RSAConference2016

Abu Dhabi | 15 – 16 November | Emirates Palace

SESSION ID: CCT-W06

DDoS Is Coming: A Story of DD4BC and the Copycat Squalls

Tin Zaw

Director, Security Solutions
Verizon Digital Media Services

@tzaw
@verizondigital

#RSAC

The following is based on a true story…

As an enterprise content delivery network provider, Verizon Digital Media Services helps its customers deal with security attacks on a regular basis.

The example that I'm going to present today is based on our actual experience working with a customer to **mitigate a Bitcoin-DDoS extortion attempt**. This is just one recent example, but I think it's worth noting that we deal with these types of attacks on a daily basis.

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

Day 1

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

Day 1

A few Company X employees receive a strange email.

PAY UP OR YOUR
WEBSITE GETS IT

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

- Not knowing if the email is just a hoax or a legitimate threat, Company X employees forward it on to senior level execs.
- 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 letter: We’ve seen this more and more.

Elements
Comes from a location that doesn’t work well with U.S. authorities
Asks recipients 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
Gives some time to get ready

Day 2

Verizon, we have a problem.

Company X had a call with Verizon team:

- Verizon: **Technical Account Manager** and a **Security Solution Architect**
- Company X: Information Security Manager and their WebOps Team

Step 1: Analyze the vulnerabilities

The “proof of concept attack” never came.

Some of the origin IPs were exposed.

HTTP Redirection from CompanyX.com to www.CompanyX.com.

Step 2: All hands to the battle station

Team	Alert
NOC	Our 24 x 7 Networking Operations Center (NOC) team were notified and given context. A specialized contact and escalation were designed.
Security Professionals	Constant and direct 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, if it became necessary to take more draconian measures.

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 Company X origin IP to NOC to enable a faster response to create more accurate signatures.
Layer 7 attack	This has the 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.

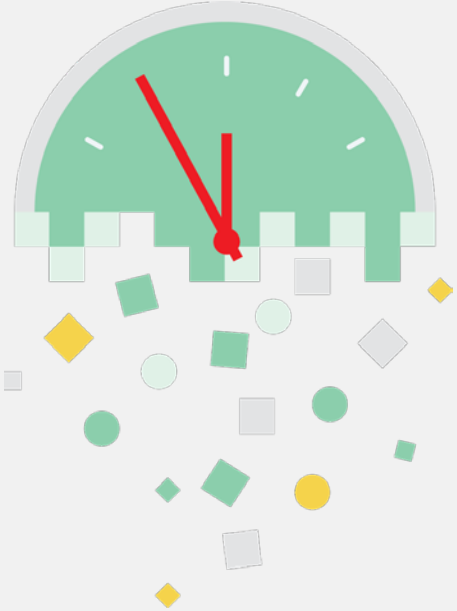
Step 4: Wait

Day 3

Major Attack Expected

Day 3

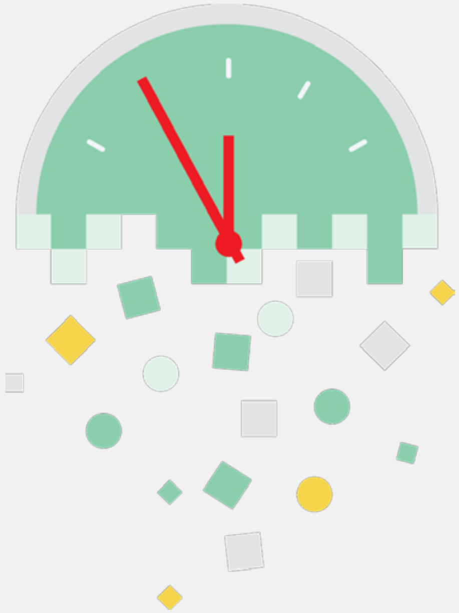
No Attack.
Nothing.



Day 4

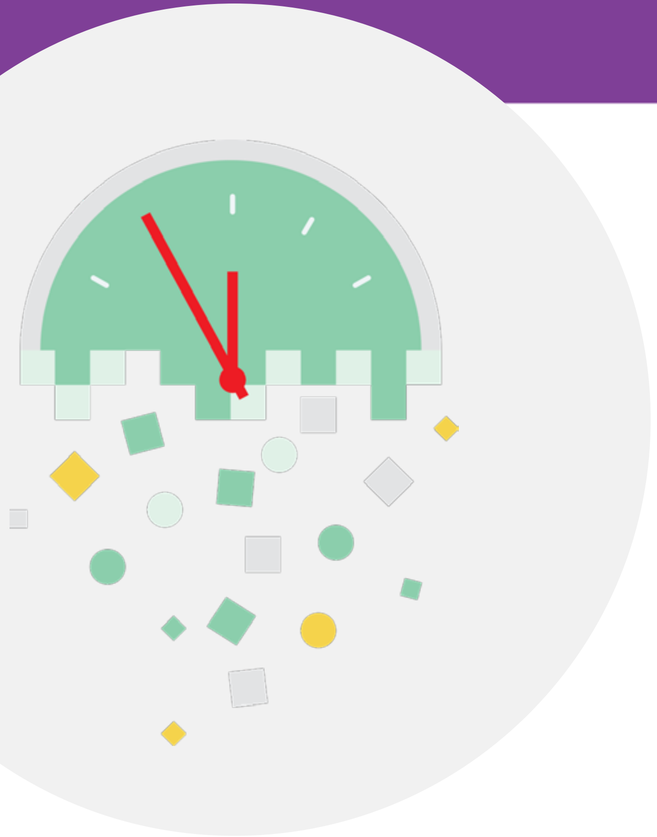
Day 4

No Attack.
Nothing.



Day 5

Day 5

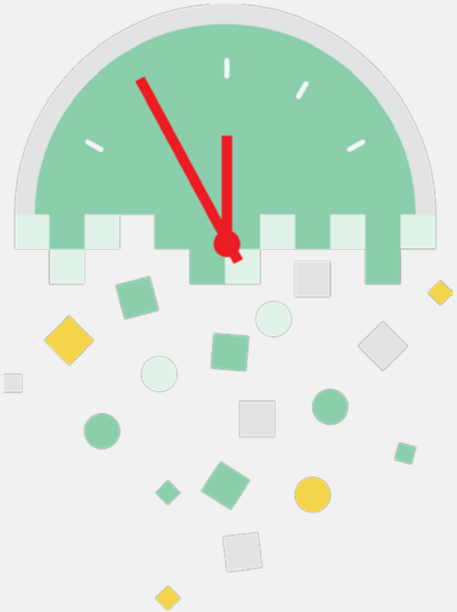


No Attack.
Nothing.

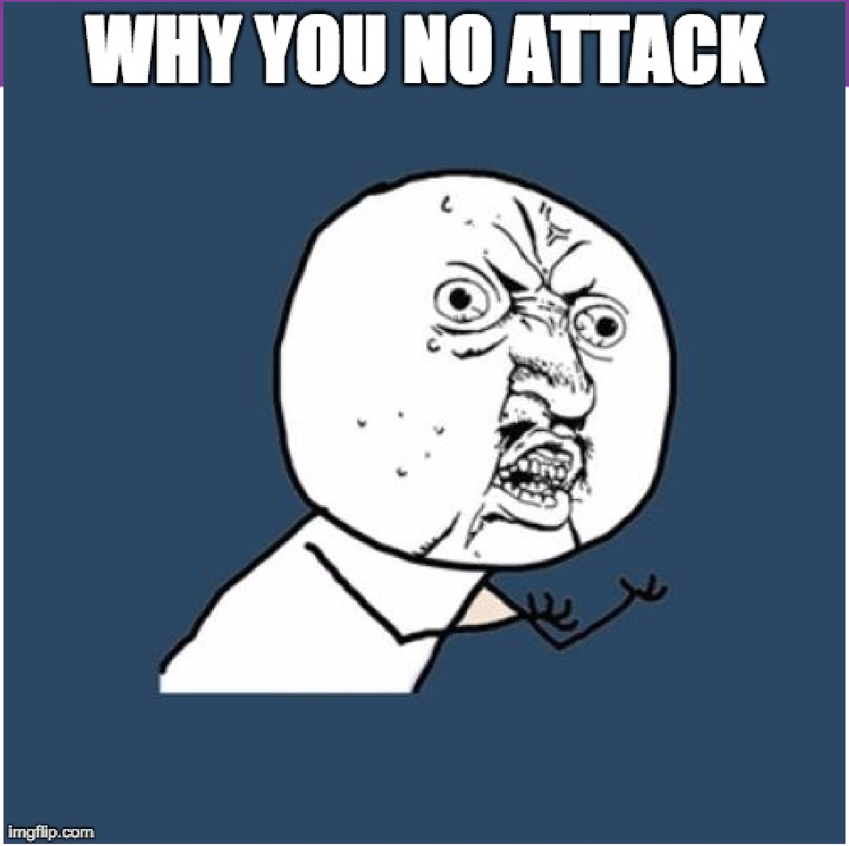
Day 6

Day 6

No Attack.
Nothing.



Day 6



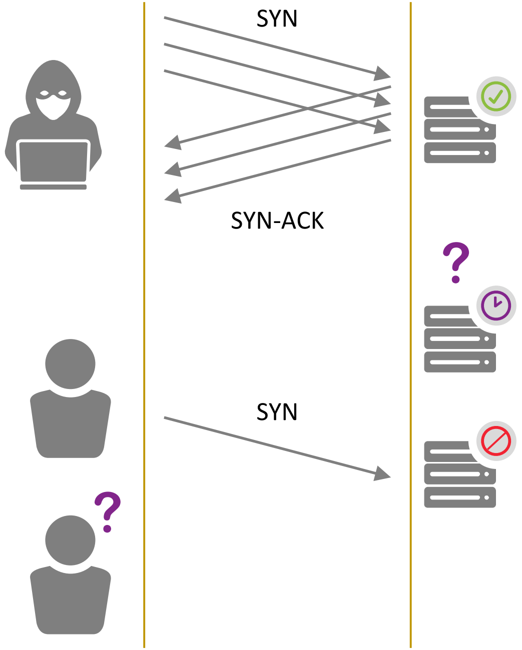
Day 7

6:40AM – DDoS is Here

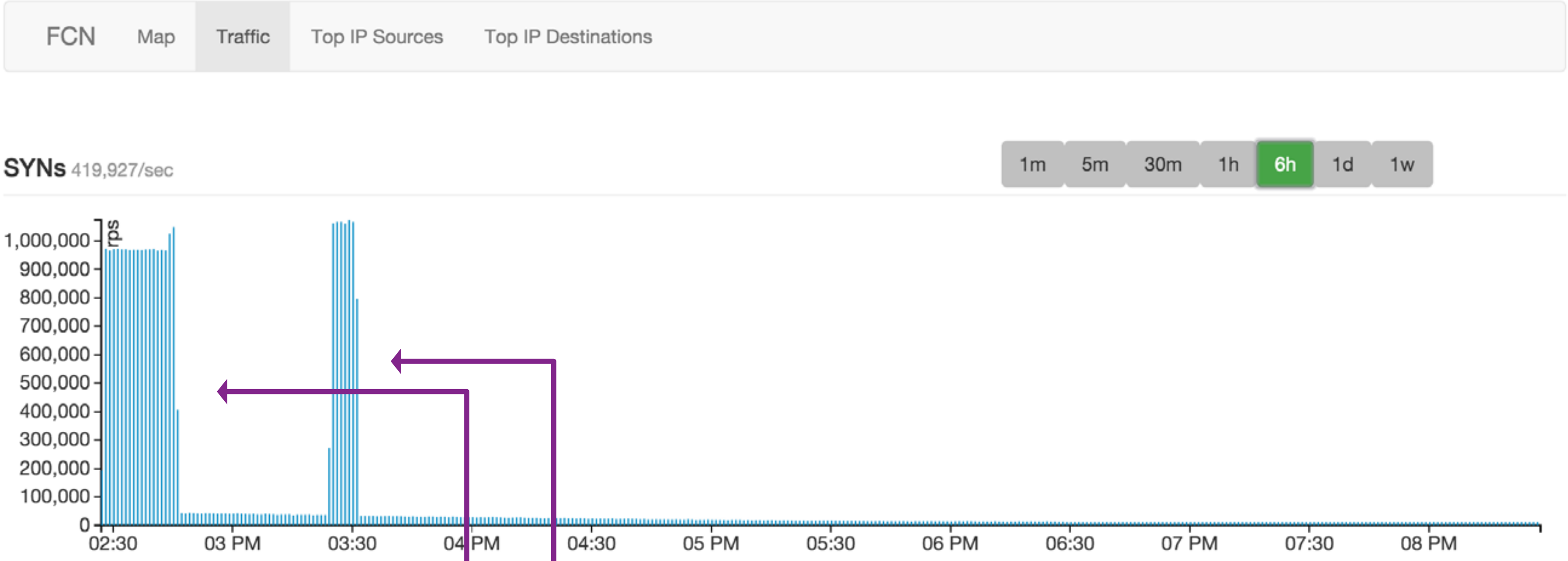
Verizon detects the attack (SYN Flood), which peaks at 80Gbps.

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 their servers and render them 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 IP Anycast has native DDoS attack mitigation (automated mitigation technology).

Super PoPs

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.

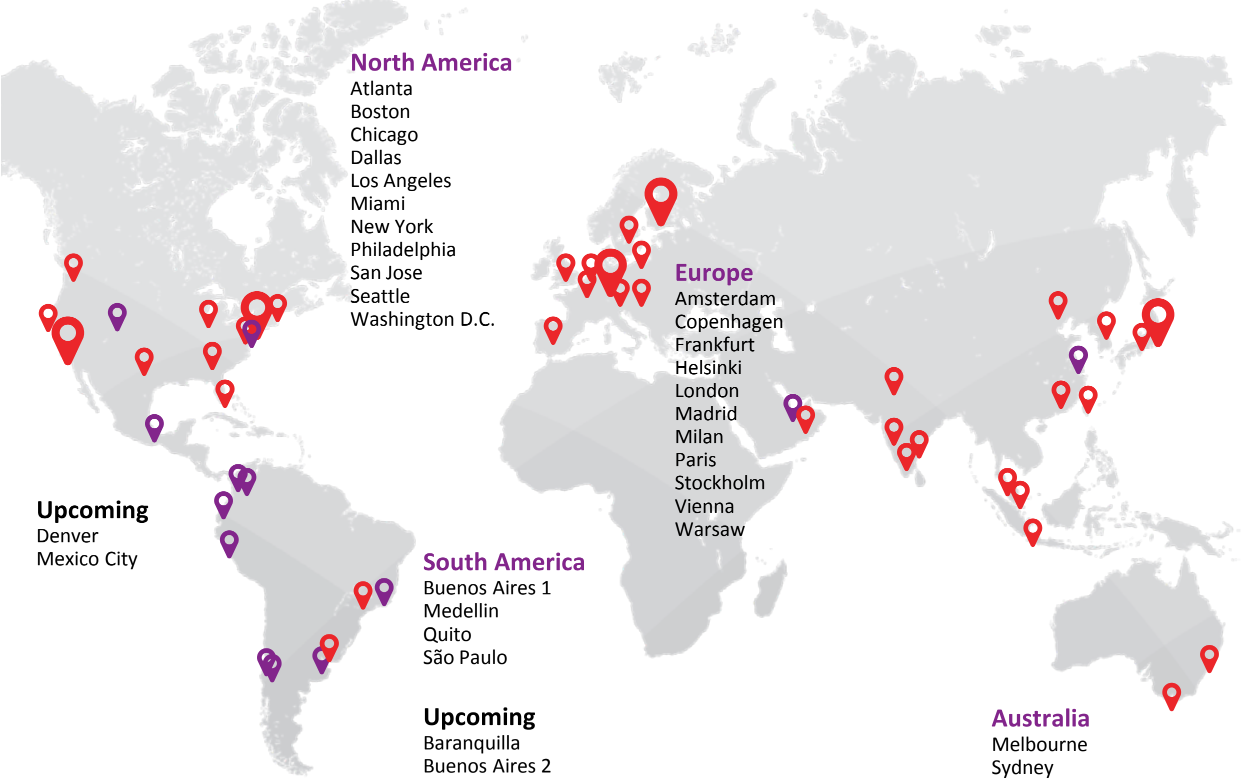
Network Attack Mitigation

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.

Our Network



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

20Tbps
Network Capacity

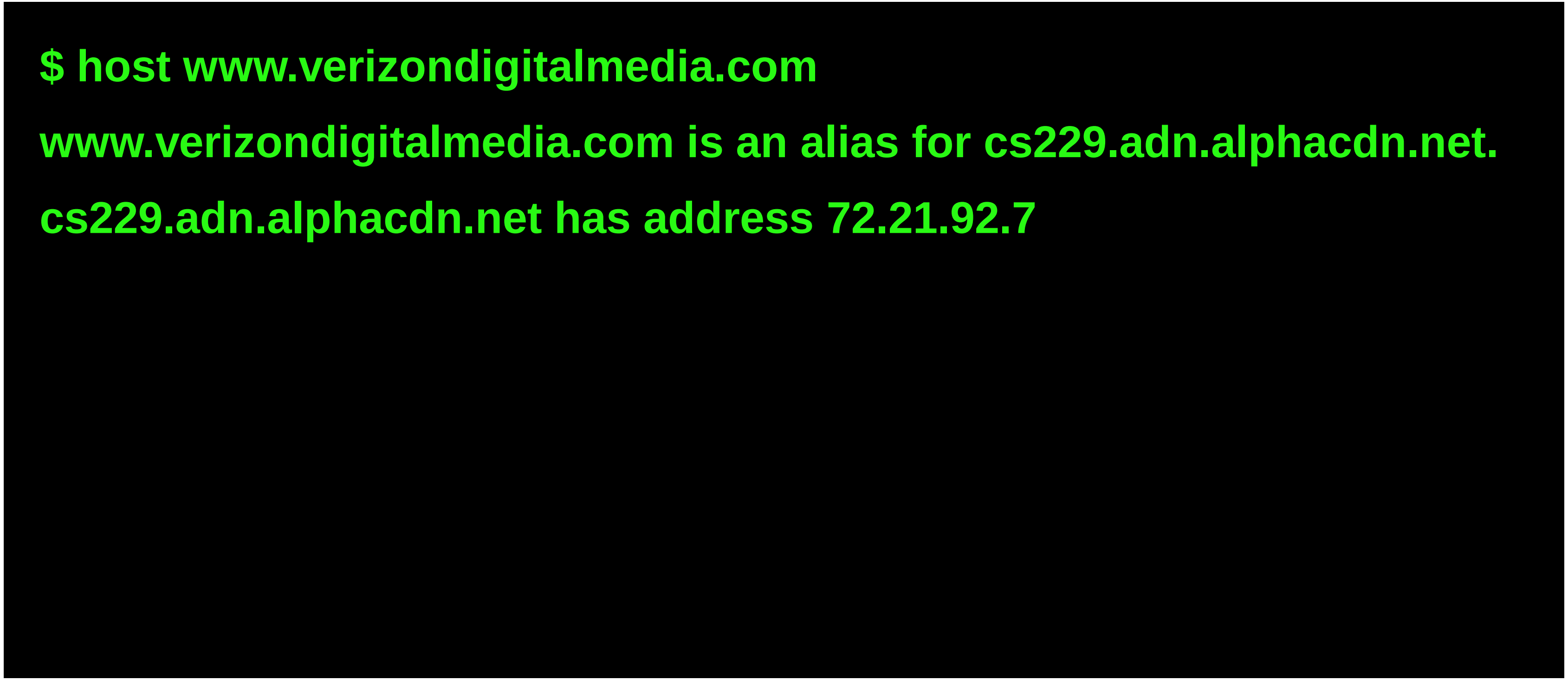
95+
PoPs

5
Continents

3,000+
Interconnects

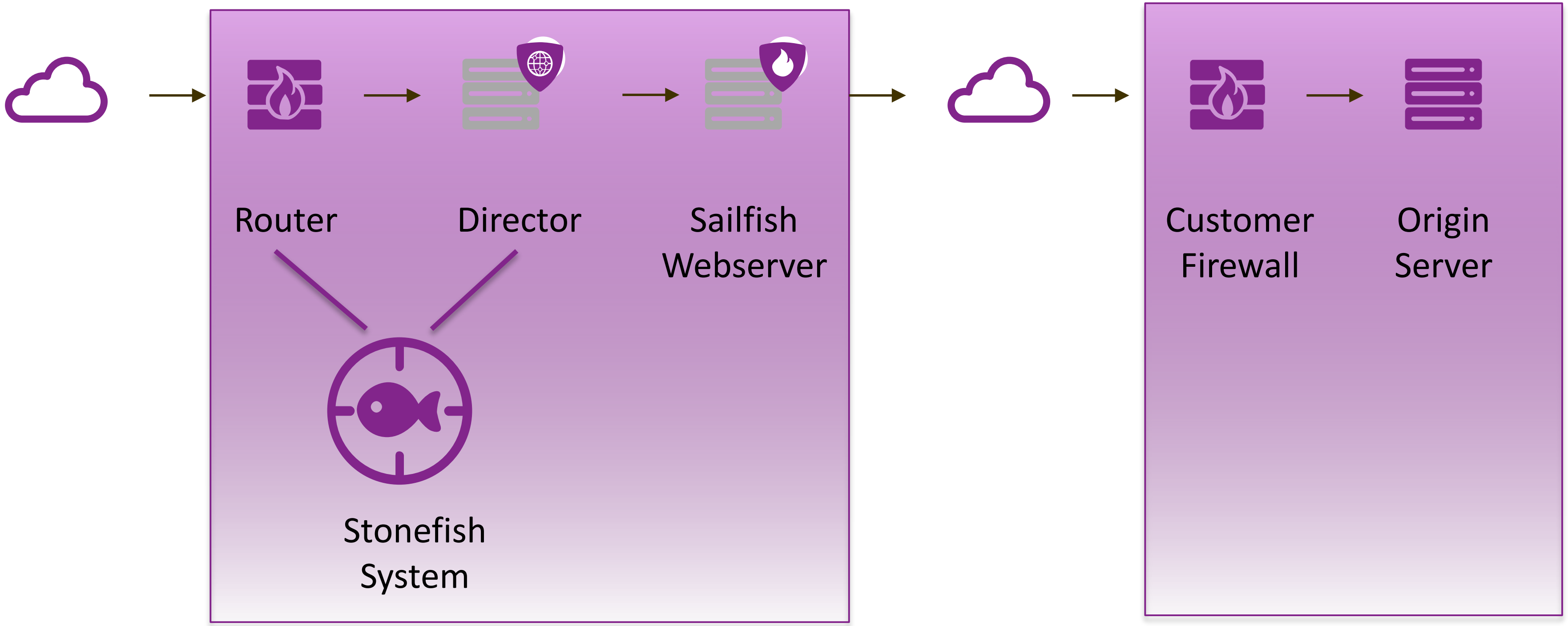
verizon✓
digital media services

Anycast CDN 101



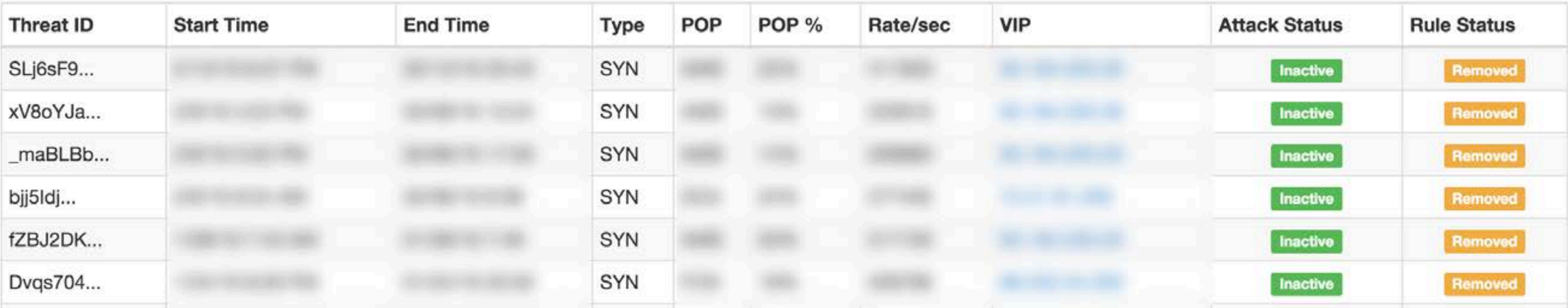
```
$ host www.verizondigitalmedia.com
www.verizondigitalmedia.com is an alias for cs229.adn.alphacdn.net.
cs229.adn.alphacdn.net has address 72.21.92.7
```

Layered Defense



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...	[illegible]	[illegible]	SYN	[illegible]	[illegible]	[illegible]	[illegible]	Inactive	Removed
xV8oYJa...	[illegible]	[illegible]	SYN	[illegible]	[illegible]	[illegible]	[illegible]	Inactive	Removed
_maBLBb...	[illegible]	[illegible]	SYN	[illegible]	[illegible]	[illegible]	[illegible]	Inactive	Removed
bjj5Idj...	[illegible]	[illegible]	SYN	[illegible]	[illegible]	[illegible]	[illegible]	Inactive	Removed
fZBJ2DK...	[illegible]	[illegible]	SYN	[illegible]	[illegible]	[illegible]	[illegible]	Inactive	Removed
Dvqs704...	[illegible]	[illegible]	SYN	[illegible]	[illegible]	[illegible]	[illegible]	Inactive	Removed

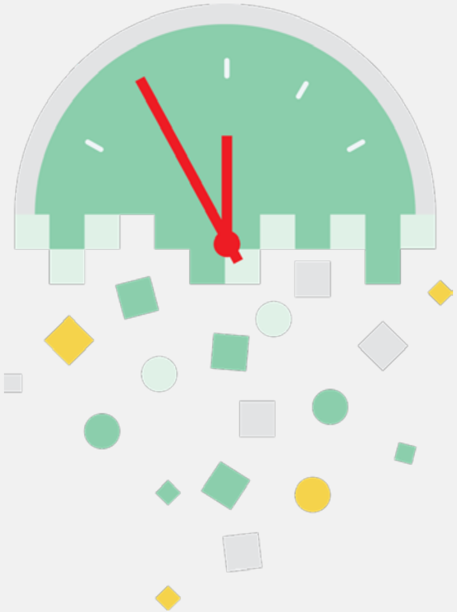
Staying Vigilant

- 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.

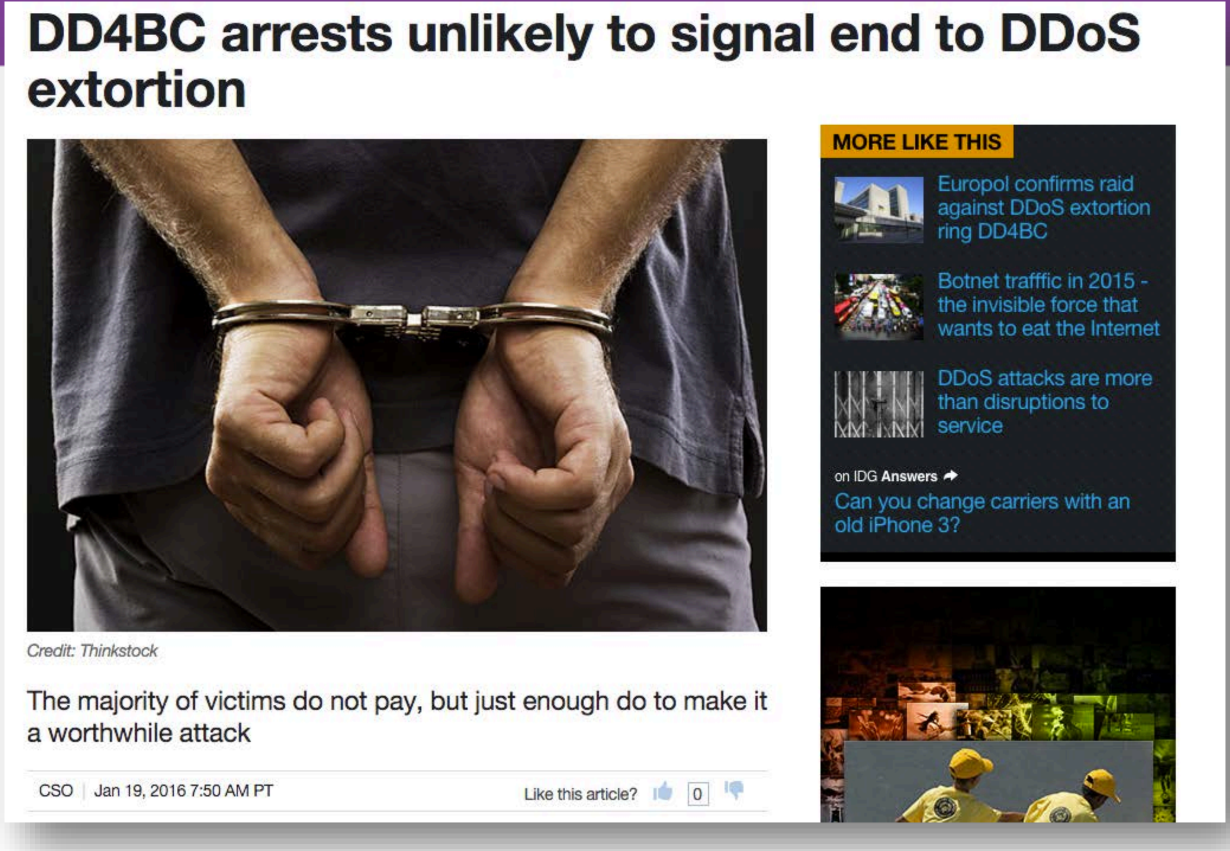
Day 8

Day 8

No Attack.
Nothing.



Many
many
days
later



DD4BC arrests unlikely to signal end to DDoS extortion

Credit: Thinkstock

The majority of victims do not pay, but just enough do to make it a worthwhile attack

CSO | Jan 19, 2016 7:50 AM PT

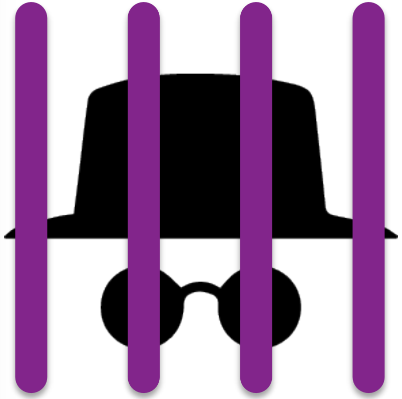
Like this article? 0

MORE LIKE THIS

- Europol confirms raid against DDoS extortion ring DD4BC
- Botnet trafffic in 2015 - the invisible force that wants to eat the Internet
- DDoS attacks are more than disruptions to service

on IDG **Answers**

Can you change carriers with an old iPhone 3?



Lessons

Learned

Apply Them

Lessons Learned

#1

Protect your origin IP:

Origin cloaking is best practice.

Lessons Learned

#2

Don’t forget to protect apex domain:

http://yourdomainnamehere.com

Lessons Learned

#3

You need a plan.

Do your employees know who to escalate to?

Do you know what your attack surface is?

Lessons Learned

#4

You need on-demand scalability and capacity.

Attacks won’t happen on schedule.

You need massive capacity on standby, globally.

Lessons Learned

#5

What is your DDoS breaking point?

80 Gbps?

200 Gbps?

1 Tbps?

Lessons Learned

#6

Can your appliance handle it?

Average DDoS: 5.5 Gbps

Hardware Cost: $200,000

Plus Support and Operation costs

Lessons Learned

#7

You need agile WAF.

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

Lessons Learned

#8

You need agile security service.

How fast can your vendor come to your aid?

The Sequel…

Armada Collective?

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

We are Armada Collective.

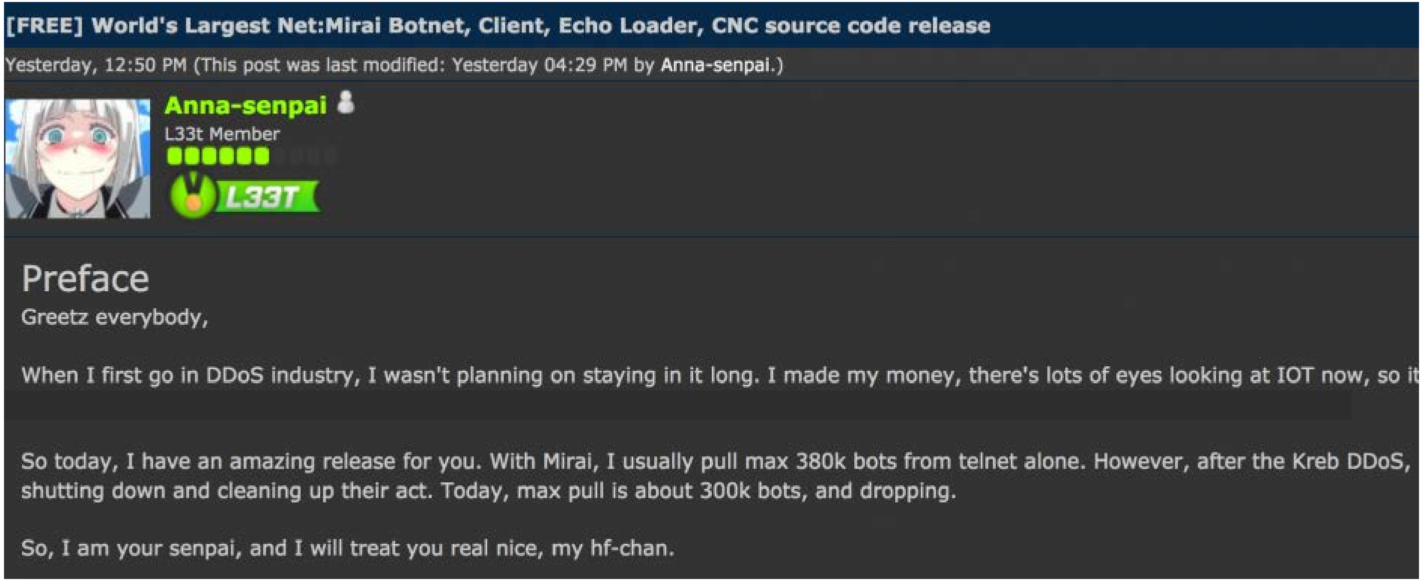
http://lmgtfy.com/?q=Armada+Collective

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

L33T

Preface

Greetz everybody,

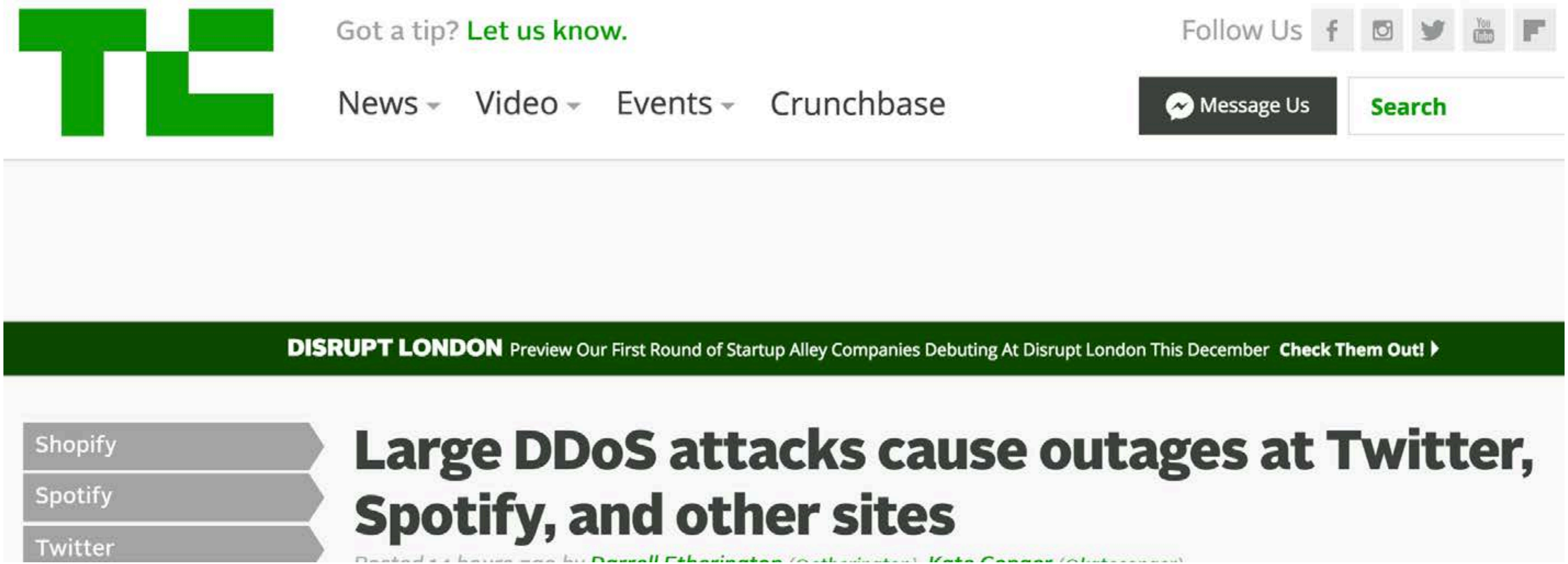
When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it

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 …

October 21, 2016

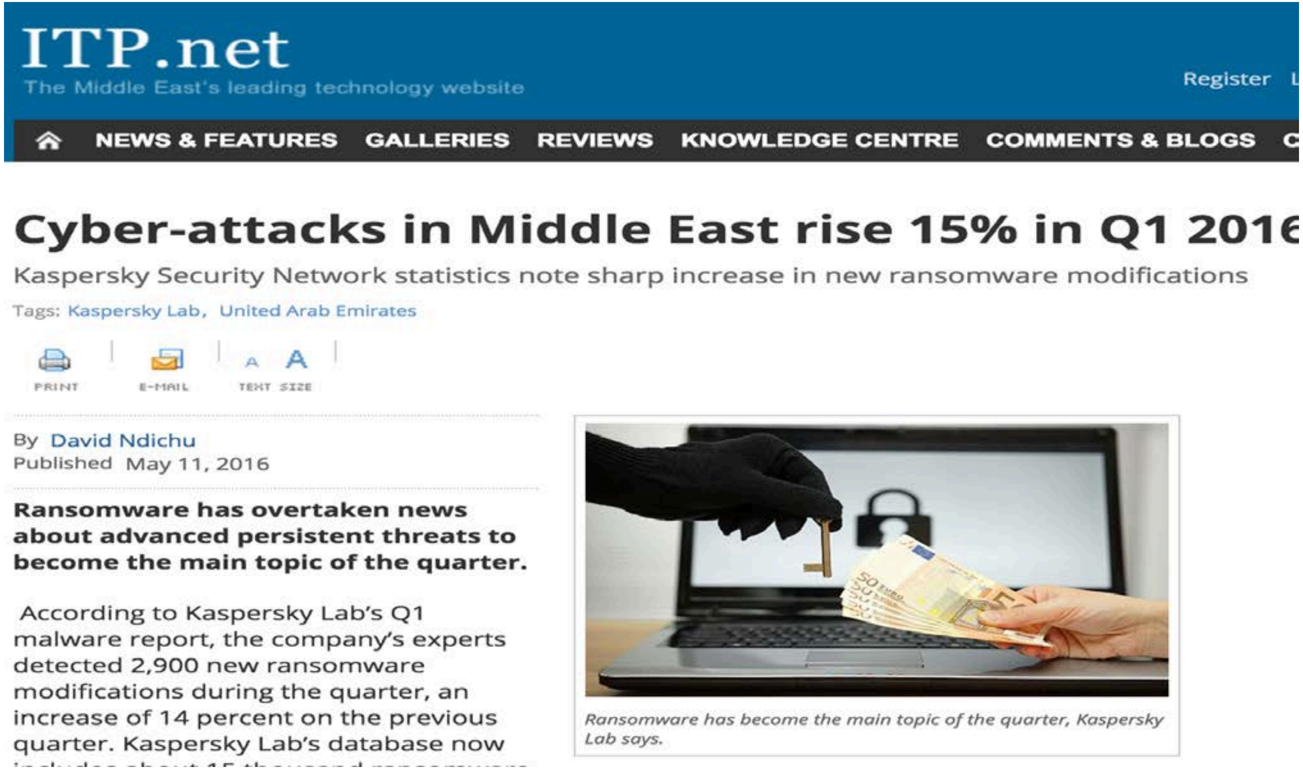


DISRUPT LONDON Preview Our First Round of Startup Alley Companies Debuting At Disrupt London This December Check Them Out!

Large DDoS attacks cause outages at Twitter, Spotify, and other sites

Posted 14 hours ago by Darrell Etherington (@etherington), Kate Conger (@katecconger)

Closer to home …



Cyber-attacks in Middle East rise 15% in Q1 2016

Kaspersky Security Network statistics note sharp increase in new ransomware modifications

Tags: Kaspersky Lab, United Arab Emirates

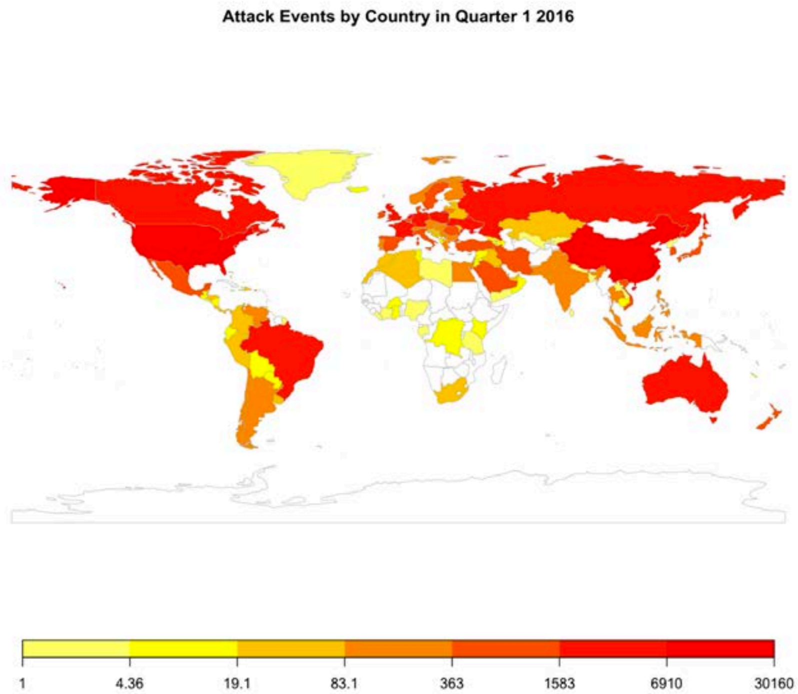
By David Ndichu
Published May 11, 2016

Ransomware has overtaken news about advanced persistent threats to become the main topic of the quarter.

According to Kaspersky Lab's Q1 malware report, the company's experts detected 2,900 new ransomware modifications during the quarter, an increase of 14 percent on the previous quarter. Kaspersky Lab's database now includes about 15 thousand ransomware

Ransomware has become the main topic of the quarter, Kaspersky Lab says.

Nexusguard Q1 2016 DDoS Threat Report



“we see an increasing focus on the Middle East”

-Nexusguard

Thank You

Tin Zaw
Director, Security Solutions
Verizon Digital Media Services

@tzaw | @verizondigital
www.verizondigitalmedia.com