DDoS is Coming

Tin Zaw

Director, Security Solutions
Verizon Digital Media Services

The following is based on a true story …

As an enterprise content delivery network provider, Verizon Digital Media Services helps its customers defend cyber attacks.

Although names have been withheld, the story in this presentation is based on our actual experience working with a customer to **mitigate a Bitcoin-DDoS extortion attempt**.

We deal with these types of attacks everyday.

The Rise of Cyber Extortion

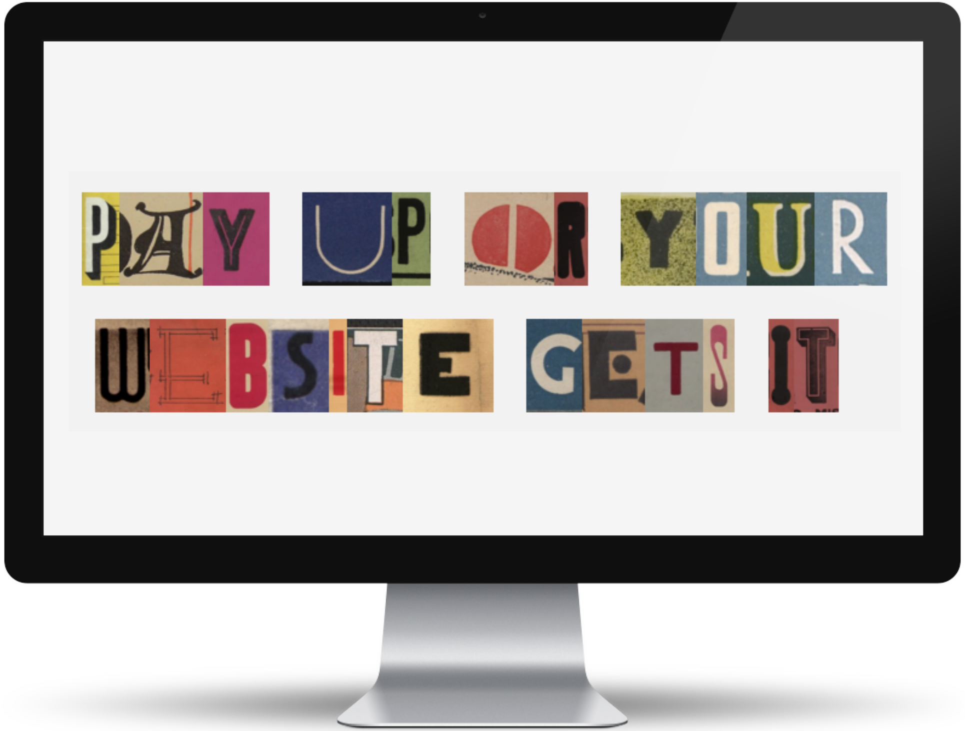
In recent years, there has been an emergence of cybercriminal groups that threaten their targets with massive DDoS attacks unless they are paid a hefty Bitcoin ransom.

If left unaddressed, these attacks can disrupt business practices, damage branding and cause financial loss.

Day 1

It's the holiday season in 2015. The busiest shopping season of the year.

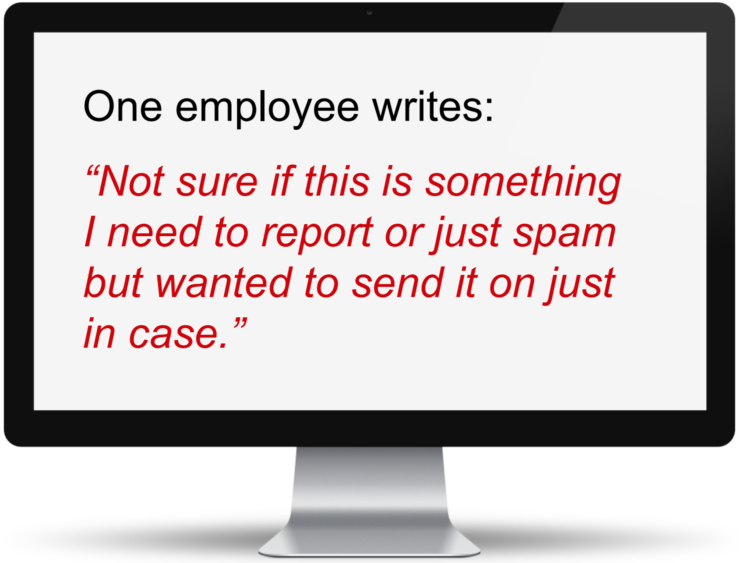
A few ACME Corp employees receive a strange email.



verizon✓

Skeptical, they forward the email up the chain of command.

- Not knowing if the email is just a hoax or legitimate threat, the ACME employees forward it on.
- It eventually makes its way up to the CSO, and catches his attention.



One employee writes:

“Not sure if this is something I need to report or just spam but wanted to send it on just in case.”

Elements of the e-mail: We’ve seen this more and more.

Elements
Comes from a location that doesn’t work well with U.S. authorities
Asks recipient to forward the email → attackers don’t know the decision makers, so they spam many people
Tries to establish credibility in some way
Requests payment in Bitcoins (very hard to trace)
Includes bold claims of attack abilities
Surges pricing
Will attack all IP addresses
Allows some time to provide payment

Day 2

Verizon, we have a problem.

Fortunately, ACME is a subscriber to Verizon Digital Media Services' Security Service

verizon✓

ACME requested a call with our Security Professional Services team:

- Customer asked that we have our security professionals on the call.
- We had the full team present, including a Technical Account Manager and a Security Solution Architect.
- ACME had its information security manager and its web operations team present.

Step 1: Analyze the Vulnerabilities

- **The “proof of concept attack” never came and the log does not show an attack.**

Step 2: Red Alert! All hands to battle station ...

Team	Alert
NOC	Our 24x7 Network Operations Center (NOC) team were notified and given context. Specialized contact and escalation were designed.
Dedicated Security Professionals	Constant and direct (emails and mobile) lines of communication were initiated with relevant customer teams.
Engineering	We checked capacity and hardware to prepare for attack.
Management	Our CTO and General Counsel were notified so they could make quick decisions.

Step 3: Putting a Plan in Place

Attack Source	Mitigation Strategy
Layer 3 and 4 Attack	Verizon's Edgecast Content Delivery Network (CDN) is accustomed to network layer attacks as part of running a CDN. • We created a **Proactive Ticket** with our 24 x 7 Network Operations Center to expect an attack. • We provided ACME origin IP to NOC enable a faster response to create more accurate signatures.
Layer 7 Attack	This has most potential for damage. • We activated more restrictive **Web Application Firewall** rules to minimize the attack surface. • We enabled more rules for alerts to create more visibility to possible attacks. • We increased the frequency of log reviews to detect attacks.
Unprotected Origin	No time to migrate to Verizon solution. • If attacked, ACME may take down origin to prevent layer 7 compromises, like SQL injection.

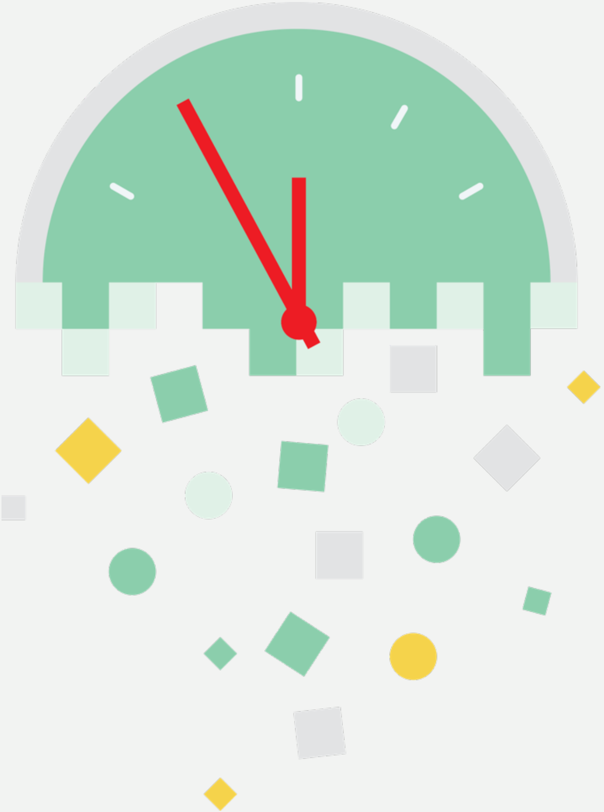
Step 4: Wait

Day 3

Major Attack Expected

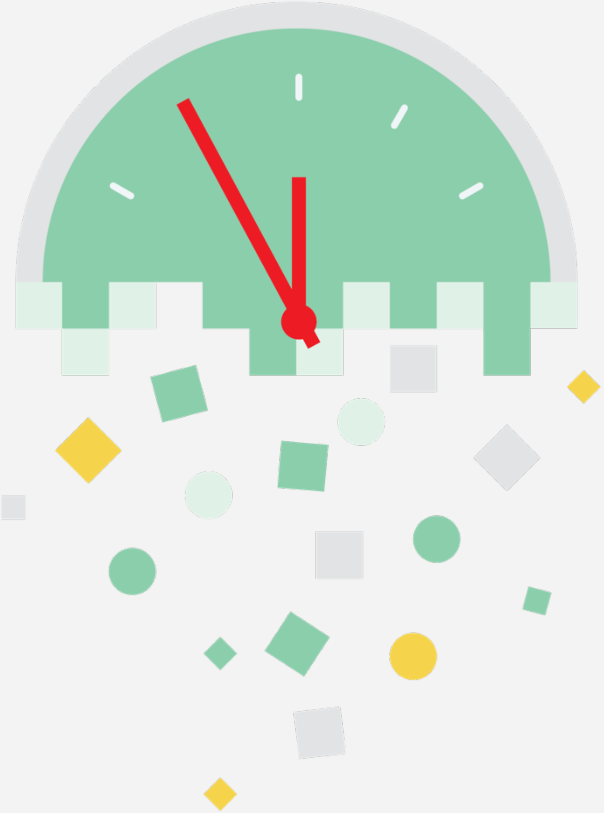
verizon✓

No Attack.
Nothing.



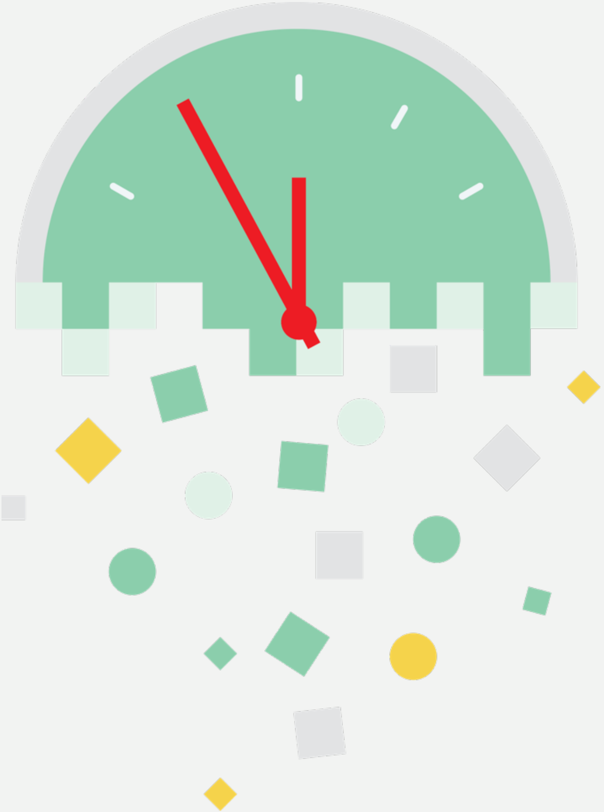
Day 4

No Attack. Nothing.



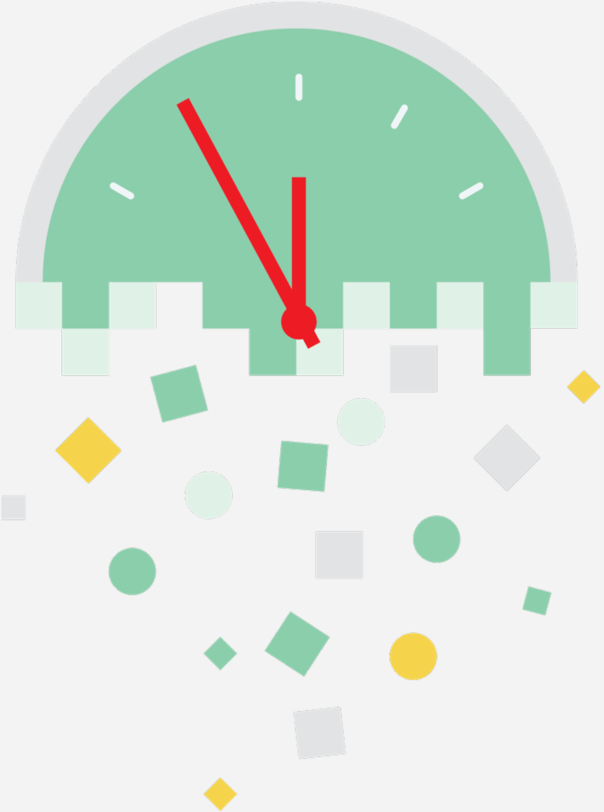
Day 5

No Attack. Nothing.



Day 6

No Attack.
Nothing.



WHY YOU NO ATTACK
imgflip.com

Day 7

6:40 a.m.: DoS is Here

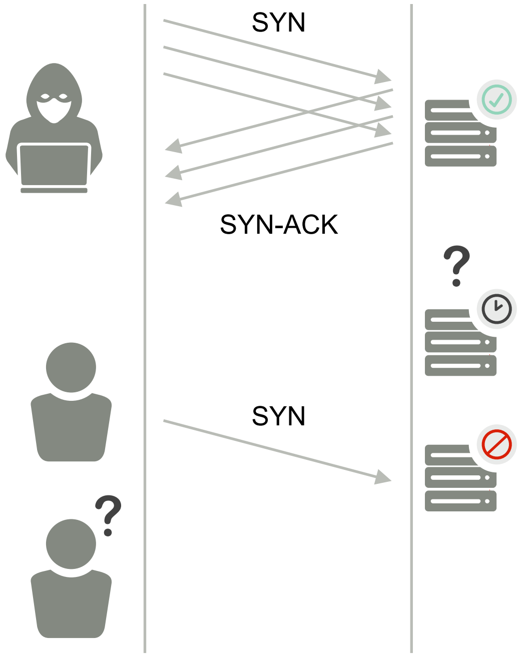
Verizon detects the attack (SYN Flood), which peaks at 80Gbps.

Attack Type: SYN Floods

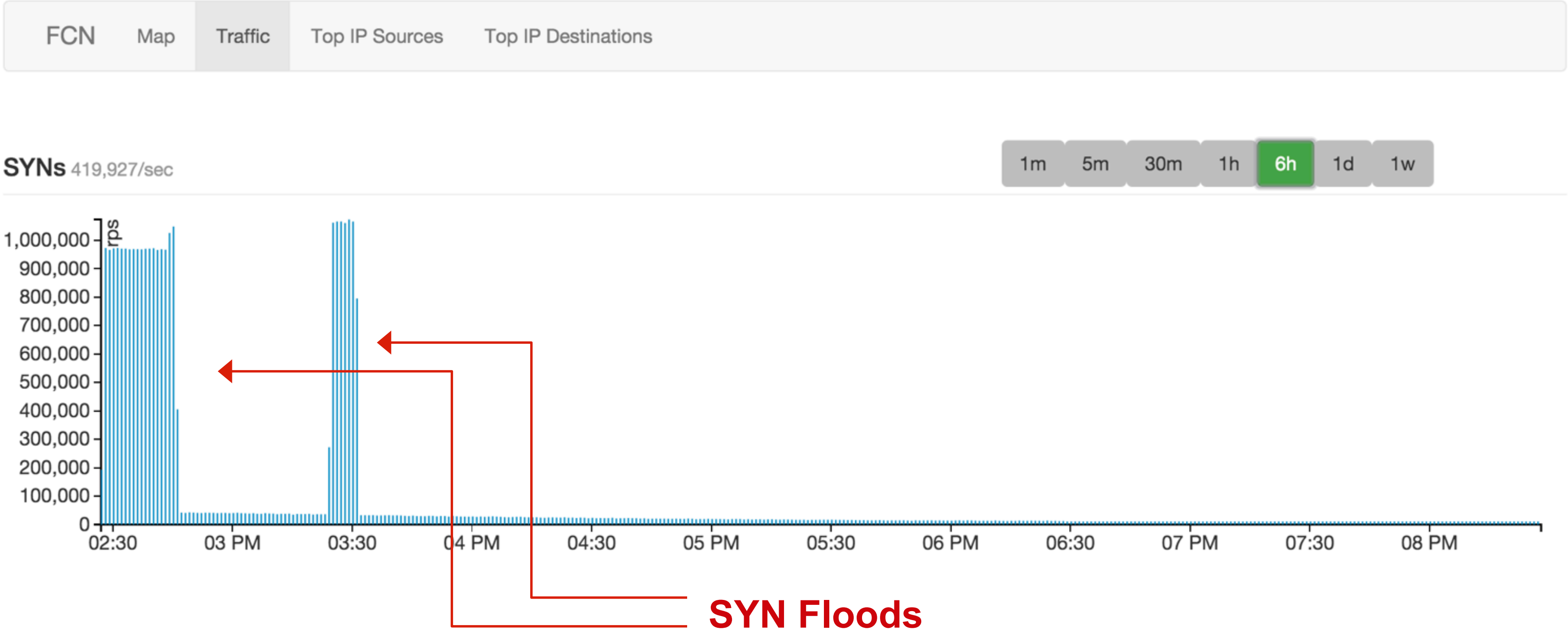
- SYN Floods are a common form of DDoS.

- Attackers send a flood of fake server connection requests to their target's system in order to overload the target's servers and render the target unresponsive and unable to process legitimate requests.

- SYN Floods are considered L4 (Transport Layer) attacks.



What a SYN Flood Looks Like



SYNs 419,927/sec

SYN Floods

Mitigated in Minutes

Verizon immediately reacts with countermeasures and the attack is blocked at the edge.

Really!

Secure by Design

IP Anycast

Verizon’s Edgecast Content Delivery Network uses IP Anycast (where would the DDoS packet go?)

Super PoPs with Massive Capacity

We place high-capacity PoPs in strategic global locations to handle massive surges in demand or attacks; 20 Tbps of global capacity and 95+ Super PoPs.

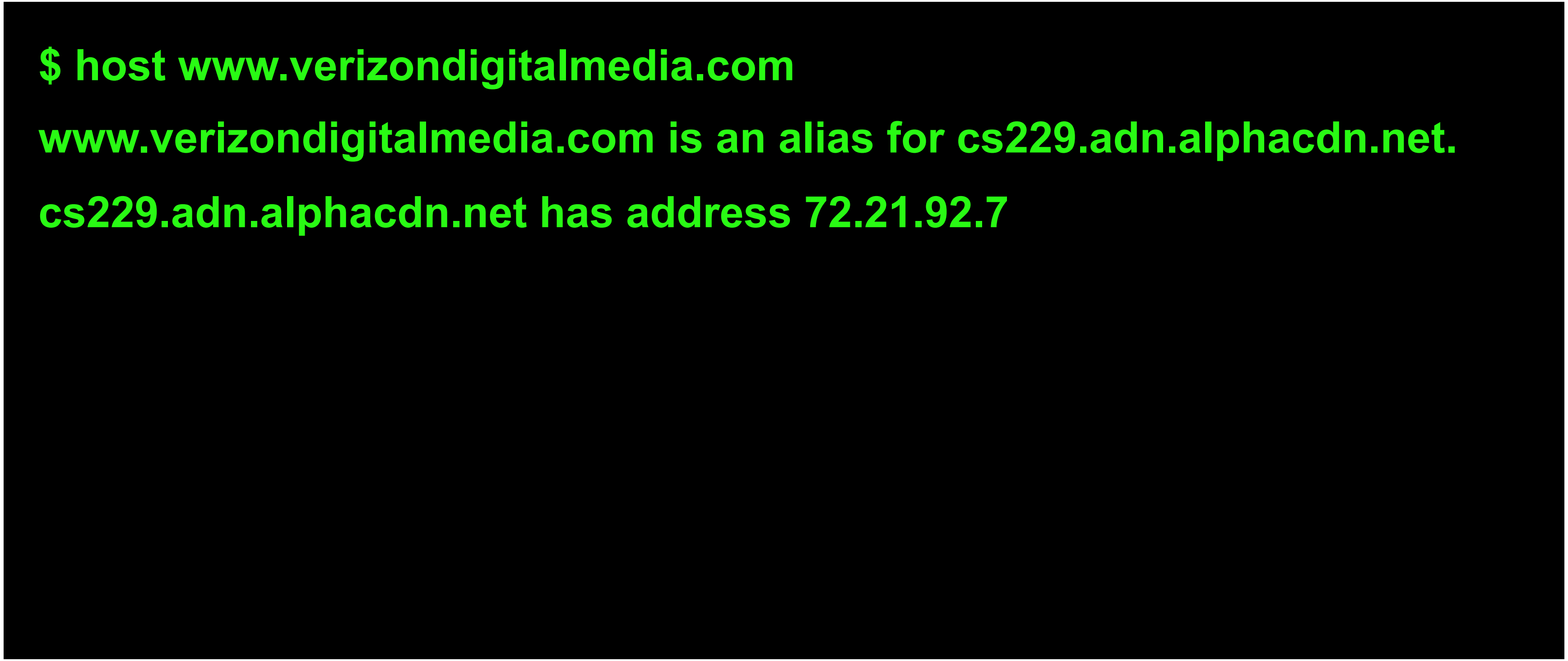
Network Attack Mitigation

We have proprietary network attack detection and a response system codenamed *Stonefish*.

Web Application Firewall

It has powerful protection, threat detection and virtual patching with over 2,000 rules.

Anycast CDN 101



```
$ host www.verizondigitalmedia.com
www.verizondigitalmedia.com is an alias for cs229.adn.alphacdn.net.
cs229.adn.alphacdn.net has address 72.21.92.7
```

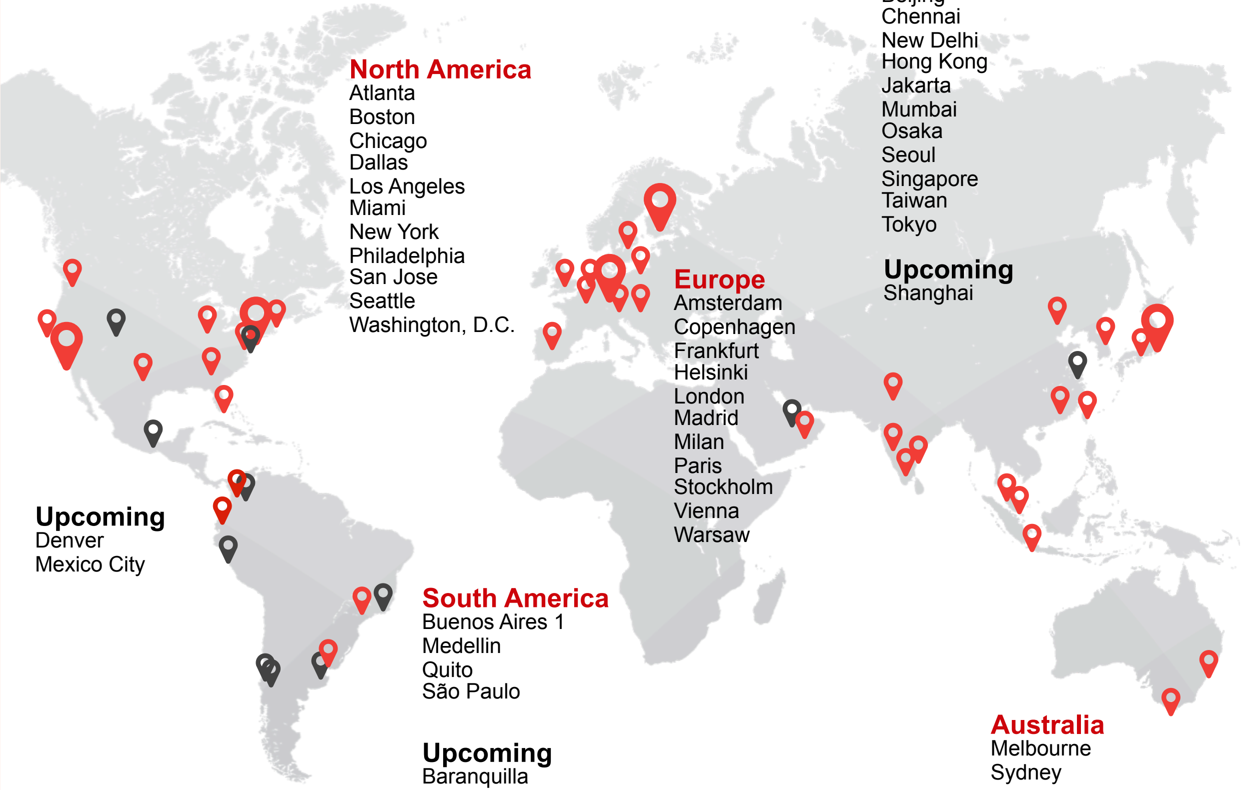
Our Network

20 Tbps
Network Capacity

95+
PoPs

5
Continents

3,000+
Interconnects



North America
Atlanta
Boston
Chicago
Dallas
Los Angeles
Miami
New York
Philadelphia
San Jose
Seattle
Washington, D.C.

Upcoming
Denver
Mexico City

South America
Buenos Aires 1
Medellin
Quito
São Paulo

Upcoming
Baranquilla
Buenos Aires 2
Lima
Rio de Janeiro
Santiago

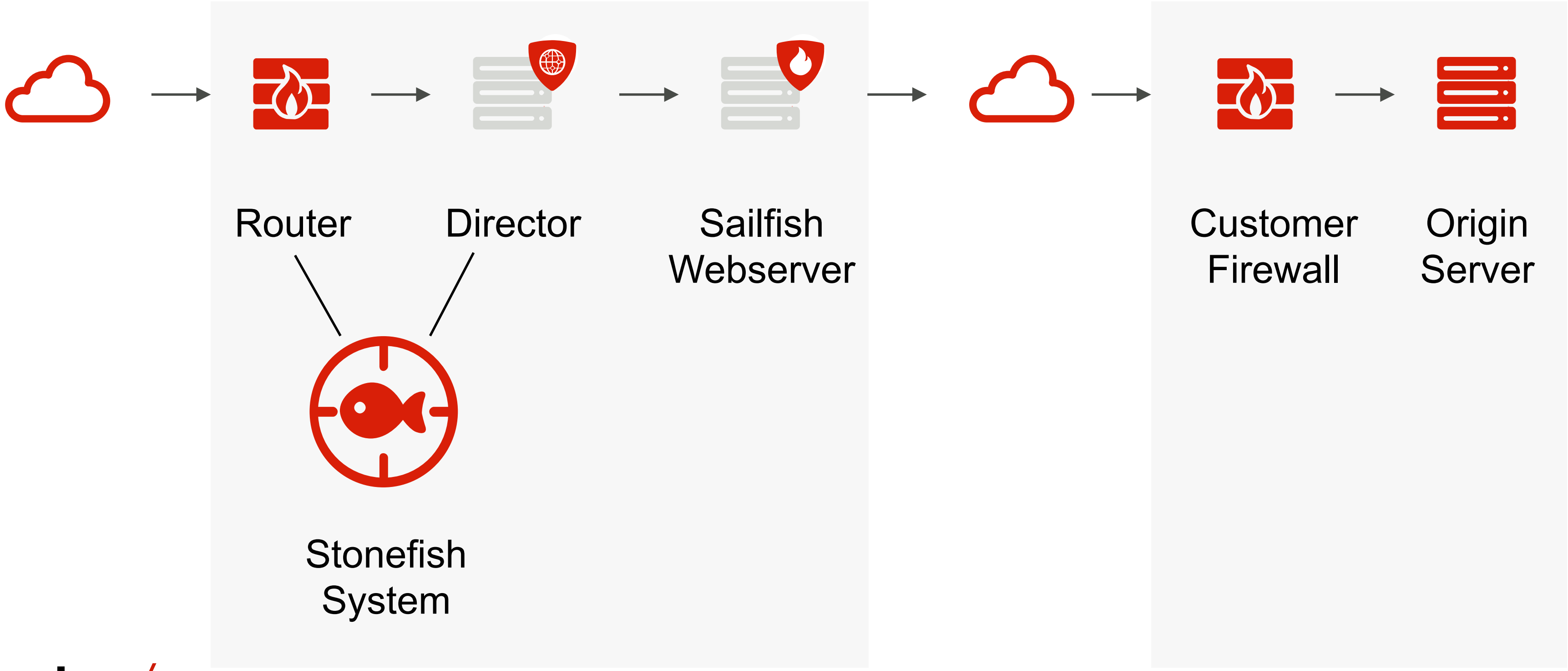
Europe
Amsterdam
Copenhagen
Frankfurt
Helsinki
London
Madrid
Milan
Paris
Stockholm
Vienna
Warsaw

Asia
Bangalore
Batam
Beijing
Chennai
New Delhi
Hong Kong
Jakarta
Mumbai
Osaka
Seoul
Singapore
Taiwan
Tokyo

Upcoming
Shanghai

Australia
Melbourne
Sydney

Layered Defense



Router

Director

Sailfish Webserver

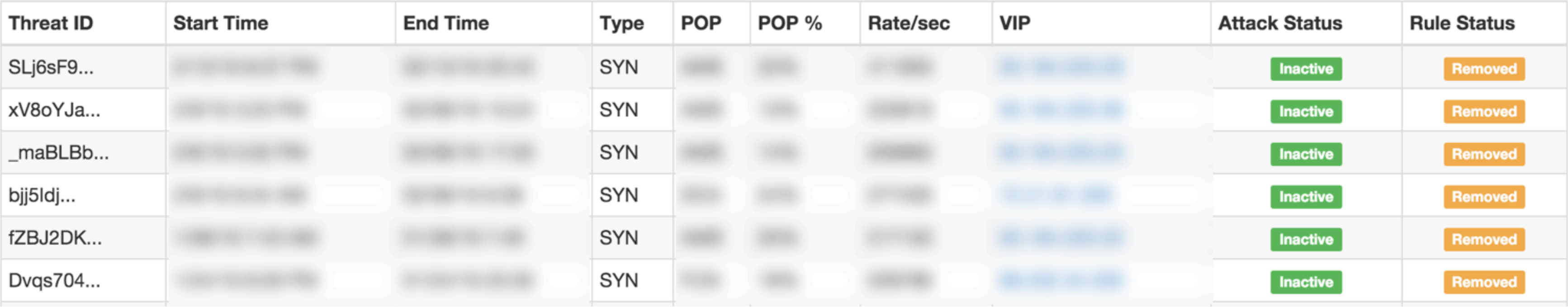
Stonefish System

Customer Firewall

Origin Server

Countermeasures

Verizon immediately identifies the attack signature and creates rules to block malicious traffic. This effectively thwarts the attack.



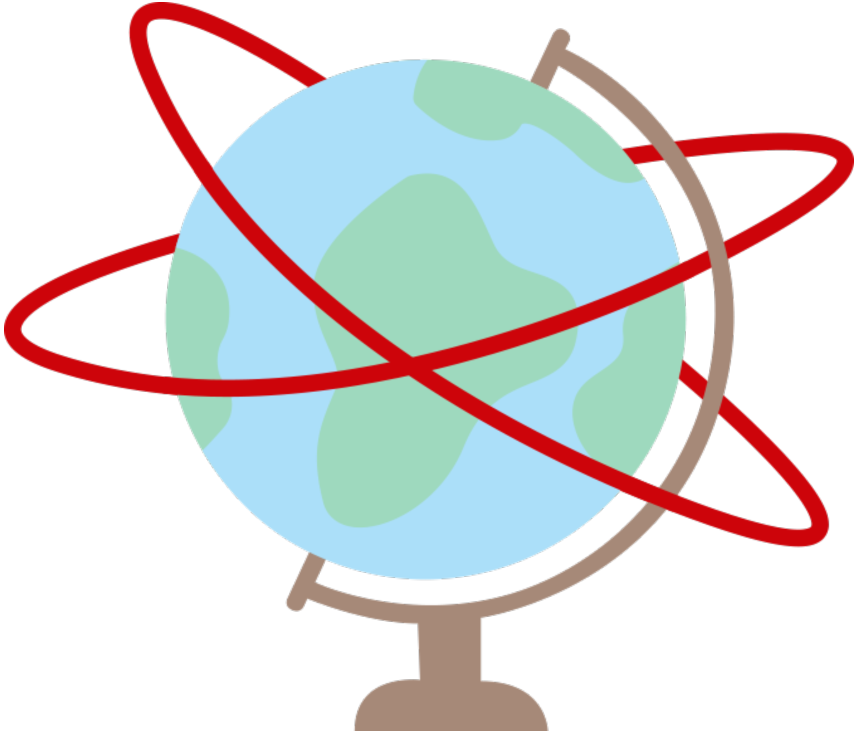
Threat ID	Start Time	End Time	Type	POP	POP %	Rate/sec	VIP	Attack Status	Rule Status
SLj6sF9...	[redacted]	[redacted]	SYN	[redacted]	[redacted]	[redacted]	[redacted]	Inactive	Removed
xV8oYJa...	[redacted]	[redacted]	SYN	[redacted]	[redacted]	[redacted]	[redacted]	Inactive	Removed
_maBLBb...	[redacted]	[redacted]	SYN	[redacted]	[redacted]	[redacted]	[redacted]	Inactive	Removed
bjj5Idj...	[redacted]	[redacted]	SYN	[redacted]	[redacted]	[redacted]	[redacted]	Inactive	Removed
fZBJ2DK...	[redacted]	[redacted]	SYN	[redacted]	[redacted]	[redacted]	[redacted]	Inactive	Removed
Dvqs704...	[redacted]	[redacted]	SYN	[redacted]	[redacted]	[redacted]	[redacted]	Inactive	Removed

Staying Vigilant

- Despite thwarting the attack, Verizon stayed prepared for Round 2, in case the attackers tried a different approach.
- Other possible attack scenarios include a Layer 7 (Application) attack.
- We enabled restrictive rules and activated many alerts in anticipation.
- No Layer 7 observed.

Staying in Touch

We remained in communication with the customer throughout the attack.



verizon✓

Lessons Learned …

#1

Protect your origin IP: Apply Origin Cloaking.

#2

Don’t forget to protect apex domain: http://yourdomainnamehere.com

#3

You need a plan.

Does your employee know who to escalate to?
Do you know what your attack surface is?

#4

You need on-demand scalability and capacity.
Attacks won't happen on schedule; you need to have massive capacity on standby, globally.

#5

You need lots of bandwidth:

Average DDoS: 5.5Mbps or 2Mpps

Can your appliance handle that?

What is your DDoS breaking point?

#6

You need agile WAF.

How fast can your WAF change rules to create customized defense?

#7

You need agile security service.
How fast can your vendor come to your aid?

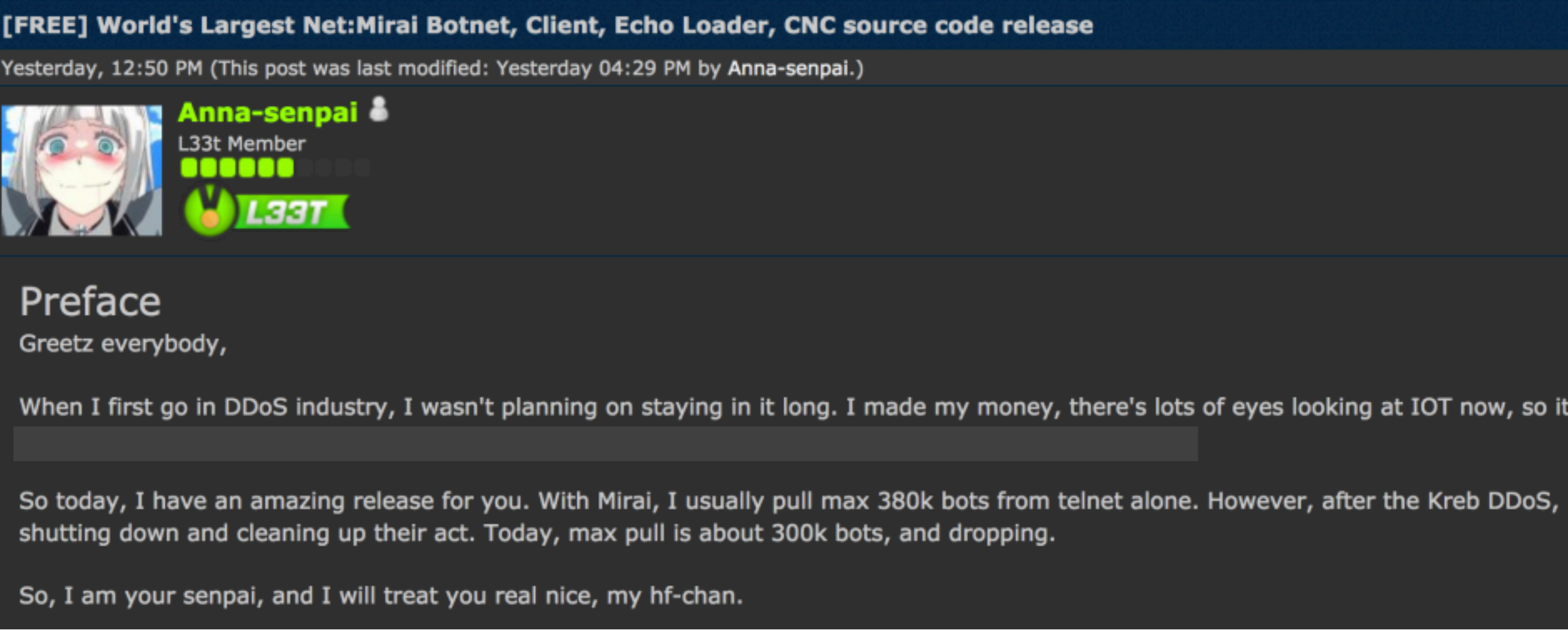
The Sequel

verizon✓

Armada Collective?

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

We are Armada Collective.

http://lmgtfy.com/?q=Armada+Collective

You will be DDoS-ed starting Thursday (April 21) if you don't pay protection fee -
20 Bitcoins @ 1KdDx

You will be DDoS-ed starting Thursday (April 21) if you don't pay protection fee -
20 Bitcoins @ 1HYak

You will be DDoS-ed starting Thursday (April 21) if you don't pay protection fee -
20 Bitcoins @ 15Zrn
```

Attacks never came.



[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)

Anna-senpai

L33t Member

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it

[redacted]

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS, shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

To be continued … ?

Thank you.

Tin Zaw
Director, Security Solutions
Verizon Digital Media Services

@tzaw | @verizondigital
www.verizondigitalmedia.com