CLOUDPIERCER

BYPASSING CLOUD-BASED SECURITY PROVIDERS

AGENDA

CLOUD SECURITY

What is cloud-based security?

VULNERABILITIES

How can cloud security be bypassed?

DEFENSES

How can we prevent these vulnerabilities?

ONLINE TOOL

Discover our online tool to scan for vulnerabilities

CLOUD SECURITY

What are cloud-based security providers (CBSPs)?

CLOUD-BASED SECURITY

DDoS attacks

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

    Volumetric attacks

    Application-level attacks

- Classic on-premises security devices are usually ineffective

    Network connections saturate

- Attacks become ever larger and more common

CLOUD-BASED SECURITY PROVIDERS

DDoS attacks – *Larger*

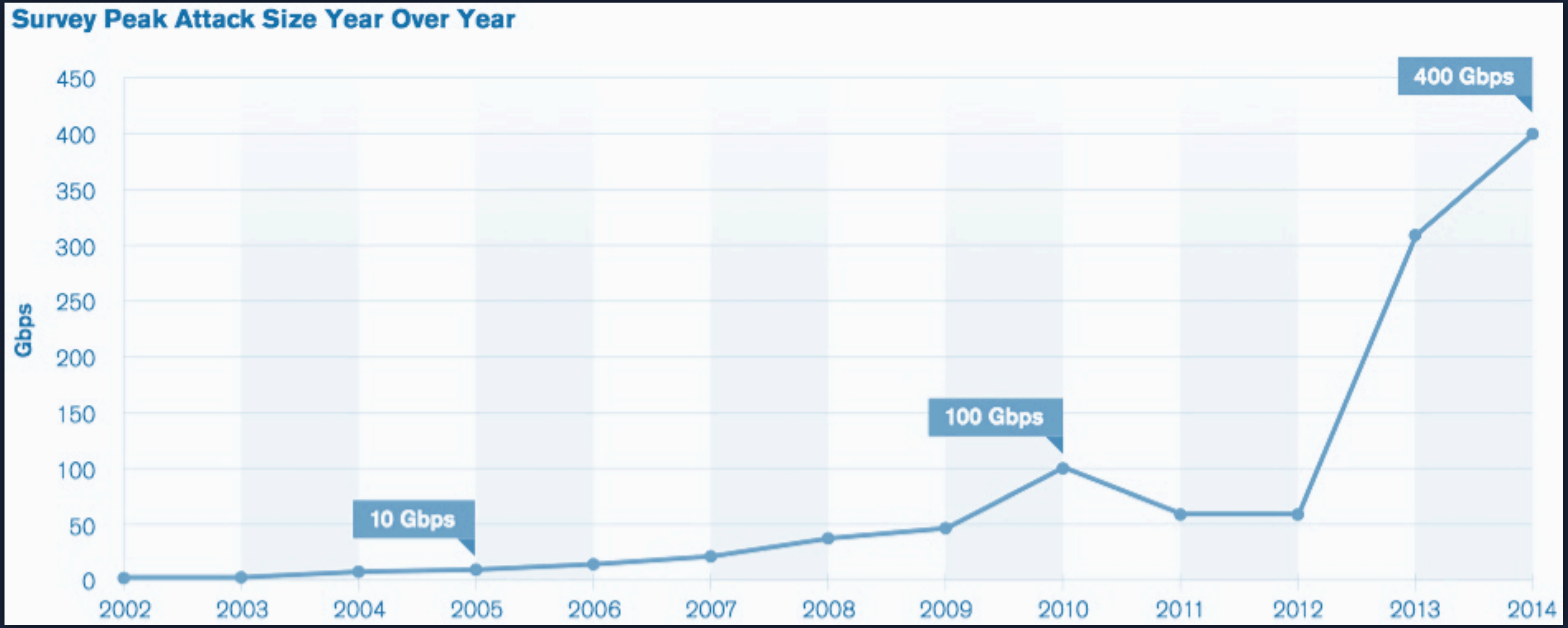


Image from Arbor Networks

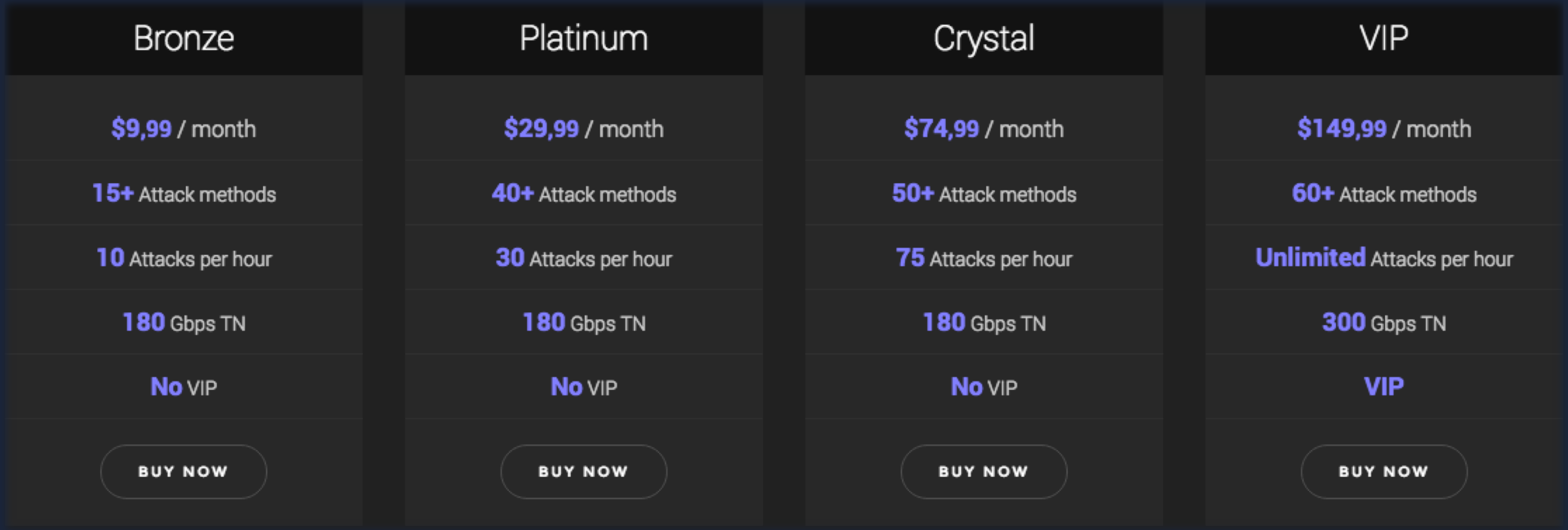
CLOUD-BASED SECURITY PROVIDERS

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)



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

Image from Arbor Networks

Also about… Web application attacks

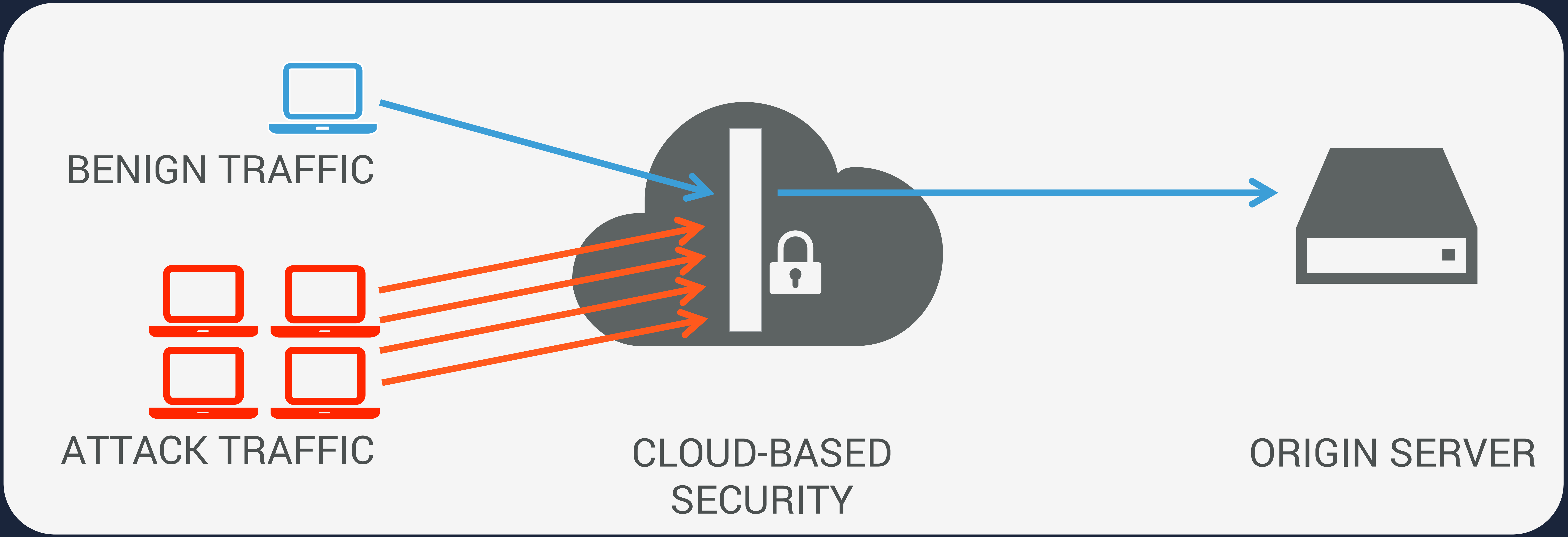
- SQL injections, XSS, …

  OWASP TOP10

- WAF: Often rules and signatures are used to detect attacks

  Distinguishing between benign and malicious web request is a complex and delicate process

CLOUD-BASED SECURITY



CBSPs reroute and filter the customers' traffic through their cloud

> CBSP forwards clean traffic to customer's server

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

- Other types

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

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 security was a $4.5 Billion market in 2015 – by 2020, $12 billion market

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

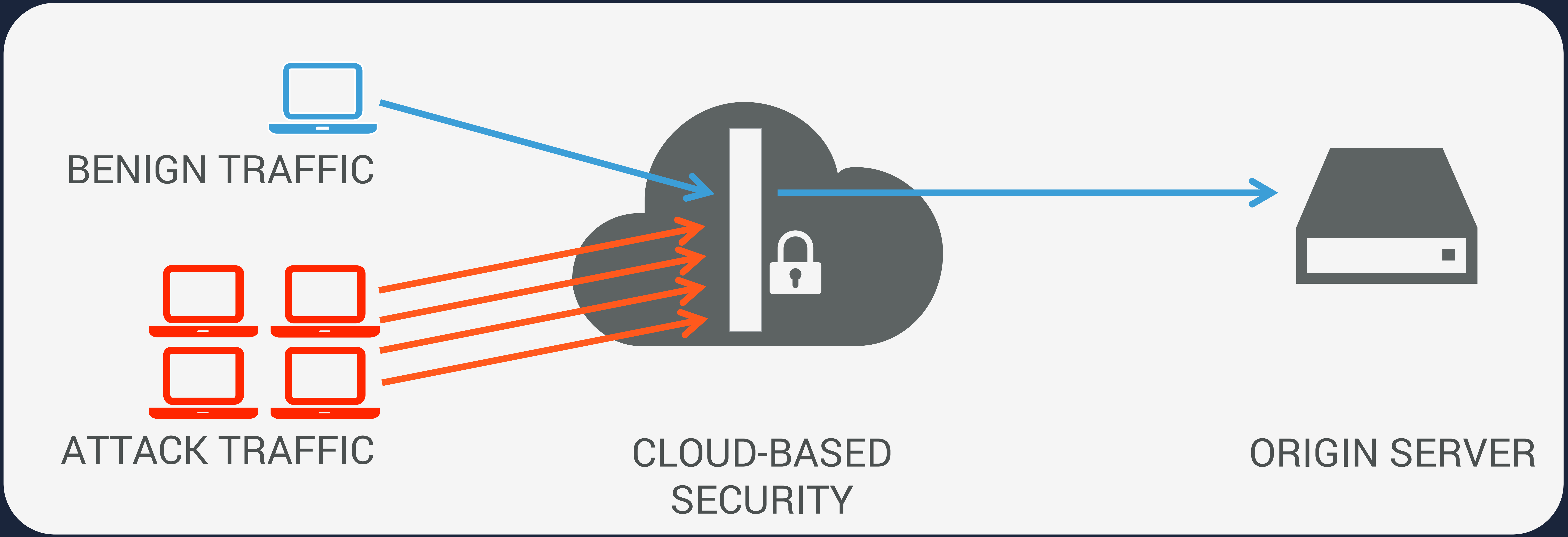
  > No expertise needed

  > Quick and easy installation (change DNS records)

  > Low cost (sometimes free)

CLOUDFLARE
DOS arrest
Internet security
sucuri
Incapsula
Akamai
PROLEXIC

CLOUD-BASED SECURITY PITFALL

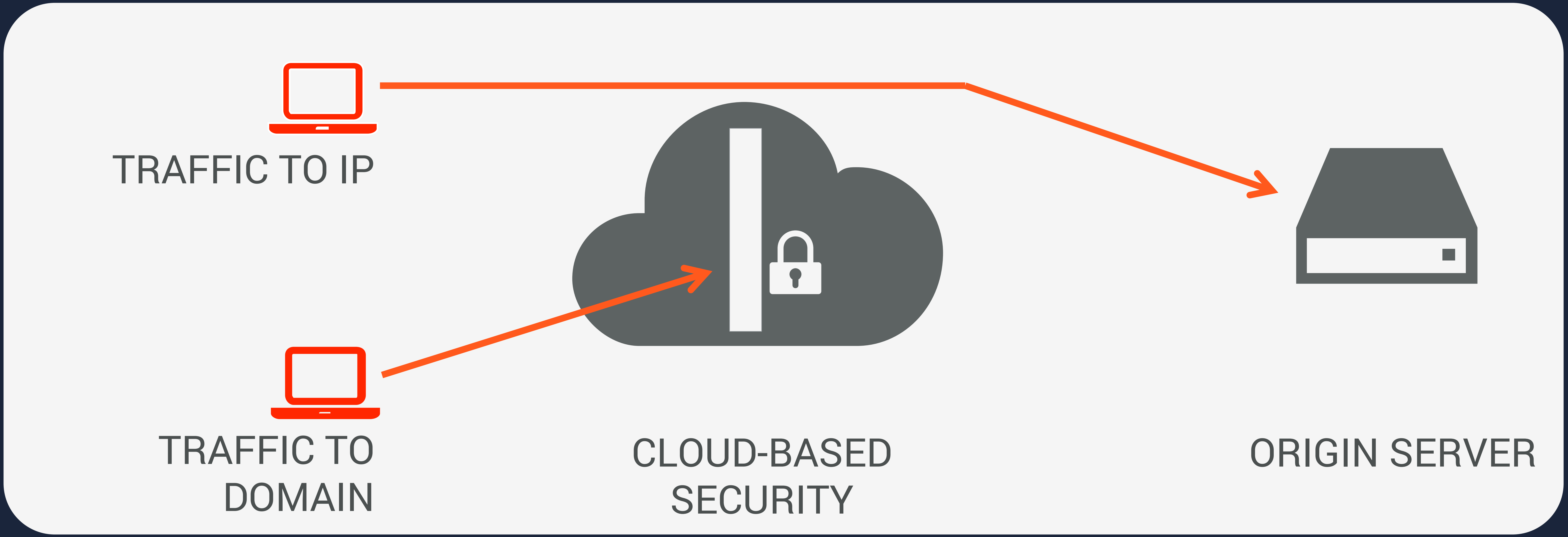


CBSPs reroute and filter the customers’ traffic through their cloud

> *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

VULNERABILITIES

How can the server's IP address be exposed ?

VULNERABILITY 1: SUBDOMAINS

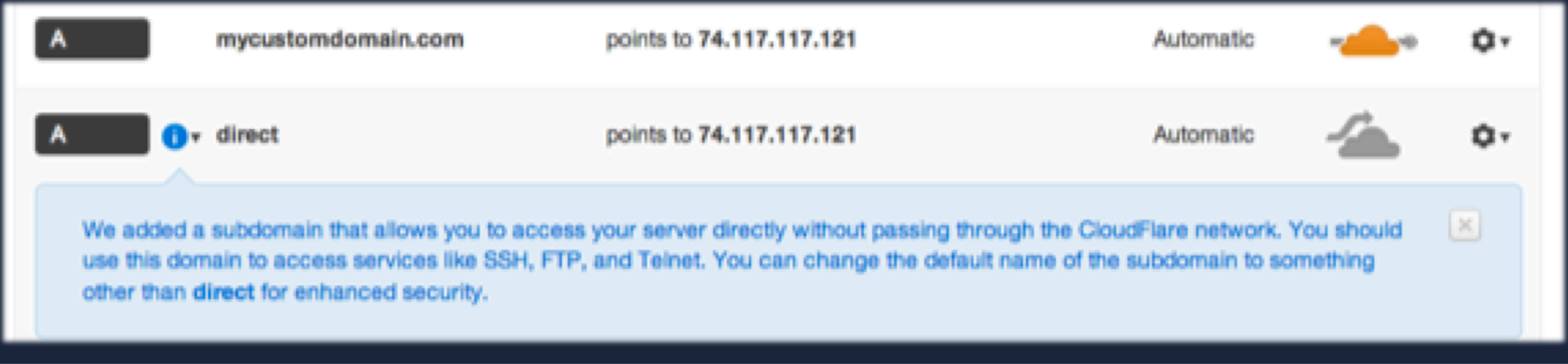
- CBSPs rely on HTTP “*Host”* header to forward requests

  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.

VULNERABILITY 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)
…	

VULNERABILITY 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.

VULNERABILITY 2: DNS RECORDS

Our findings

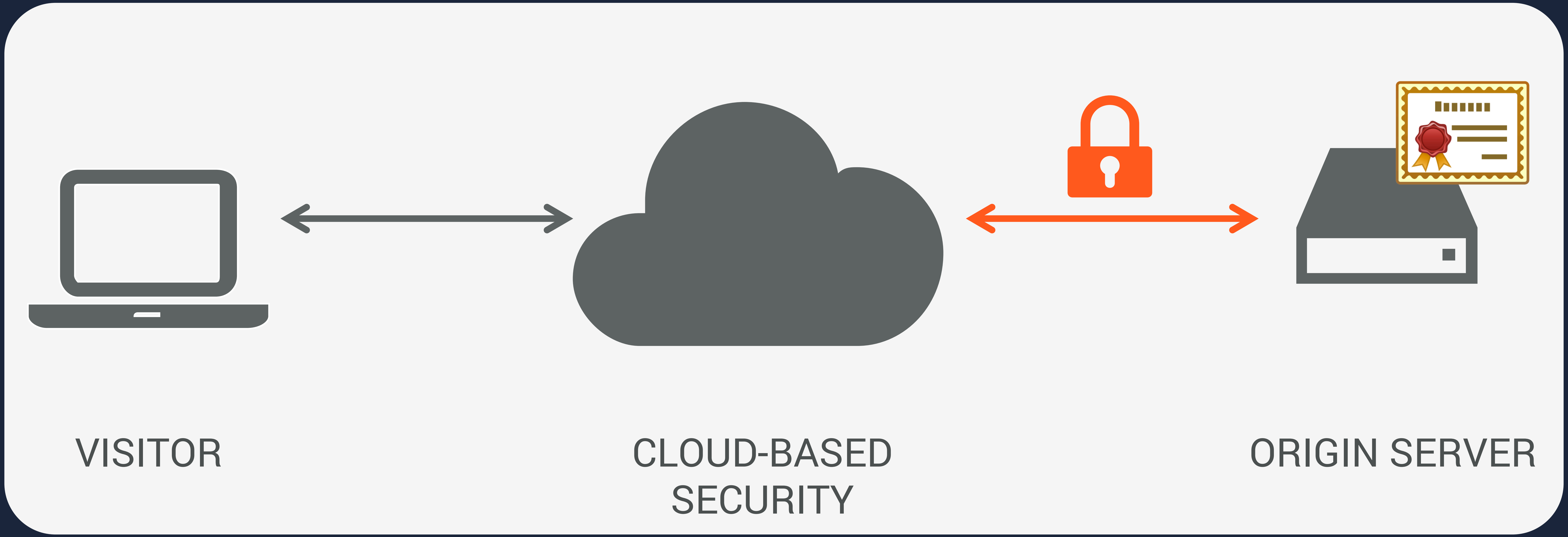
- Queried all DNS RR types for every domain

  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	

VULNERABILITY 3: SSL CERTIFICATES



- HTTPS connection between CBSP and origin

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

VULNERABILITY 3: SSL CERTIFICATES

Our findings

- Harvest certificates from all IP addresses

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

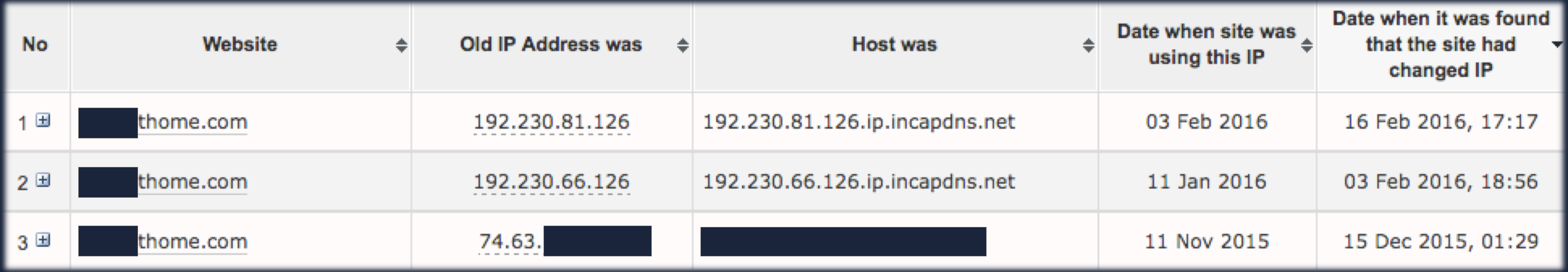
  Censys.io: a new search engine for this data.

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

VULNERABILITY 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

VULNERABILITY 4: IP HISTORY

Our findings

- We queried these IP History databases

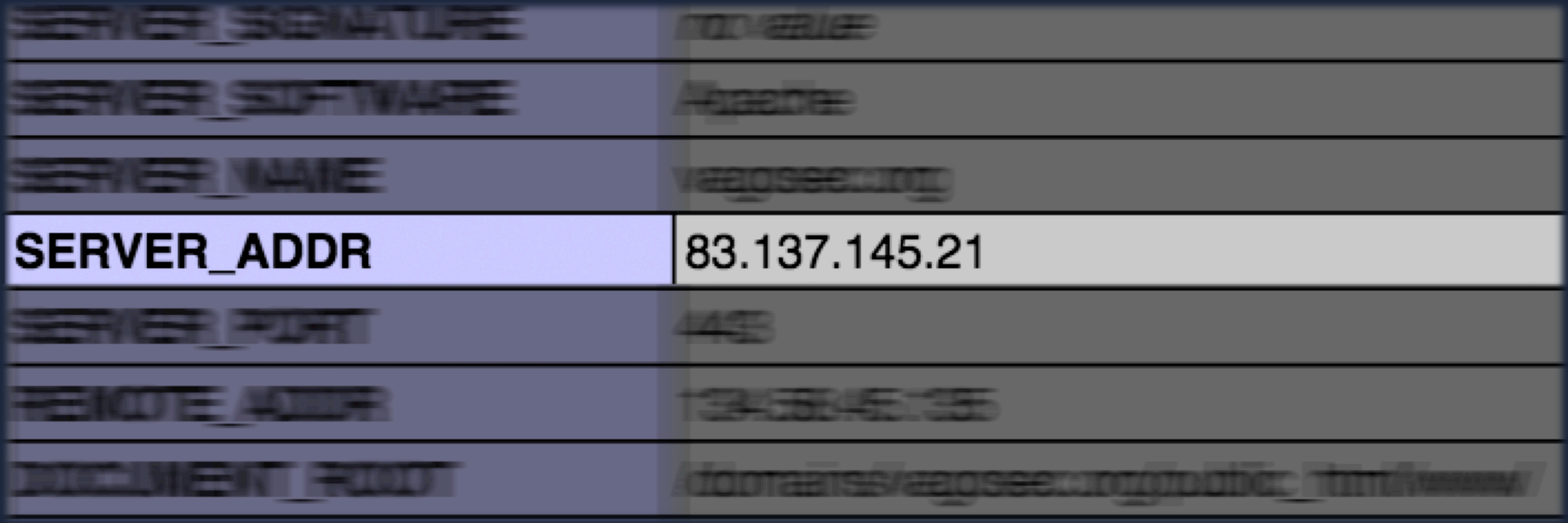
  We verified each listed historic IP address for all domains.

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

VULNERABILITY 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]

VULNERABILITY 5: SENSITIVE FILES

Our findings

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

  /info.php

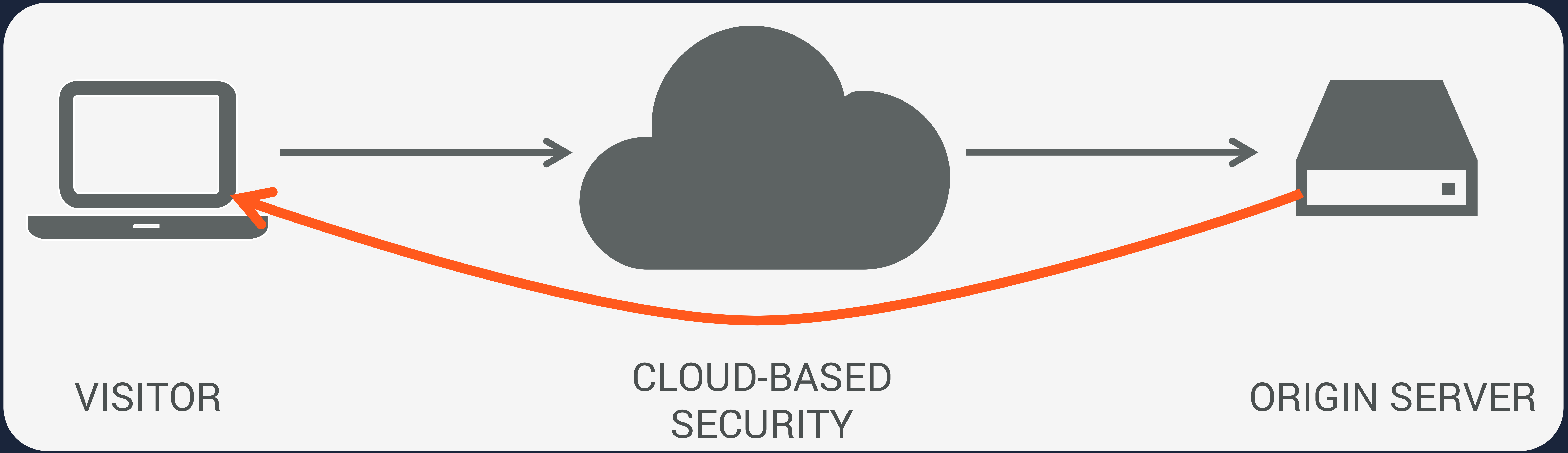
  /phpinfo.php

  /test.php

  /phpMyAdmin/phpinfo.php

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

VULNERABILITY 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.

VULNERABILITY 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

REMAINING VULNERABILITIES

- Temporary exposure

  4% vulnerable

- Origin IP address in Content

  1% vulnerable

ORIGIN-EXPOSING VULNERABILITIES (1)

MOST COMMON

SUBDOMAINS

In order not to break some protocols, several websites configured subdomains that resolve directly to the origin

43%

DNS RECORDS

Domains still reveal their web server's IP address through MX, SPF and other DNS records.

27%

SENSITIVE FILES

Administrators often forget to restrict access to development or log files which expose sensitive information such as the server's IP address.

5%

MOST COMMON

IP HISTORY

A website's IP address can be listed in databases that keep track of historical DNS data.

41%

ORIGIN-EXPOSING VULNERABILITIES (2)

CERTIFICATES

Internet-wide scanners can find the servers that present SSL certificates for the website's domain name.

9%

OUTBOUND CONNECTION

For example, PingBack's verification mechanism can be leveraged to trigger an outbound connection from your website's origin, revealing its origin to the recipient.

7%

ORIGIN IN CONTENT

The domain's origin IP address can be written in the HTML content of the website

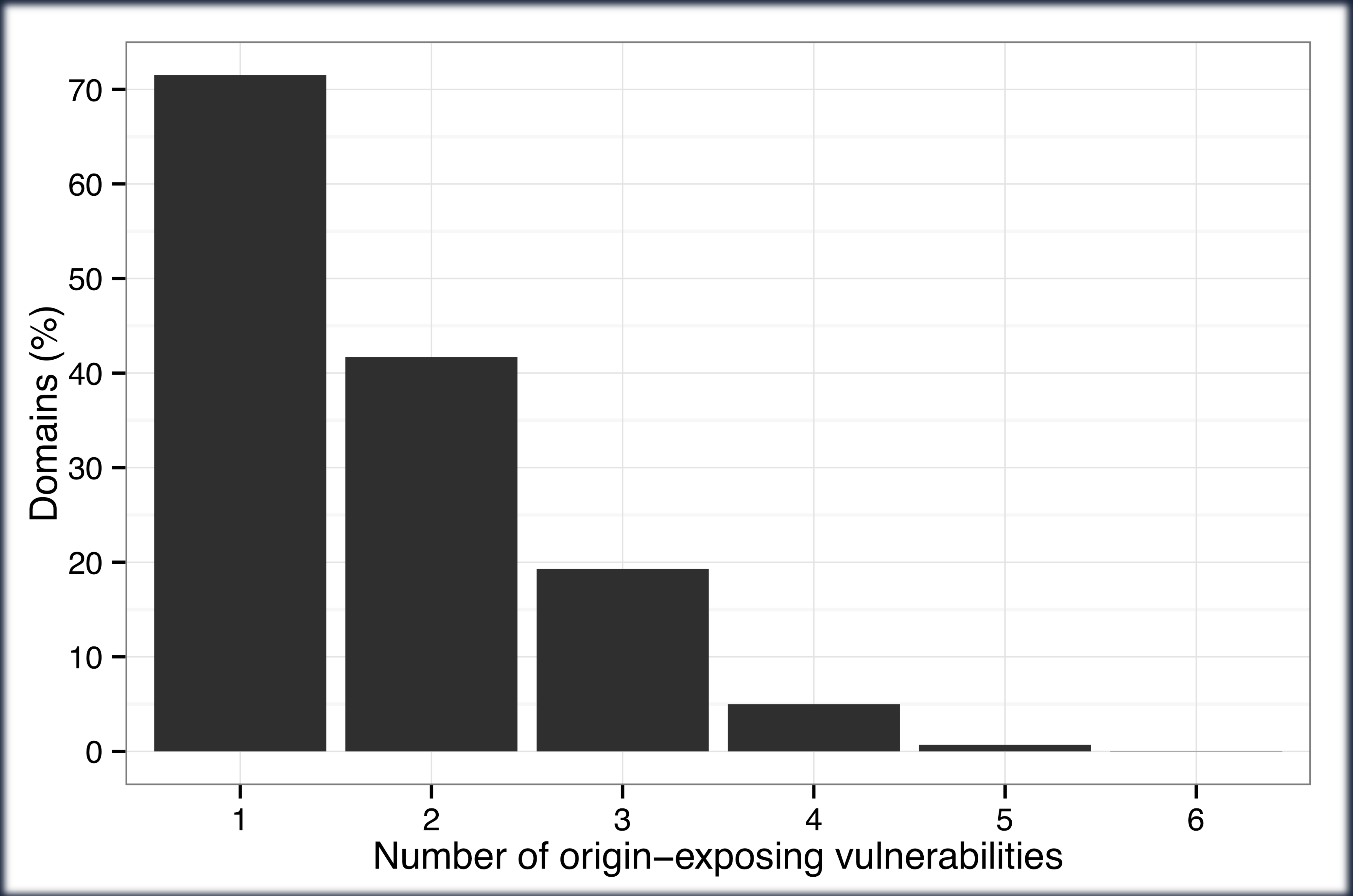
1%

TEMPORARY EXPOSURE

Administrator temporarily bypassed the cloud protection.

4%

"HOW MANY DO YOU HAVE?"



DEFENSES

How can I prevent my origin IP address from leaking?

PREVENTING ORIGIN EXPOSURE

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

  Protects you from historic 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

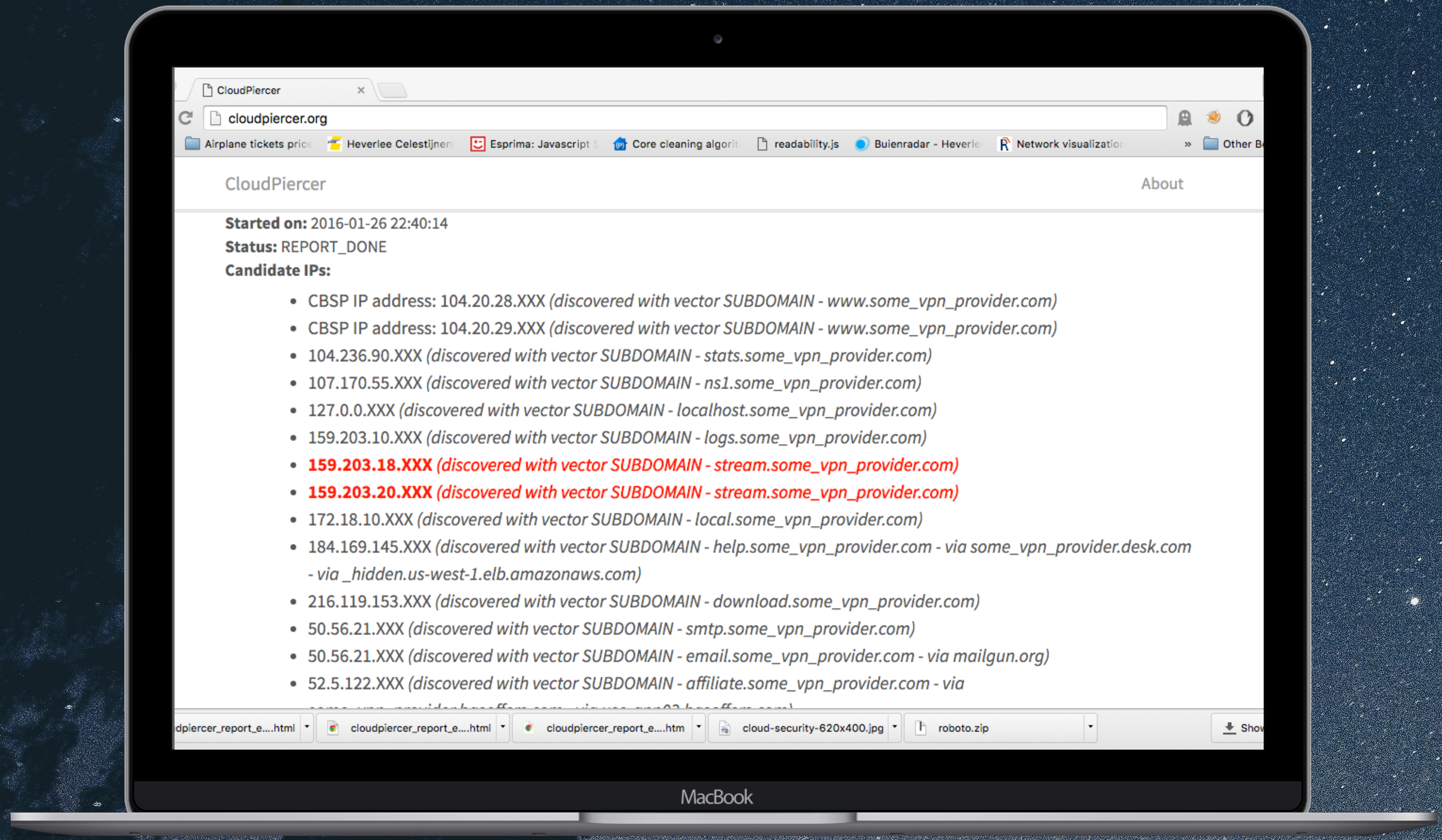
- ⚡ Use cloudpiercer.org to scan your website

  Tests all discussed vulnerabilities

ONLINE TOOL

Discover our online tool to scan for vulnerabilities

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

CloudPiercer is made available online at https://cloudpiercer.org.
We hope that the community will benefit from this service by allowing administrators to discover and eliminate vulnerabilities on their websites, before they are discovered by attackers.

IMPACT

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

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

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

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

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

Fear of a Filled Pipe - The Origin Exposed

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

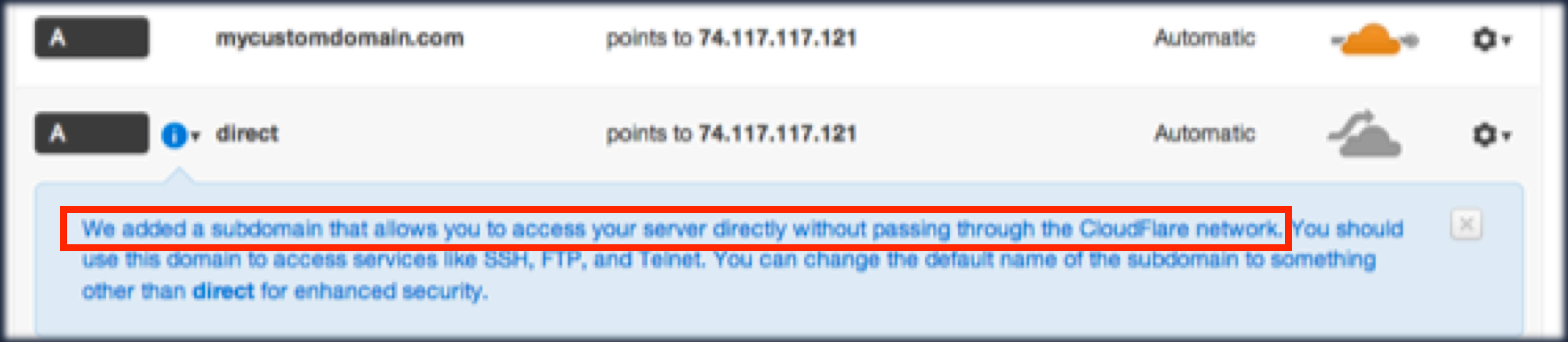
Volumetric attacks were the reason for the birth and growth of cloud based DDoS attack mitigation service providers. With the recent research rela
flaw in the current solutions has been uncovered. The paper linked here exposes critical weaknesses in the mechanisms for cloud-based DDoS att
weaknesses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

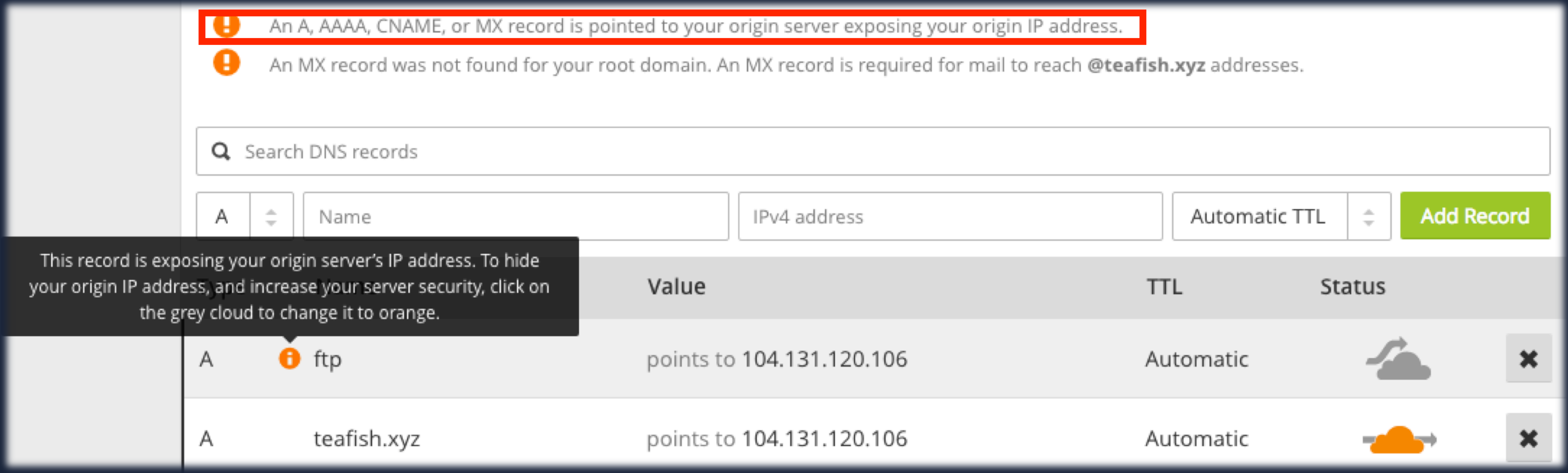
1. Attacks should be blocked closer to the source via a globally distributed network of mitigation nodes.

IMPACT



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.



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	

thomas.vissers@cs.kuleuven.be
cloudpiercer.org