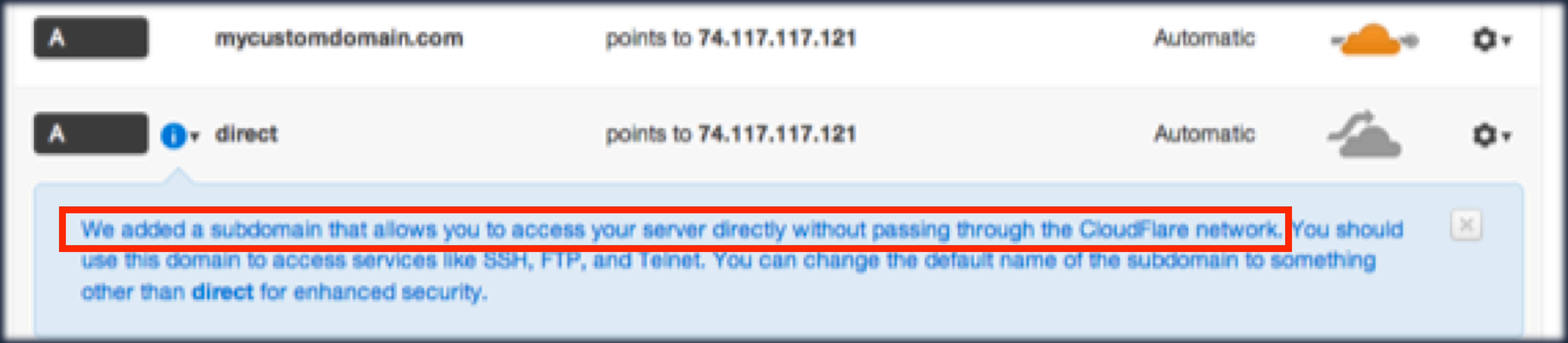
- CBSP IP address: 104.20.28.XXX *(discovered with vector SUBDOMAIN - www.some_vpn_provider.com)*
- CBSP IP address: 104.20.29.XXX *(discovered with vector SUBDOMAIN - www.some_vpn_provider.com)*
- 104.236.90.XXX *(discovered with vector SUBDOMAIN - stats.some_vpn_provider.com)*
- 107.170.55.XXX *(discovered with vector SUBDOMAIN - ns1.some_vpn_provider.com)*
- 127.0.0.XXX *(discovered with vector SUBDOMAIN - localhost.some_vpn_provider.com)*
- 159.203.10.XXX *(discovered with vector SUBDOMAIN - logs.some_vpn_provider.com)*
- **159.203.18.XXX** *(discovered with vector SUBDOMAIN - stream.some_vpn_provider.com)*
- **159.203.20.XXX** *(discovered with vector SUBDOMAIN - stream.some_vpn_provider.com)*
- 172.18.10.XXX *(discovered with vector SUBDOMAIN - local.some_vpn_provider.com)*
- 184.169.145.XXX *(discovered with vector SUBDOMAIN - help.some_vpn_provider.com - via some_vpn_provider.desk.com - via _hidden.us-west-1.elb.amazonaws.com)*
- 216.119.153.XXX *(discovered with vector SUBDOMAIN - download.some_vpn_provider.com)*
- 50.56.21.XXX *(discovered with vector SUBDOMAIN - smtp.some_vpn_provider.com)*
- 50.56.21.XXX *(discovered with vector SUBDOMAIN - email.some_vpn_provider.com - via mailgun.org)*
- 52.5.122.XXX *(discovered with vector SUBDOMAIN - affiliate.some_vpn_provider.com - via*

CLOUDPIERCER.ORG

Prevent origin exposure by using our free online vulnerability scanner!

IMPACT

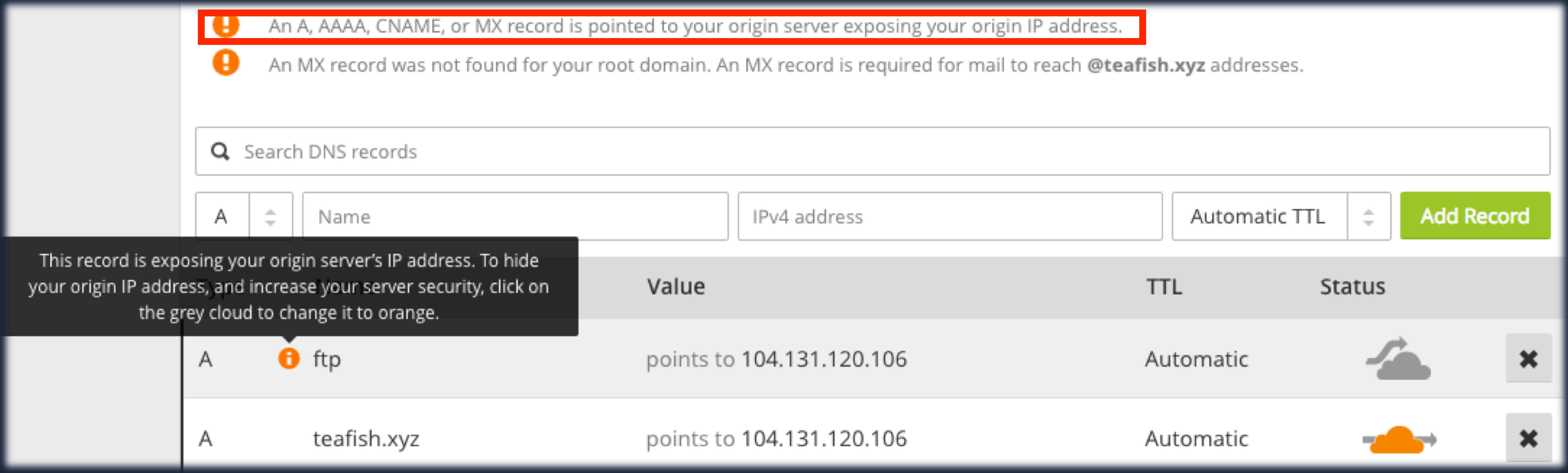
BEFORE



A	mycustomdomain.com	points to **74.117.117.121**	Automatic
A	direct	points to **74.117.117.121**	Automatic

We added a subdomain that allows you to access your server directly without passing through the CloudFlare network. You should use this domain to access services like SSH, FTP, and Telnet. You can change the default name of the subdomain to something other than **direct** for enhanced security.

AFTER



An A, AAAA, CNAME, or MX record is pointed to your origin server exposing your origin IP address.

An MX record was not found for your root domain. An MX record is required for mail to reach **@teafish.xyz** addresses.

This record is exposing your origin server's IP address. To hide your origin IP address, and increase your server security, click on the grey cloud to change it to orange.

		Value	TTL	Status
A	ftp	points to 104.131.120.106	Automatic	
A	teafish.xyz	points to 104.131.120.106	Automatic	

Source: cloudflare.com

PREVENTION

PREVENTING ORIGIN EXPOSURE

- Request “fresh” IP address when activating cloud-based security

  Protects you from historical knowledge attacks

- Block all non-CBSP requests with your firewall

  Prevents origin verification and web applications attacks

- Choose a CBSP that assigns a dedicated IP address to you

  One-to-one port forwarding solves the non-web protocol limitation

- Use cloudpiercer.org to scan your website

  Tests all discussed vulnerabilities

DDoS Attacks: Solutions and Pitfalls

Thomas Vissers

SecAppDev, Leuven (Mar 3, 2017)