Redes distribuidas para la protección y el crecimiento de negocios en la Web

Greivin Viquez

Gerente Comercial Regional

gviqueza@akamai.com

+506 83 28 65 65

Akamai

Experience the Edge

Akamai Snapshot

$3.2B

2020 Annual Revenue

Up 11% year-over-year and when adjusted for foreign exchange

8,396*

Current Employees

*As of December 2020

Akamai had

6,589

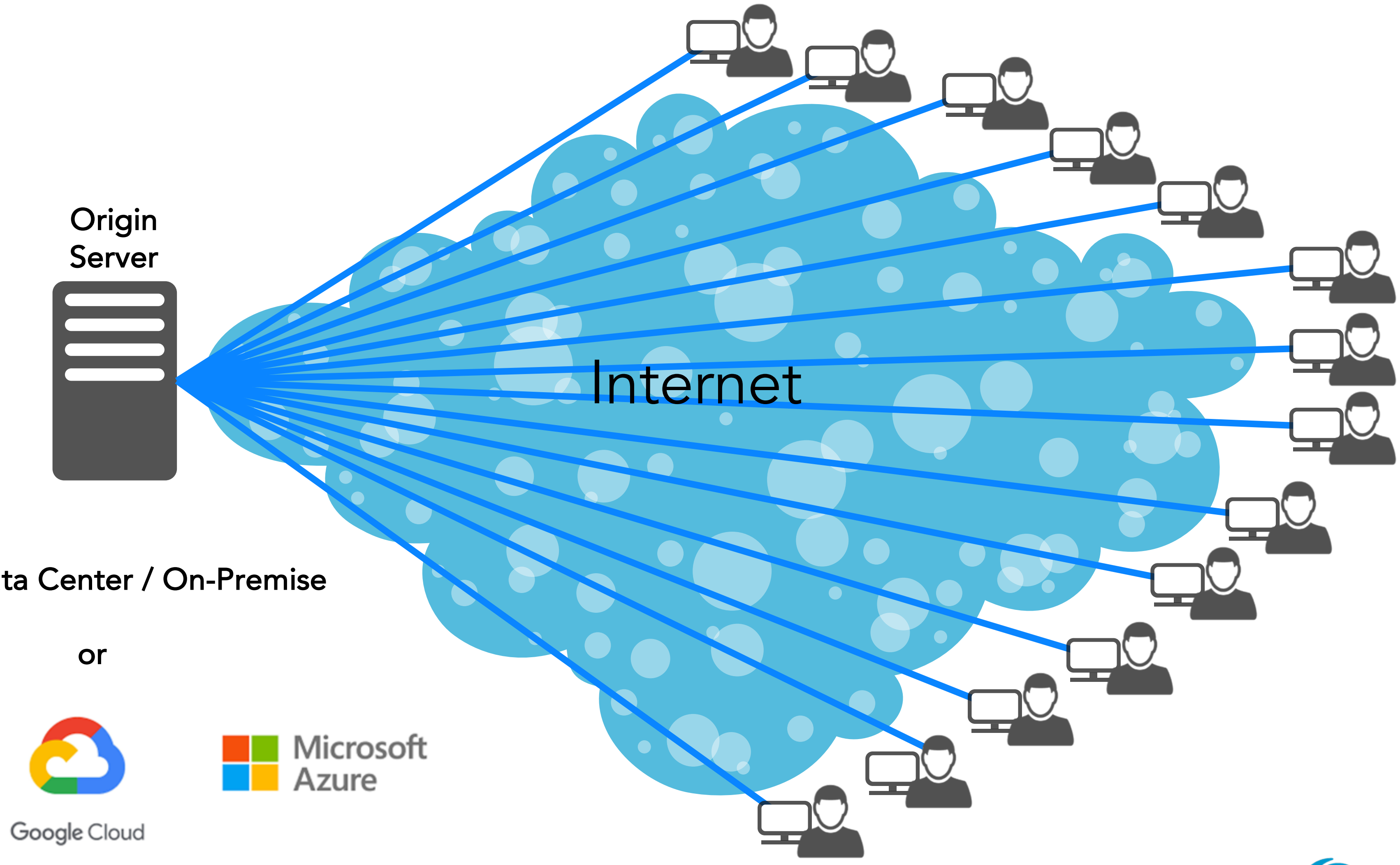
revenue generating customers at the end of Q420

- Founded in 1998 (Nasdaq:AKAM), with HQ in Cambridge, Massachusetts
- Invented Content Delivery Network (CDN), that's Akamai Intelligent Platform
- Akamai Intelligent Platform has ~350K servers delivering 200 Tbps (March 2021) in over 135 countries
- Responsible of serving 40% of all web traffic
- 85% of the world's Internet users are within a single "network hop" of Akamai's CDN

Akamai Experience the Edge

¿What is a Content Delivery Network (CDN) / Red distribuida?

Delivering content without a CDN



Private Data Center / On-Premise

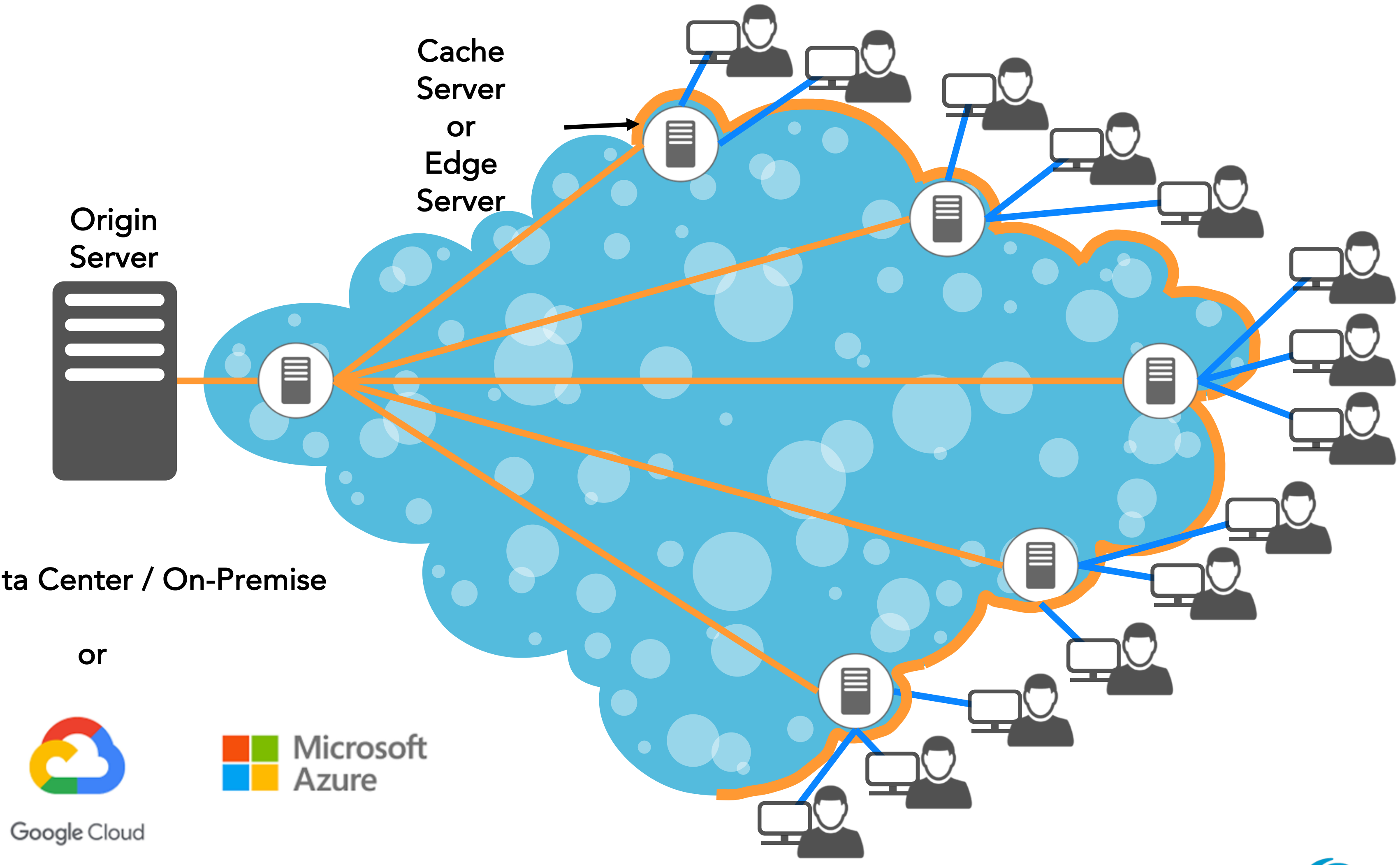
or

amazon web services

Google Cloud

Microsoft Azure

Delivering content with a CDN from the Edge



Origin Server

Cache Server or Edge Server

Private Data Center / On-Premise

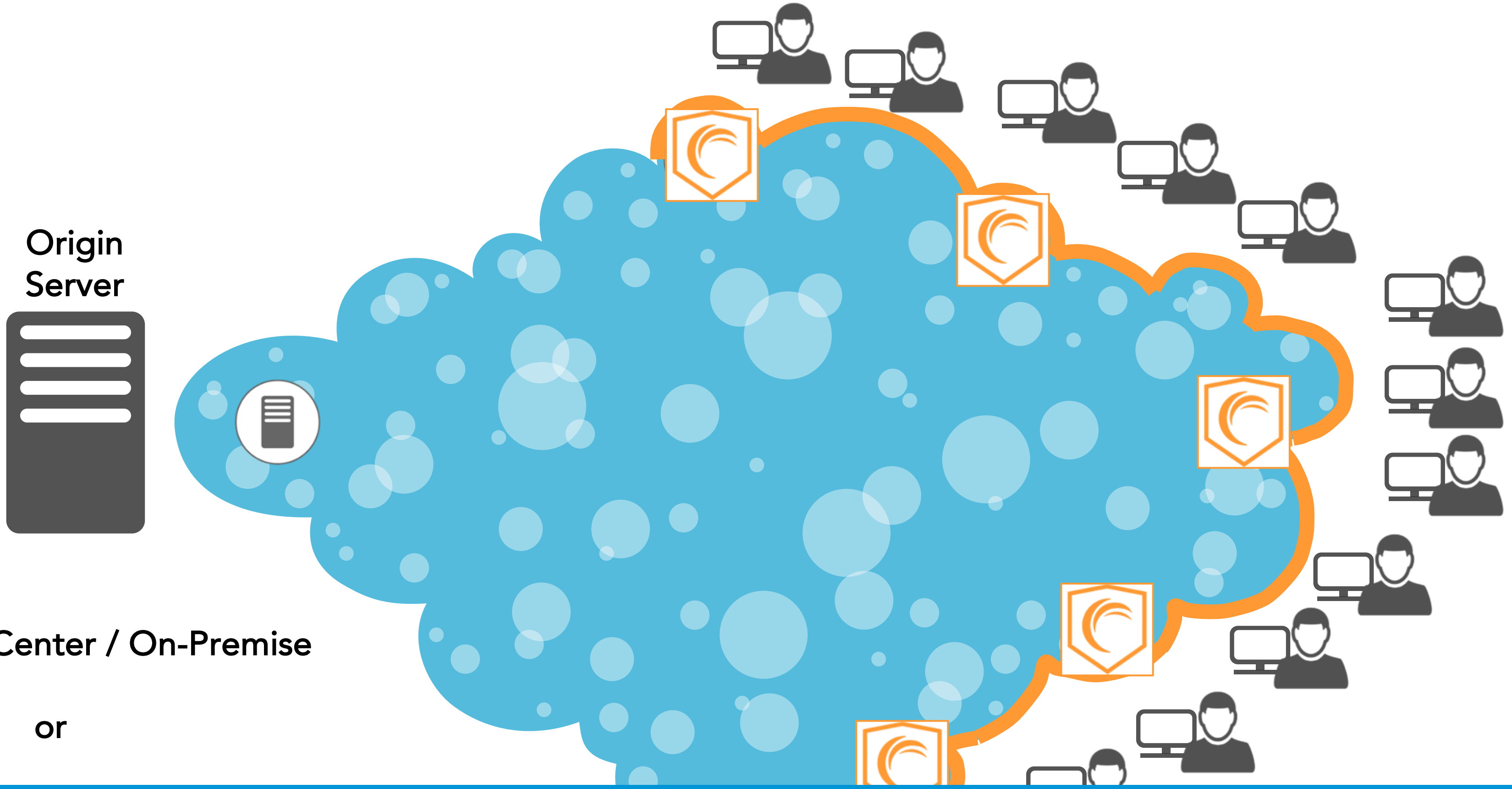
or

amazon web services

Google Cloud

Microsoft Azure

Delivering content with a CDN from the Edge+Security



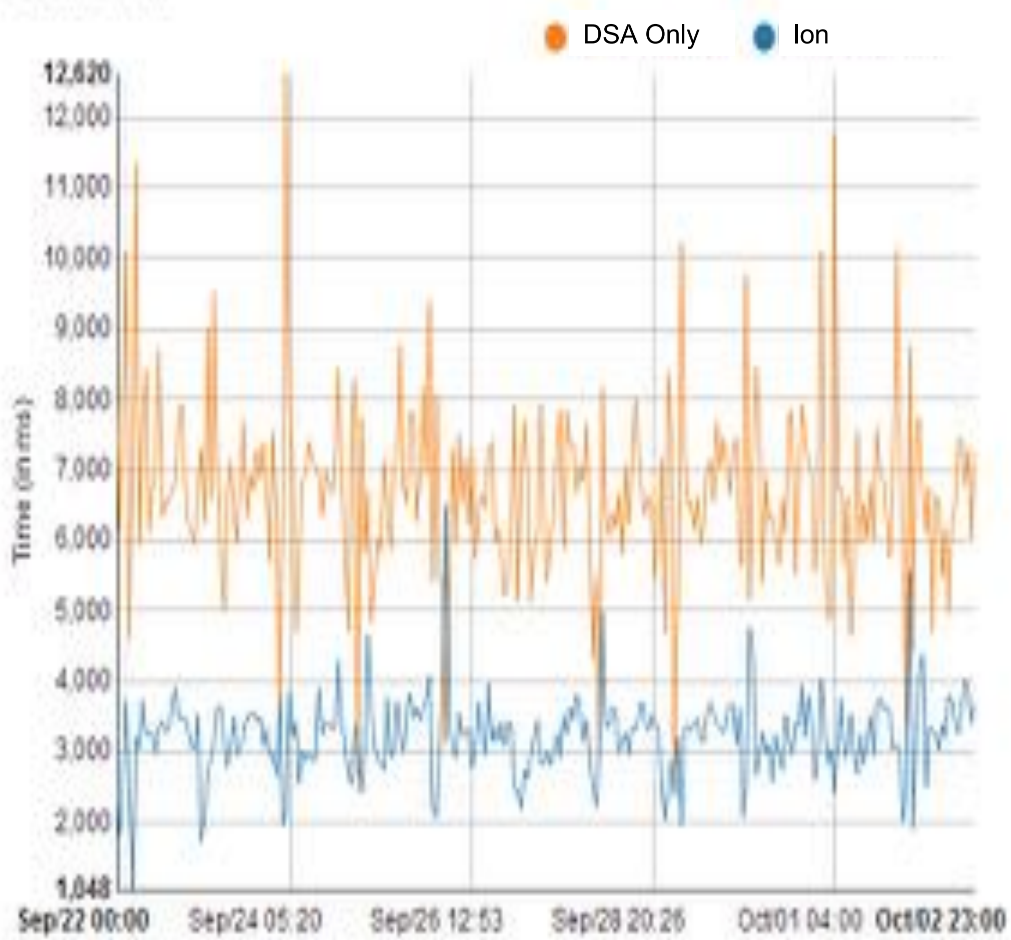
Private Data Center / On-Premise

or

Moving content closer to your users and offload your origin server

Casos de Negocio !

M and M Direct Delivers Fast, Quality Experiences with Akamai



Akamai Real User Monitoring

UK Users, UK Origin RWD Site

MandmDirect

103%

avg. performance improvement over DSA

Median:

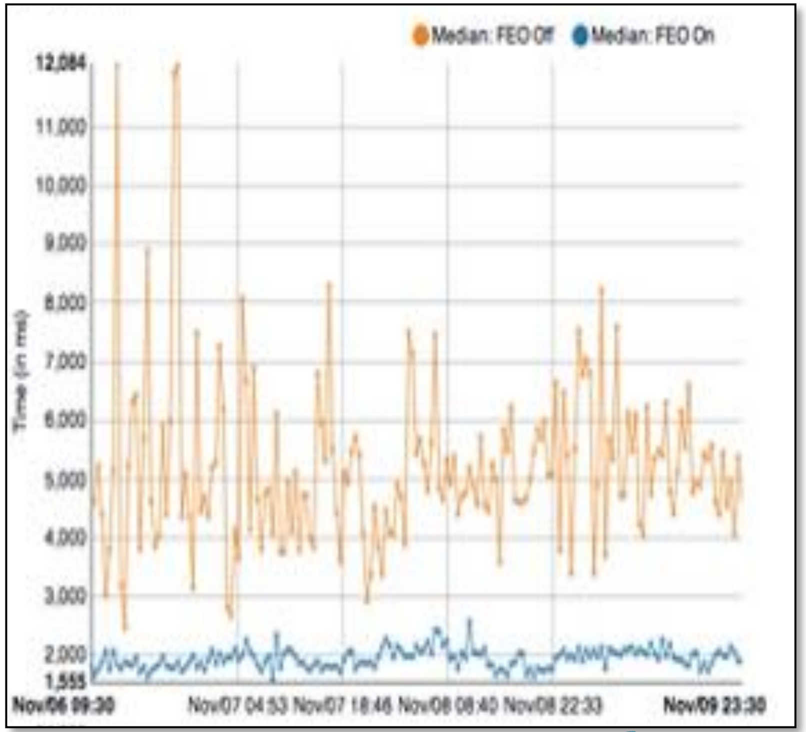
DSA Only: 6,771 ms

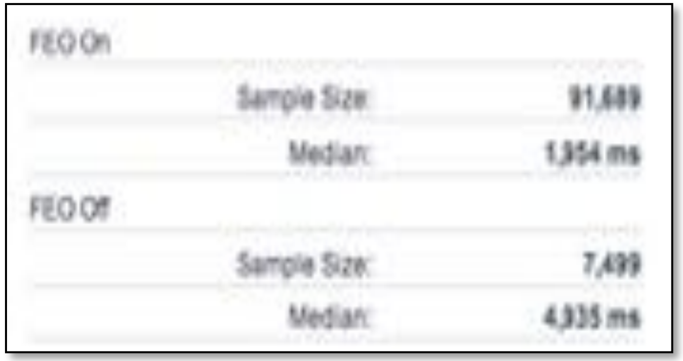
Ion: 3,338 ms

Savings of 3,433 ms

Decker’s Outdoor Corporation

- www.uggaustralia.com
- Responsive site, delivered with Ion
- Median perf improvement: **153%**
  - DSA: **4.93s**, Ion: **1.95s** (11/5 – 11/12)
- Deal signed 8/23
- Fully integrated with DPC and FEO 10/15



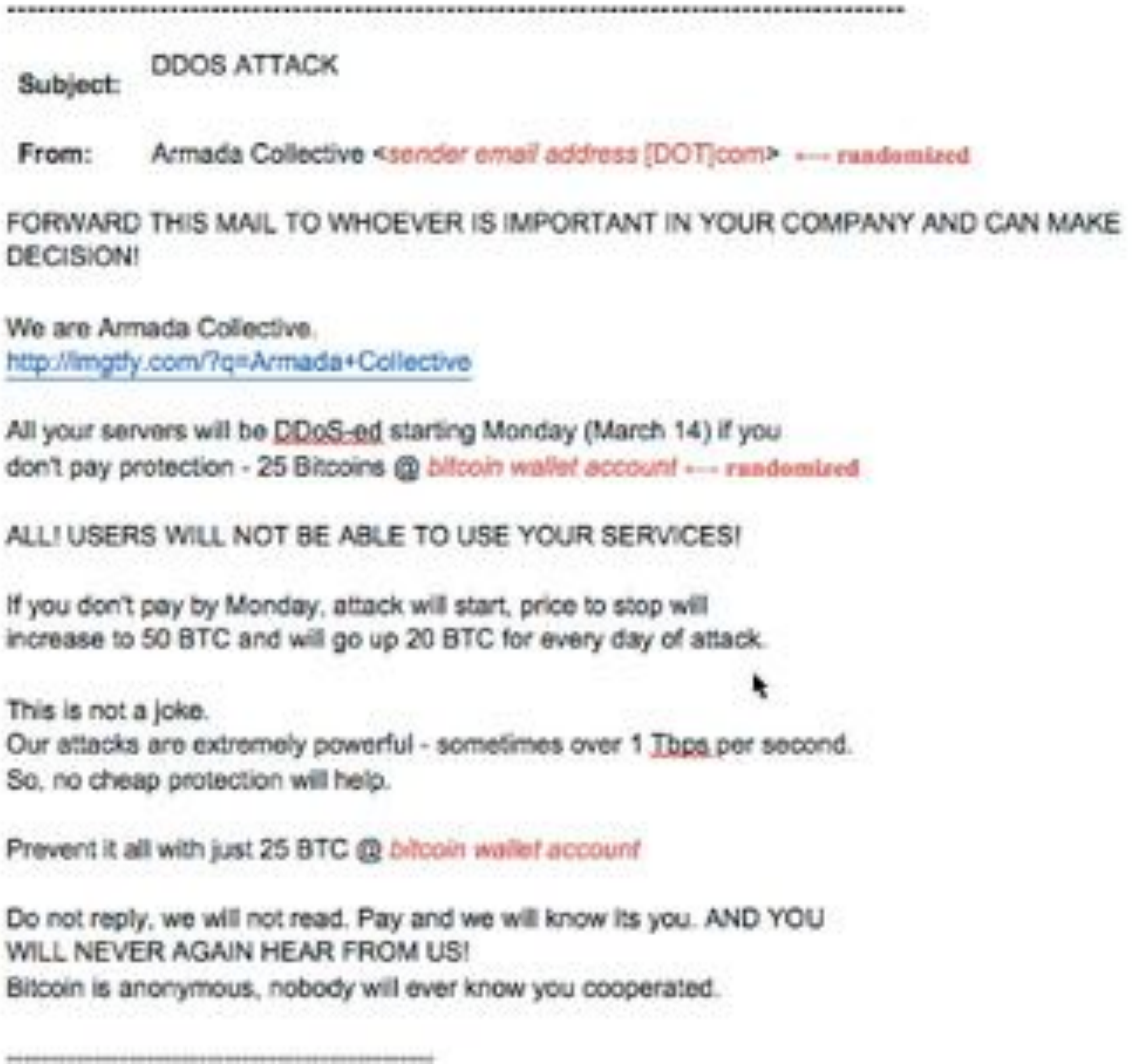


FEO On	
Sample Size	91,689
Median	1,954 ms
FEO Off	
Sample Size	7,499
Median	4,935 ms

ER

The Ransom letter

Why do t



Subject: DDOS ATTACK

From: Armada Collective <sender email address [DOT]com> ←-- randomized

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

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

All your servers will be DDoS-ed starting Monday (March 14) if you don't pay protection - 25 Bitcoins @ bitcoin wallet account ←-- randomized

ALL! USERS WILL NOT BE ABLE TO USE YOUR SERVICES!

If you don't pay by Monday, attack will start, price to stop will increase to 50 BTC and will go up 20 BTC for every day of attack.

This is not a joke.
Our attacks are extremely powerful - sometimes over 1 Tbps per second.
So, no cheap protection will help.

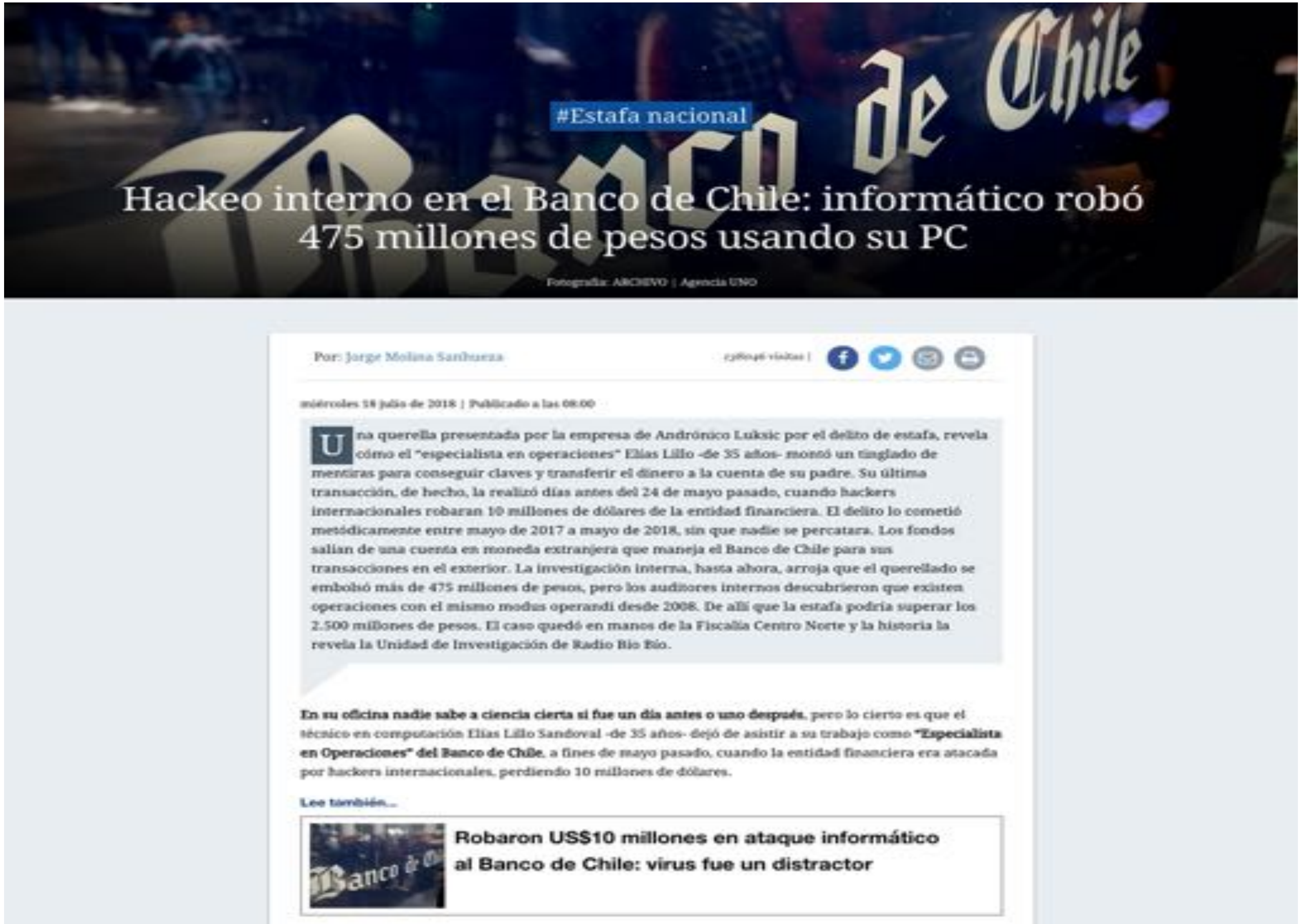
Prevent it all with just 25 BTC @ bitcoin wallet account

Do not reply, we will not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!
Bitcoin is anonymous, nobody will ever know you cooperated.

Banco de Chile

Hackeo interno en el Banco de Chile: informático robó 475 millones de pesos usando su PC

https://www.biobiochile.cl/especial/noticias/reportajes/reportajes-reportajes/2018/07/18/hackeo-interno-en-el-banco-de-chile-informatico-robo-475-millones-de-pesos-usando-su



#Estafa nacional

Hackeo interno en el Banco de Chile: informático robó 475 millones de pesos usando su PC

Fotografía: ARCHIVO | Agencia UNO

Por: Jorge Molina Sanhueza

[illegible] visitas |

miércoles 18 julio de 2018 | Publicado a las 08:00

Una querella presentada por la empresa de Andrónico Luksic por el delito de estafa, revela cómo el "especialista en operaciones" Elías Lillo -de 35 años- montó un tinglado de mentiras para conseguir claves y transferir el dinero a la cuenta de su padre. Su última transacción, de hecho, la realizó días antes del 24 de mayo pasado, cuando hackers internacionales robaran 10 millones de dólares de la entidad financiera. El delito lo cometió metódicamente entre mayo de 2017 a mayo de 2018, sin que nadie se percatara. Los fondos salían de una cuenta en moneda extranjera que maneja el Banco de Chile para sus transacciones en el exterior. La investigación interna, hasta ahora, arroja que el querellado se embolsó más de 475 millones de pesos, pero los auditores internos descubrieron que existen operaciones con el mismo modus operandi desde 2008. De allí que la estafa podría superar los 2.500 millones de pesos. El caso quedó en manos de la Fiscalía Centro Norte y la historia la revela la Unidad de Investigación de Radio Bío Bío.

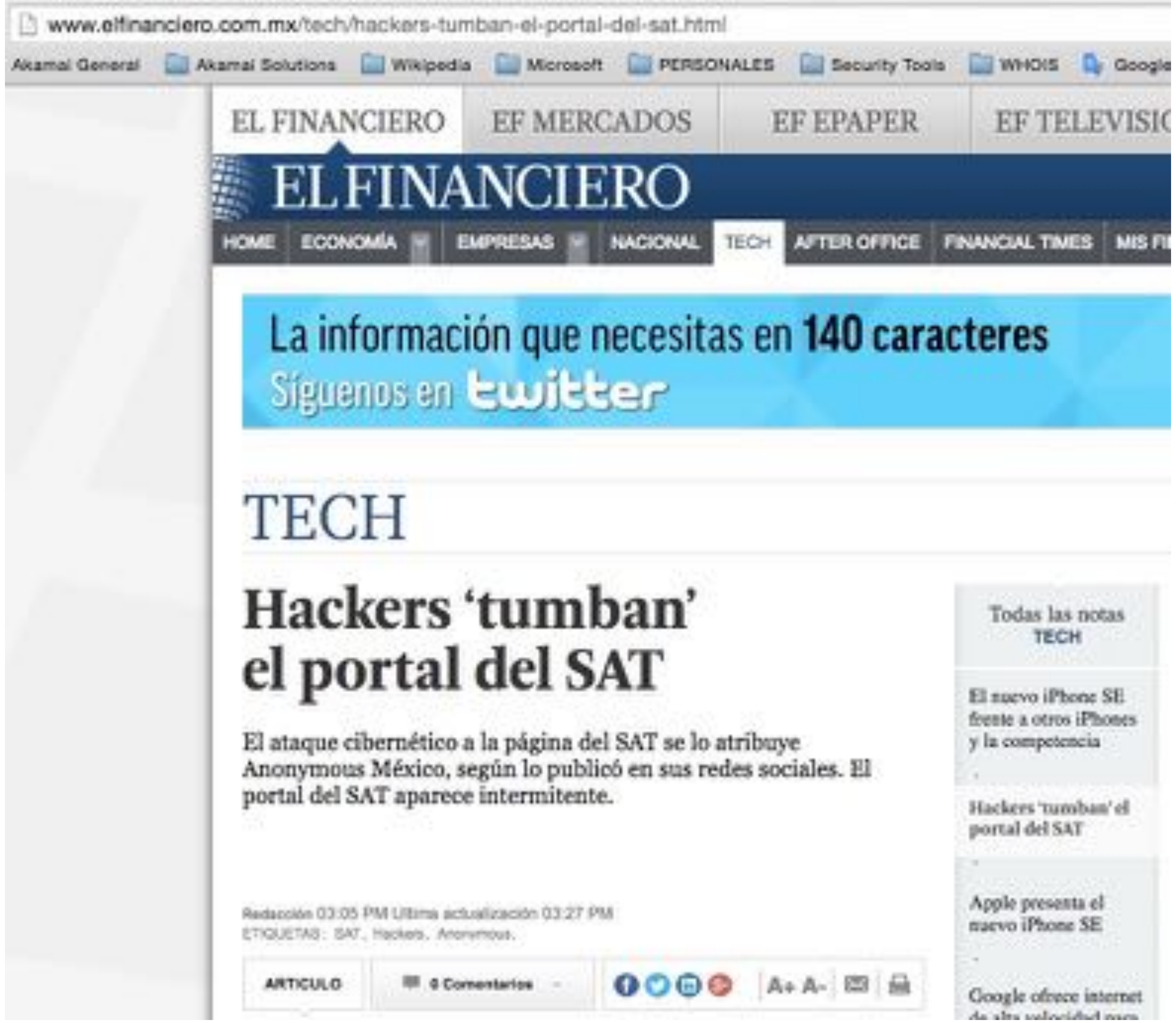
En su oficina nadie sabe a ciencia cierta si fue un día antes o uno después, pero lo cierto es que el técnico en computación Elías Lillo Sandoval -de 35 años- dejó de asistir a su trabajo como **"Especialista en Operaciones" del Banco de Chile**, a fines de mayo pasado, cuando la entidad financiera era atacada por hackers internacionales, perdiendo 10 millones de dólares.

Lee también...

Robaron US$10 millones en ataque informático al Banco de Chile: virus fue un distractor

Sistema de Administración Tributaria (SAT)

http://www.elfinanciero.com.mx/tech/hackers-tumban-el-portal-del-sat.html
https://www.facebook.com/hackersdemexico.net.mx
21/03/2016 a las 15:03 DESDE COSTA RICA



TECH

Hackers 'tumban' el portal del SAT

El ataque cibernético a la página del SAT se lo atribuye Anonymous México, según lo publicó en sus redes sociales. El portal del SAT aparece intermitente.

Redacción 03:05 PM Última actualización 03:27 PM
ETIQUETAS : SAT , Hackers , Anonymous ,

Todas las notas
TECH

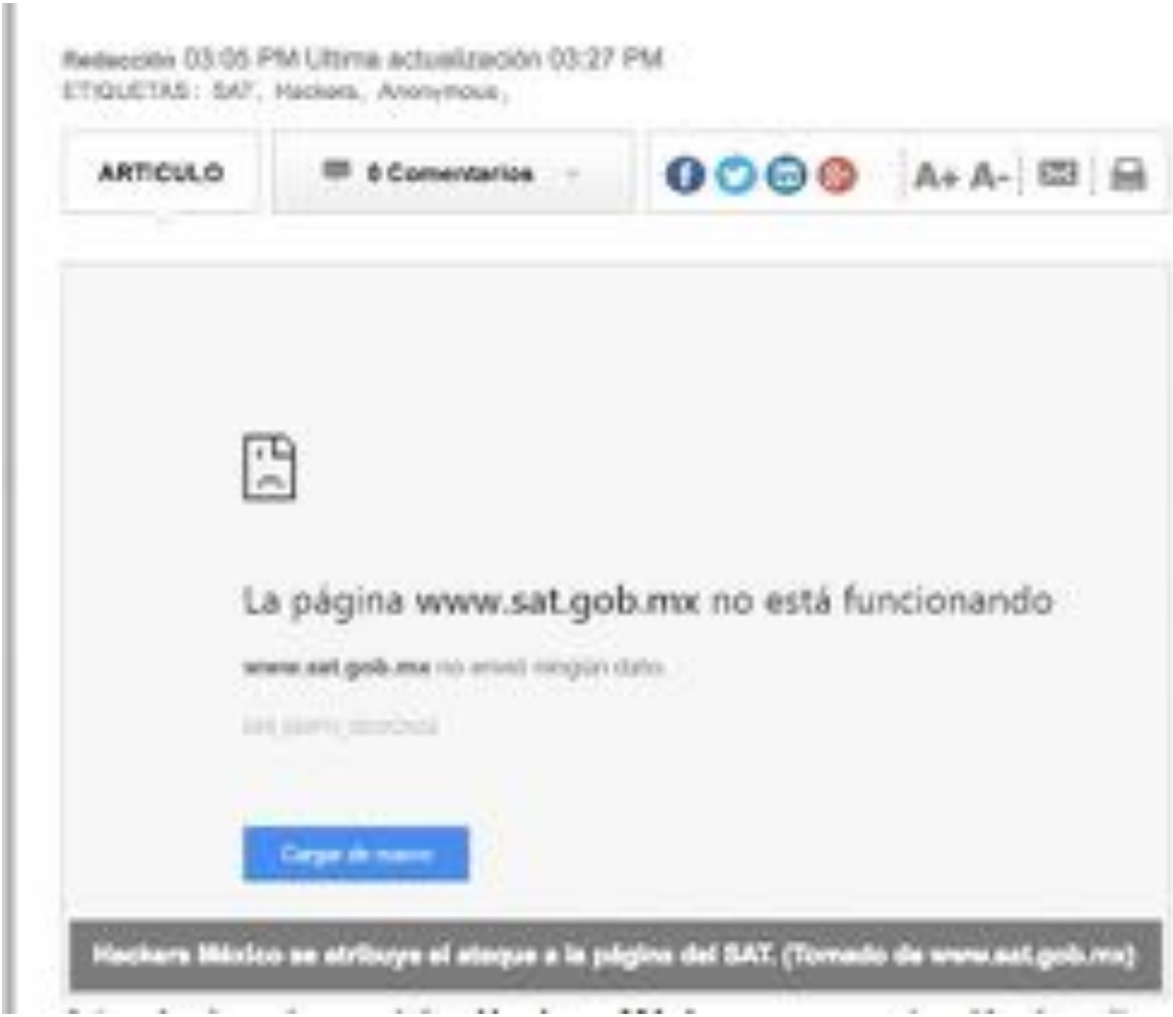
El nuevo iPhone SE frente a otros iPhones y la competencia

Hackers 'tumban' el portal del SAT

Apple presenta el nuevo iPhone SE

Google ofrece internet de alta velocidad para

Sistema de Administración Tributaria (SAT)



Redacción 03:05 PM Ultima actualización 03:27 PM
ETIQUETAS : SAT , Hackers , Anonymous ,

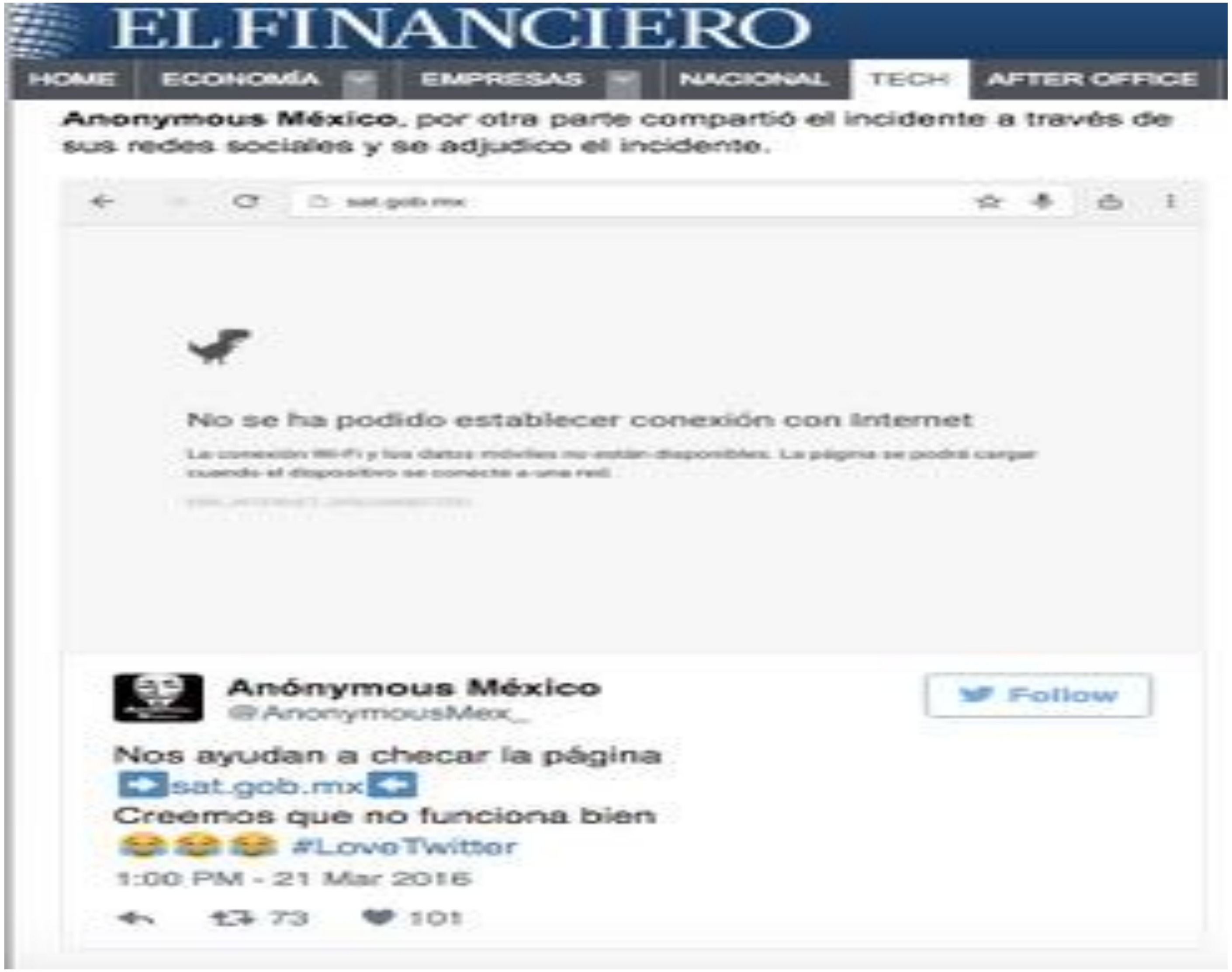
La página www.sat.gob.mx no está funcionando

www.sat.gob.mx no envió ningún dato.

ERR_EMPTY_RESPONSE

Hackers México se atribuye el ataque a la página del SAT. (Tomado de www.sat.gob.mx)

Sistema de Administración Tributaria (SAT)



Anonymous México, por otra parte compartió el incidente a través de sus redes sociales y se adjudico el incidente.

No se ha podido establecer conexión con Internet

La conexión Wi-Fi y los datos móviles no están disponibles. La página se podrá cargar cuando el dispositivo se conecte a una red.

ERR_INTERNET_DISCONNECTED

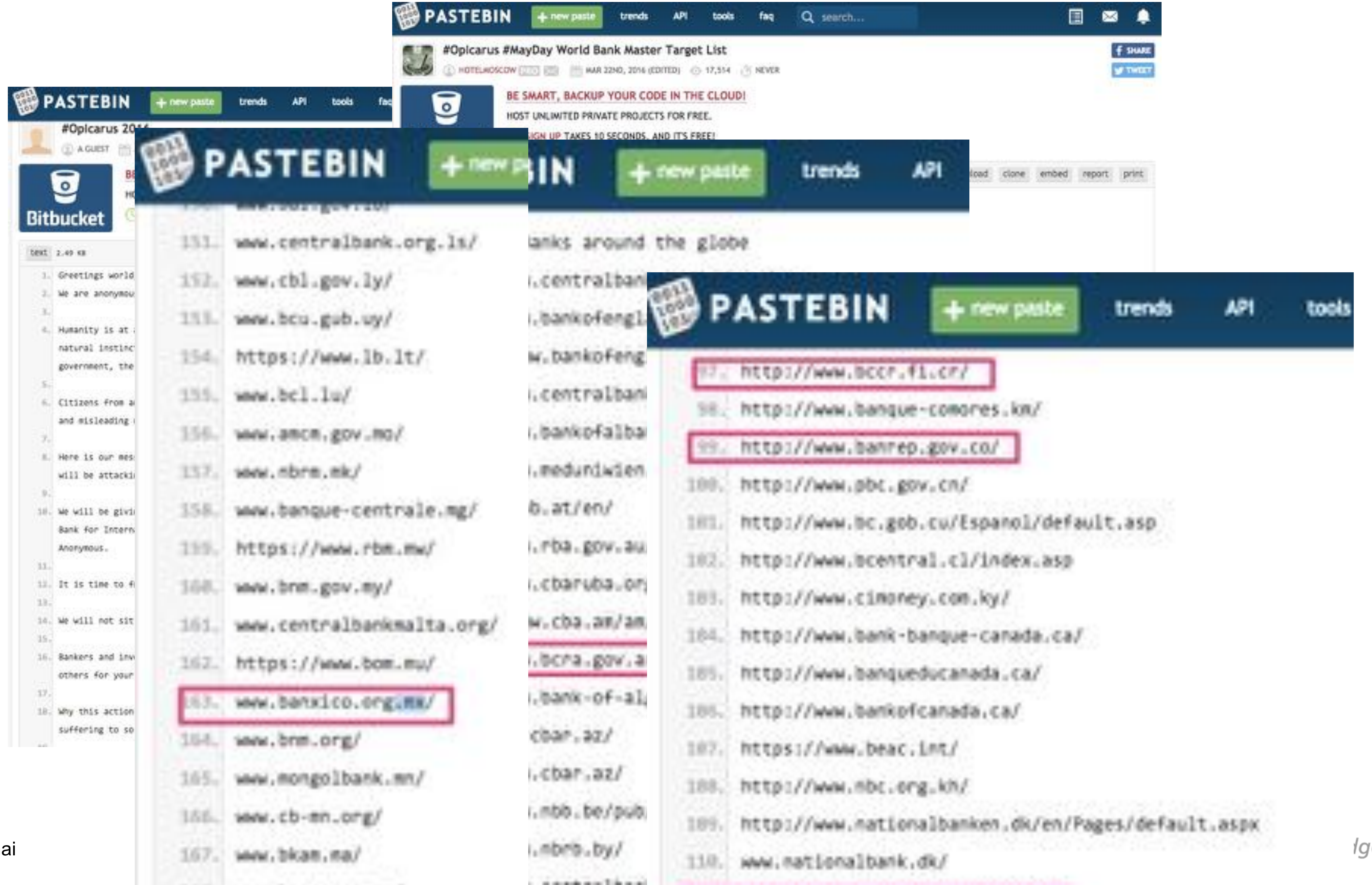
Anónymous México
@AnonymousMex_

Nos ayudan a checar la página
➡sat.gob.mx⬅
Creemos que no funciona bien
😂😂😂 #LoveTwitter

1:00 PM - 21 Mar 2016

73 ♥ 101

Sistema de Administración Tributaria (SAT)



#Opicarus #MayDay World Bank Master Target List

HOTELMOSCOW MAR 22ND, 2016 (EDITED) 17,514 NEVER

BE SMART, BACKUP YOUR CODE IN THE CLOUD!

HOST UNLIMITED PRIVATE PROJECTS FOR FREE.

SIGN UP TAKES 10 SECONDS, AND IT'S FREE!

#Opicarus 2016

A GUEST

text 2.49 KB

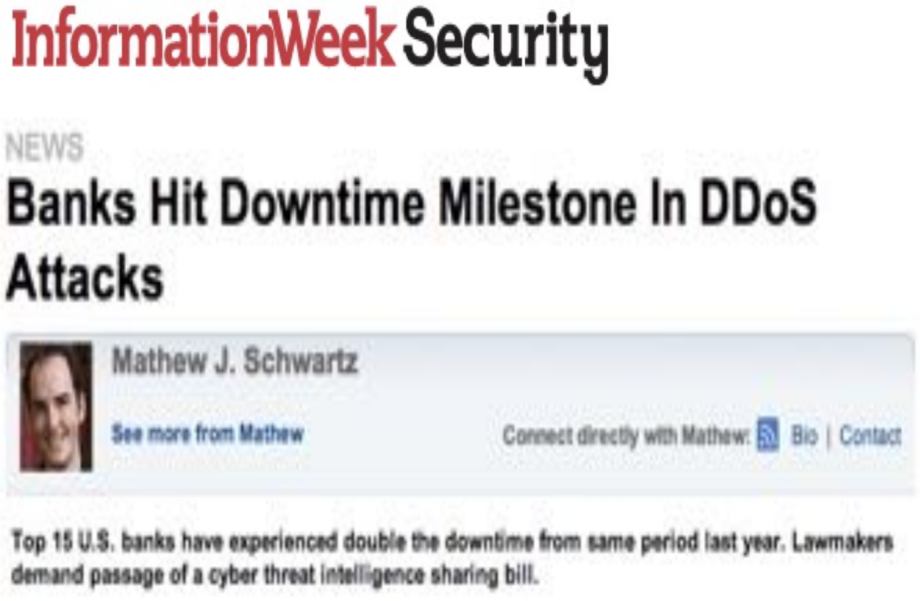
```
Greetings world
We are anonymou

Humanity is at
natural instinc
government, the

Citizens from a
and misleading

Here is our mes
will be attacki

We will be givi
Bank for Intern
Anonymous.

It is time to f

We will not sit

Bankers and inv
others for your

Why this action
suffering to so
```

```
151. www.centralbank.org.ls/
152. www.cbl.gov.ly/
153. www.bcu.gub.uy/
154. https://www.lb.lt/
155. www.bcl.lu/
156. www.amcm.gov.mo/
157. www.nbrm.mk/
158. www.banque-centrale.mg/
159. https://www.rbm.mw/
160. www.bnm.gov.my/
161. www.centralbankmalta.org/
162. https://www.bom.mu/
163. www.banxico.org.mx/
164. www.bnm.org/
165. www.mongolbank.mn/
166. www.cb-mn.org/
167. www.bkam.ma/
```

```
anks around the globe
.centralban
.bankofengl
w.bankofeng
.centralban
.bankofalba
.meduniwien
b.at/en/
.rba.gov.au
.cbaruba.or
w.cba.am/am
.bcra.gov.a
.bank-of-al
cbar.az/
.cbar.az/
.nbb.be/pub
.nbrb.by/
```

```
 97. http://www.bccr.fi.cr/
 98. http://www.banque-comores.km/
 99. http://www.banrep.gov.co/
100. http://www.pbc.gov.cn/
101. http://www.bc.gob.cu/Espanol/default.asp
102. http://www.bcentral.cl/index.asp
103. http://www.cimoney.com.ky/
104. http://www.bank-banque-canada.ca/
105. http://www.banqueducanada.ca/
106. http://www.bankofcanada.ca/
107. https://www.beac.int/
108. http://www.nbc.org.kh/
109. http://www.nationalbanken.dk/en/Pages/default.aspx
110. www.nationalbank.dk/
```

BroBot in Action



InformationWeek Security

NEWS

Banks Hit Downtime Milestone In DDoS Attacks

Mathew J. Schwartz

See more from Mathew

Connect directly with Mathew: Bio | Contact

Top 15 U.S. banks have experienced double the downtime from same period last year. Lawmakers demand passage of a cyber threat intelligence sharing bill.

Gartner.

DDOS attacks against U.S. Banks continue – linkages explored

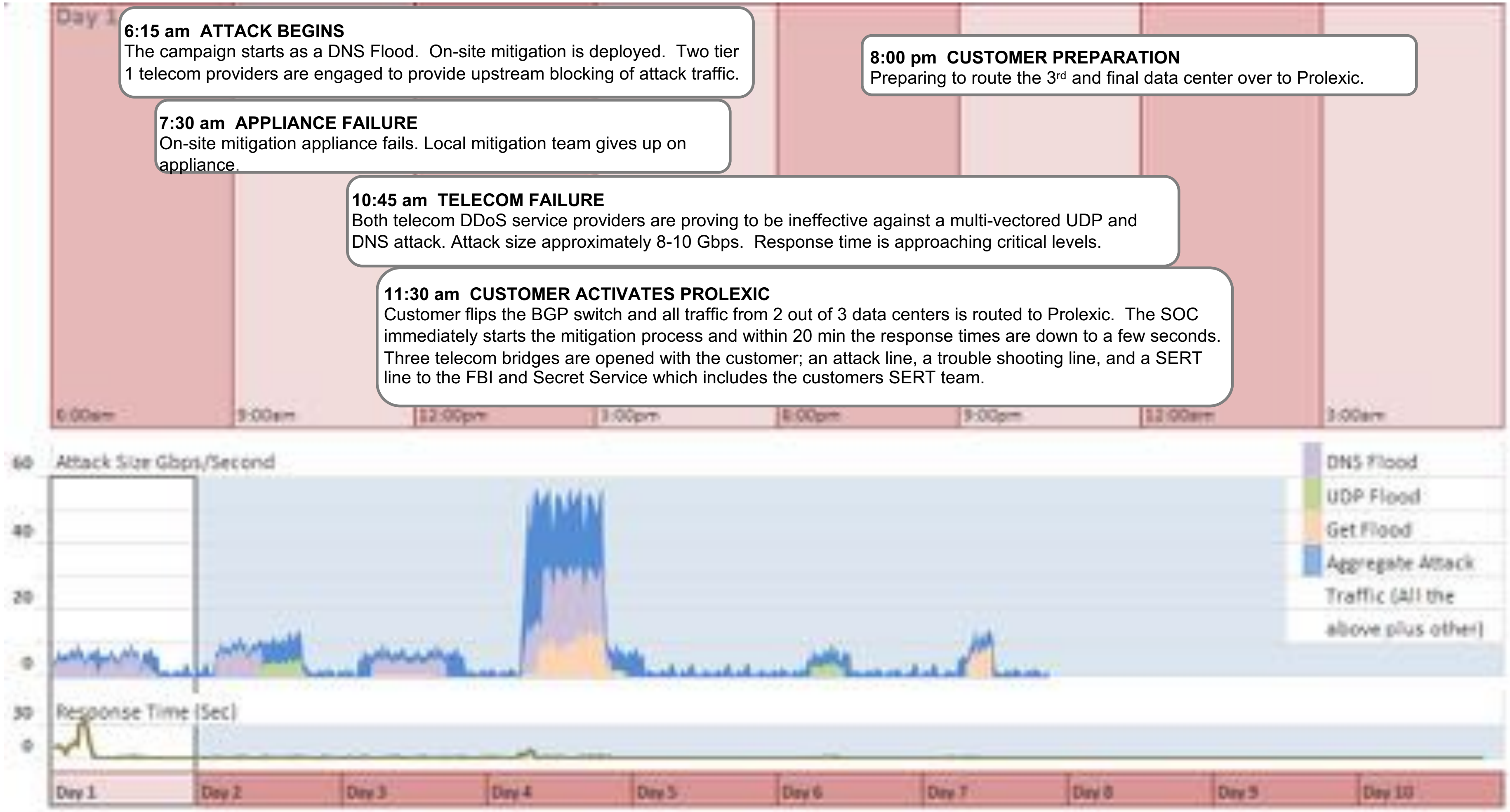
eWEEK®

DDoS Attacks on Major Banks Causing Problems for Customers

USA TODAY

NBC: Iran reportedly behind cyber attacks on U.S. banks

Case study 1: First Brobot Attack
DDoS campaign day 1 – large financial customer JAN 2012



6:15 am ATTACK BEGINS
The campaign starts as a DNS Flood. On-site mitigation is deployed. Two tier 1 telecom providers are engaged to provide upstream blocking of attack traffic.

7:30 am APPLIANCE FAILURE
On-site mitigation appliance fails. Local mitigation team gives up on appliance.

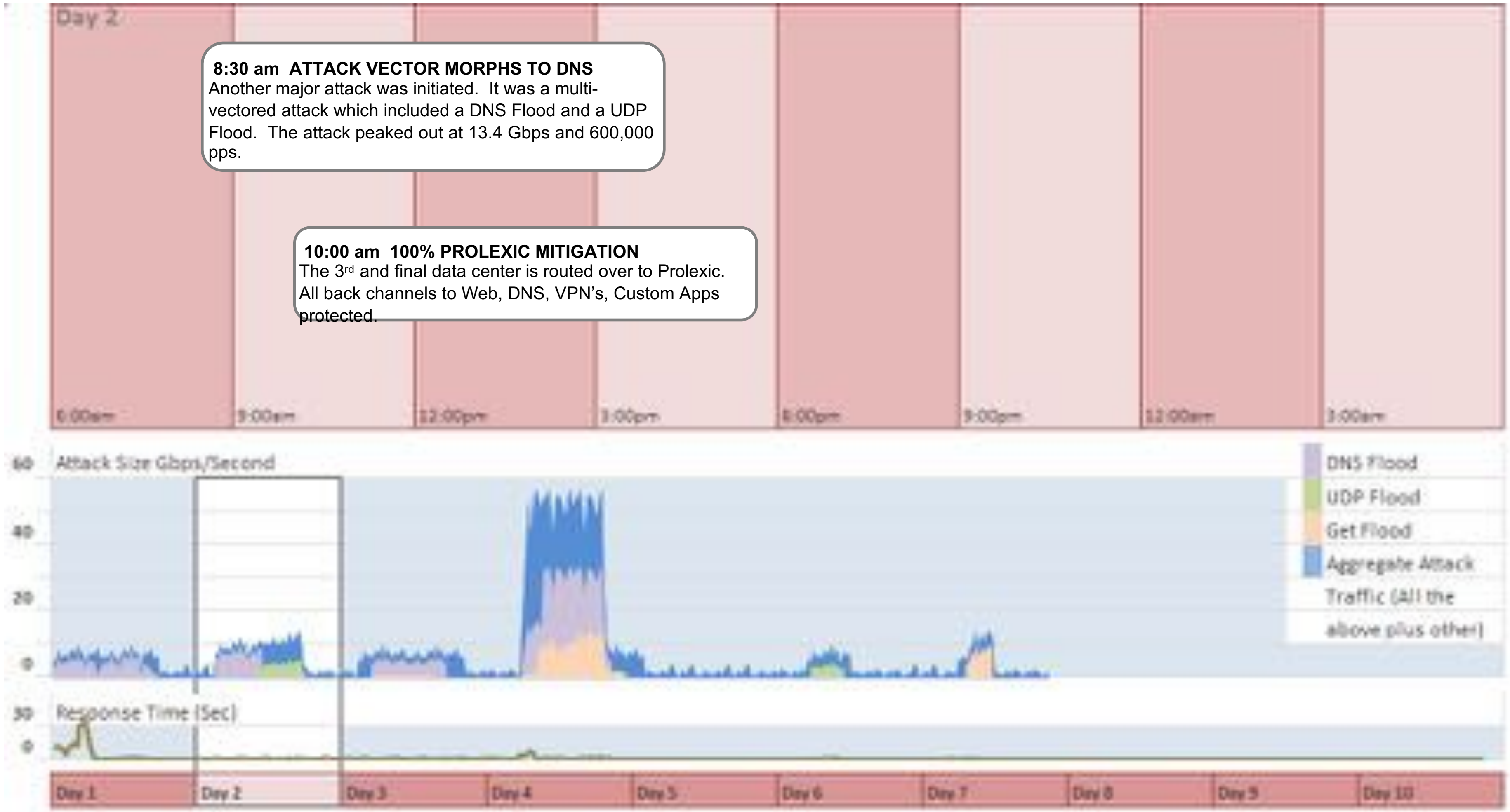
10:45 am TELECOM FAILURE
Both telecom DDoS service providers are proving to be ineffective against a multi-vectored UDP and DNS attack. Attack size approximately 8-10 Gbps. Response time is approaching critical levels.

11:30 am CUSTOMER ACTIVATES PROLEXIC
Customer flips the BGP switch and all traffic from 2 out of 3 data centers is routed to Prolexic. The SOC immediately starts the mitigation process and within 20 min the response times are down to a few seconds. Three telecom bridges are opened with the customer; an attack line, a trouble shooting line, and a SERT line to the FBI and Secret Service which includes the customers SERT team.

8:00 pm CUSTOMER PREPARATION
Preparing to route the 3rd and final data center over to Prolexic.

Akamai Experience the Edge

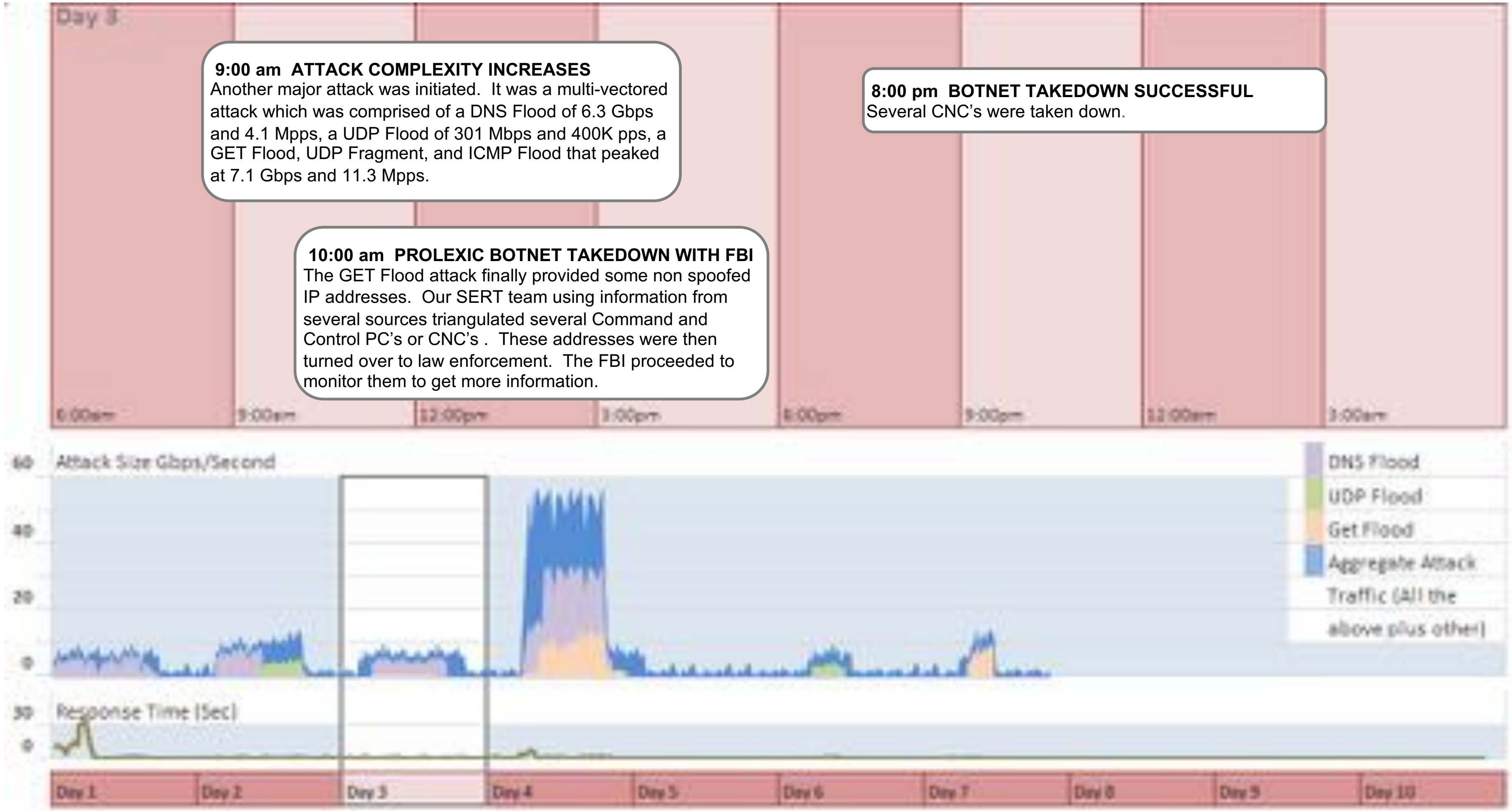
DDoS campaign day 2 – large financial customer



8:30 am ATTACK VECTOR MORPHS TO DNS
Another major attack was initiated. It was a multi-vectored attack which included a DNS Flood and a UDP Flood. The attack peaked out at 13.4 Gbps and 600,000 pps.

10:00 am 100% PROLEXIC MITIGATION
The 3rd and final data center is routed over to Prolexic. All back channels to Web, DNS, VPN's, Custom Apps protected.

DDoS campaign day 3 – large financial customer

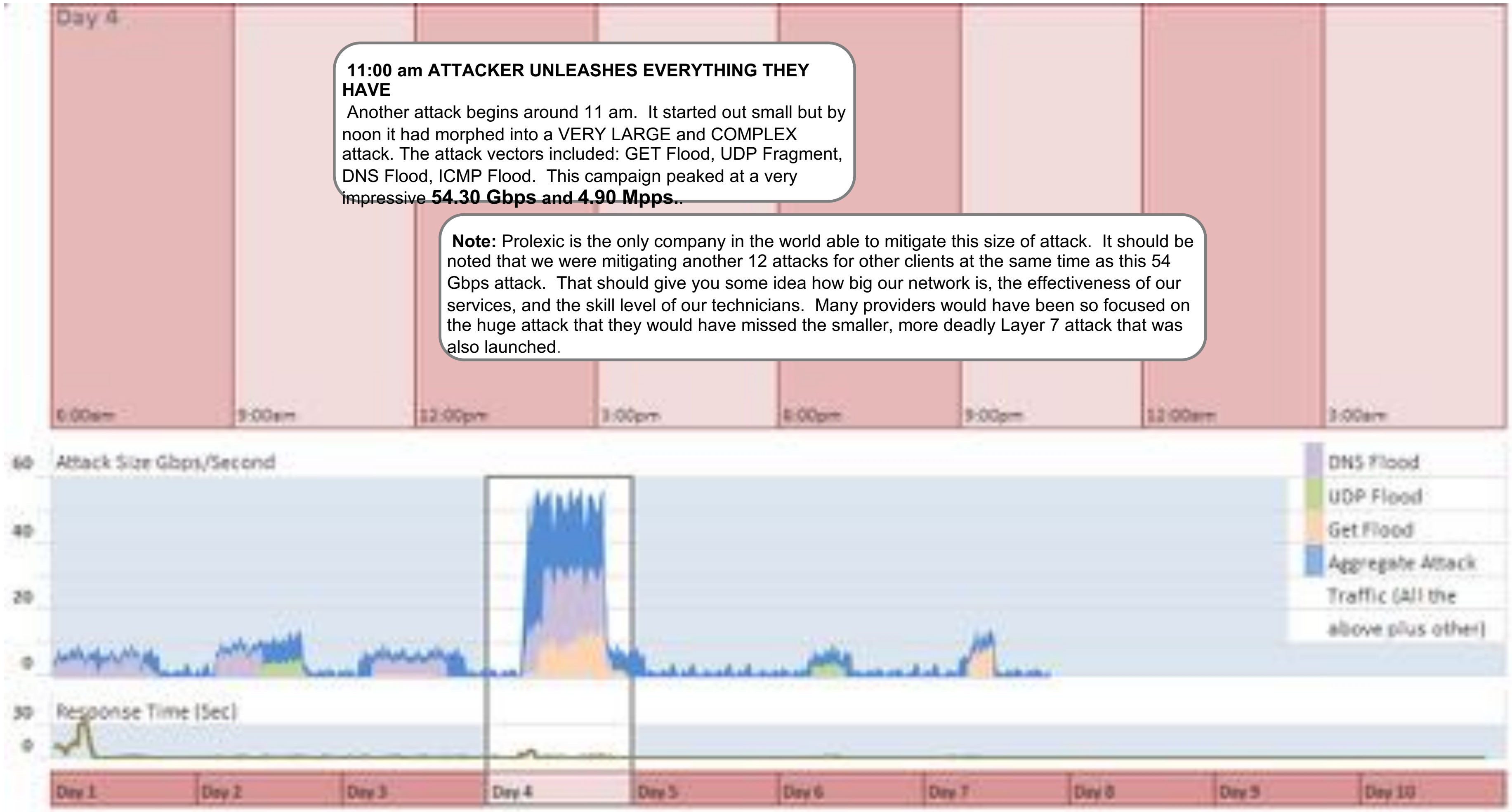


9:00 am ATTACK COMPLEXITY INCREASES
Another major attack was initiated. It was a multi-vectored attack which was comprised of a DNS Flood of 6.3 Gbps and 4.1 Mpps, a UDP Flood of 301 Mbps and 400K pps, a GET Flood, UDP Fragment, and ICMP Flood that peaked at 7.1 Gbps and 11.3 Mpps.

10:00 am PROLEXIC BOTNET TAKEDOWN WITH FBI
The GET Flood attack finally provided some non spoofed IP addresses. Our SERT team using information from several sources triangulated several Command and Control PC's or CNC's . These addresses were then turned over to law enforcement. The FBI proceeded to monitor them to get more information.

8:00 pm BOTNET TAKEDOWN SUCCESSFUL
Several CNC's were taken down.

DDoS campaign day 4 – large financial customer

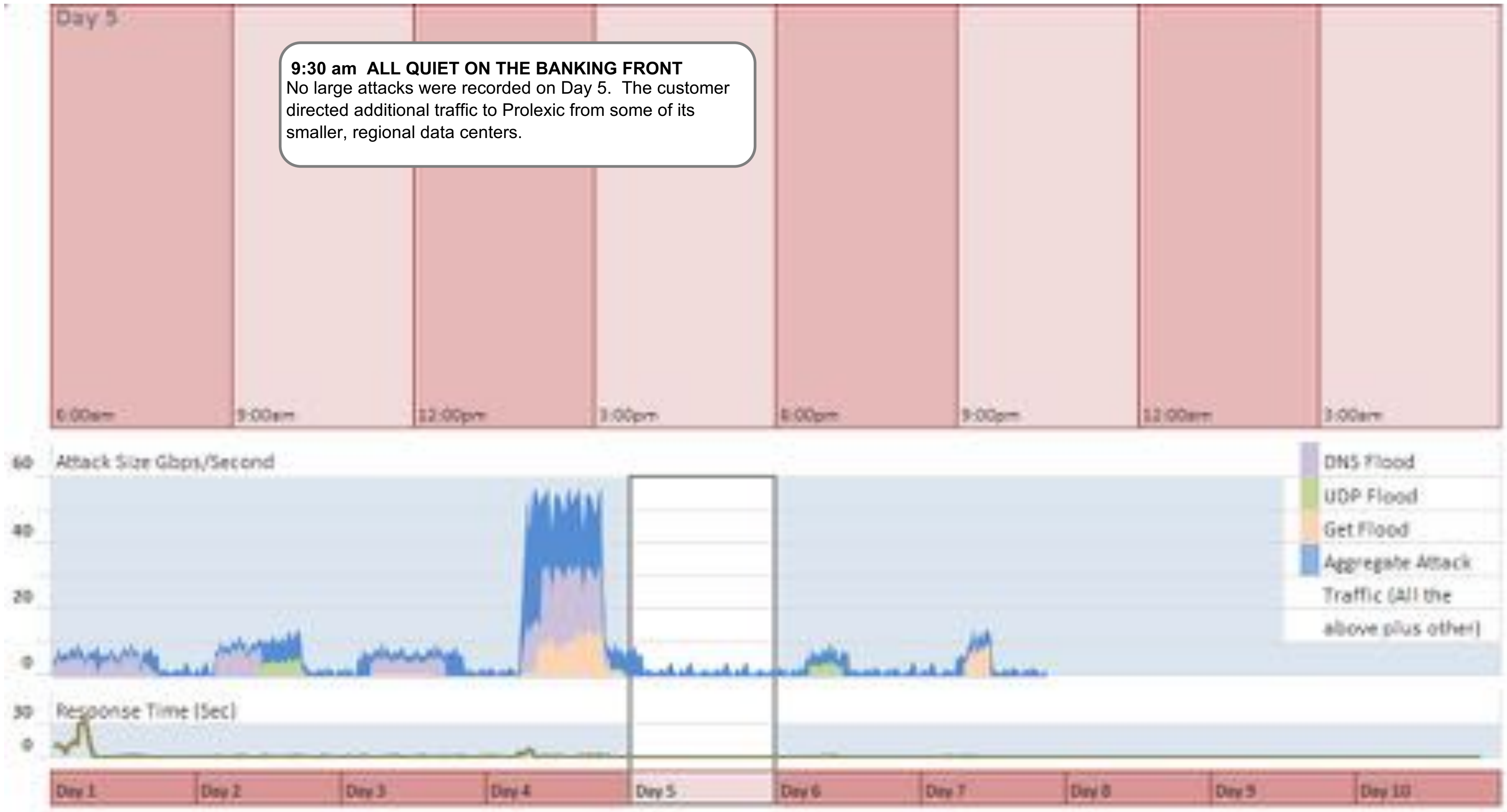


11:00 am ATTACKER UNLEASHES EVERYTHING THEY HAVE

Another attack begins around 11 am. It started out small but by noon it had morphed into a VERY LARGE and COMPLEX attack. The attack vectors included: GET Flood, UDP Fragment, DNS Flood, ICMP Flood. This campaign peaked at a very impressive **54.30 Gbps and 4.90 Mpps.**.

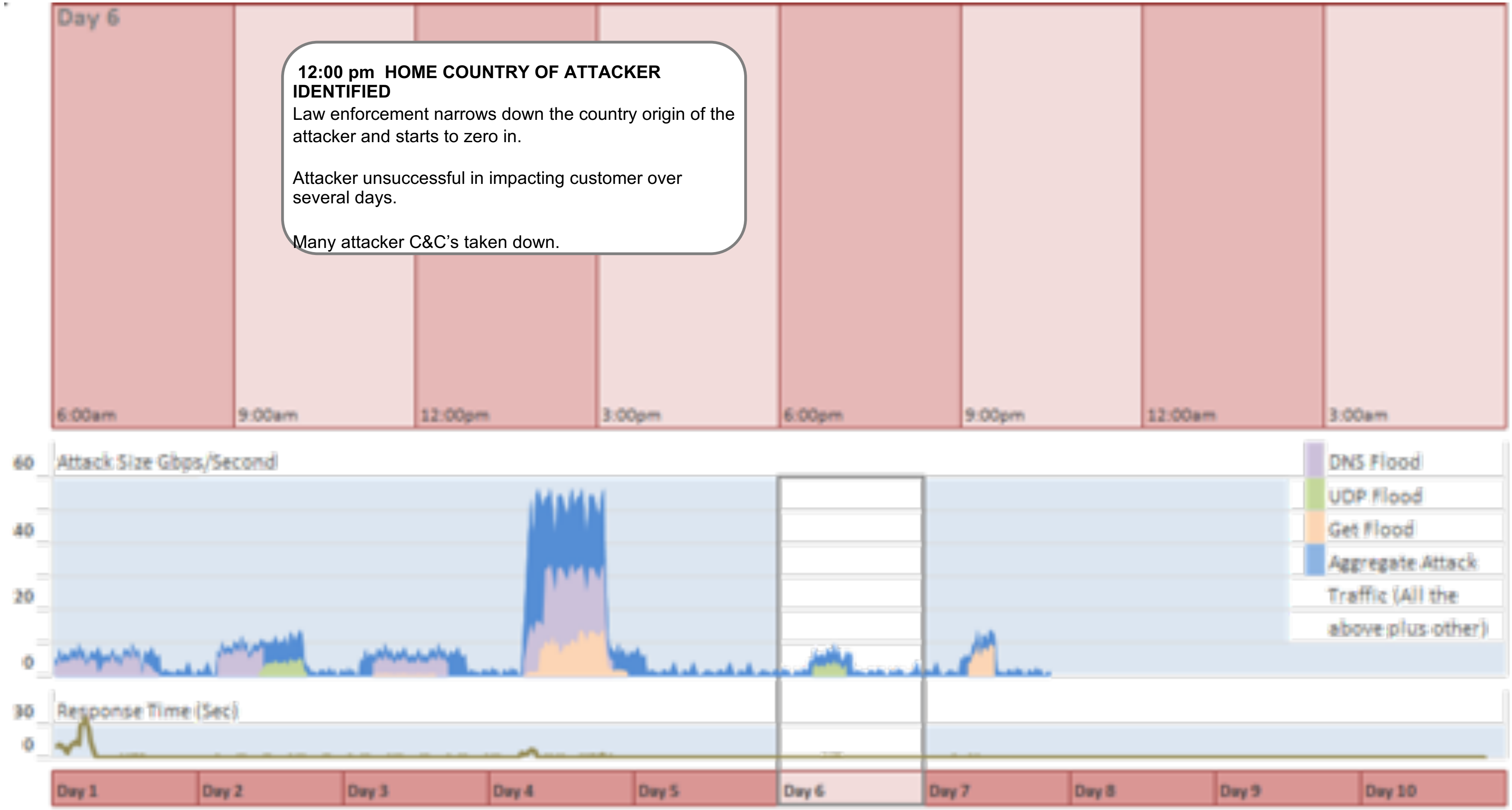
Note: Prolexic is the only company in the world able to mitigate this size of attack. It should be noted that we were mitigating another 12 attacks for other clients at the same time as this 54 Gbps attack. That should give you some idea how big our network is, the effectiveness of our services, and the skill level of our technicians. Many providers would have been so focused on the huge attack that they would have missed the smaller, more deadly Layer 7 attack that was also launched.

DDoS campaign day 5 – large financial customer



9:30 am ALL QUIET ON THE BANKING FRONT
No large attacks were recorded on Day 5. The customer directed additional traffic to Prolexic from some of its smaller, regional data centers.

DDoS campaign day 6 – large financial customer



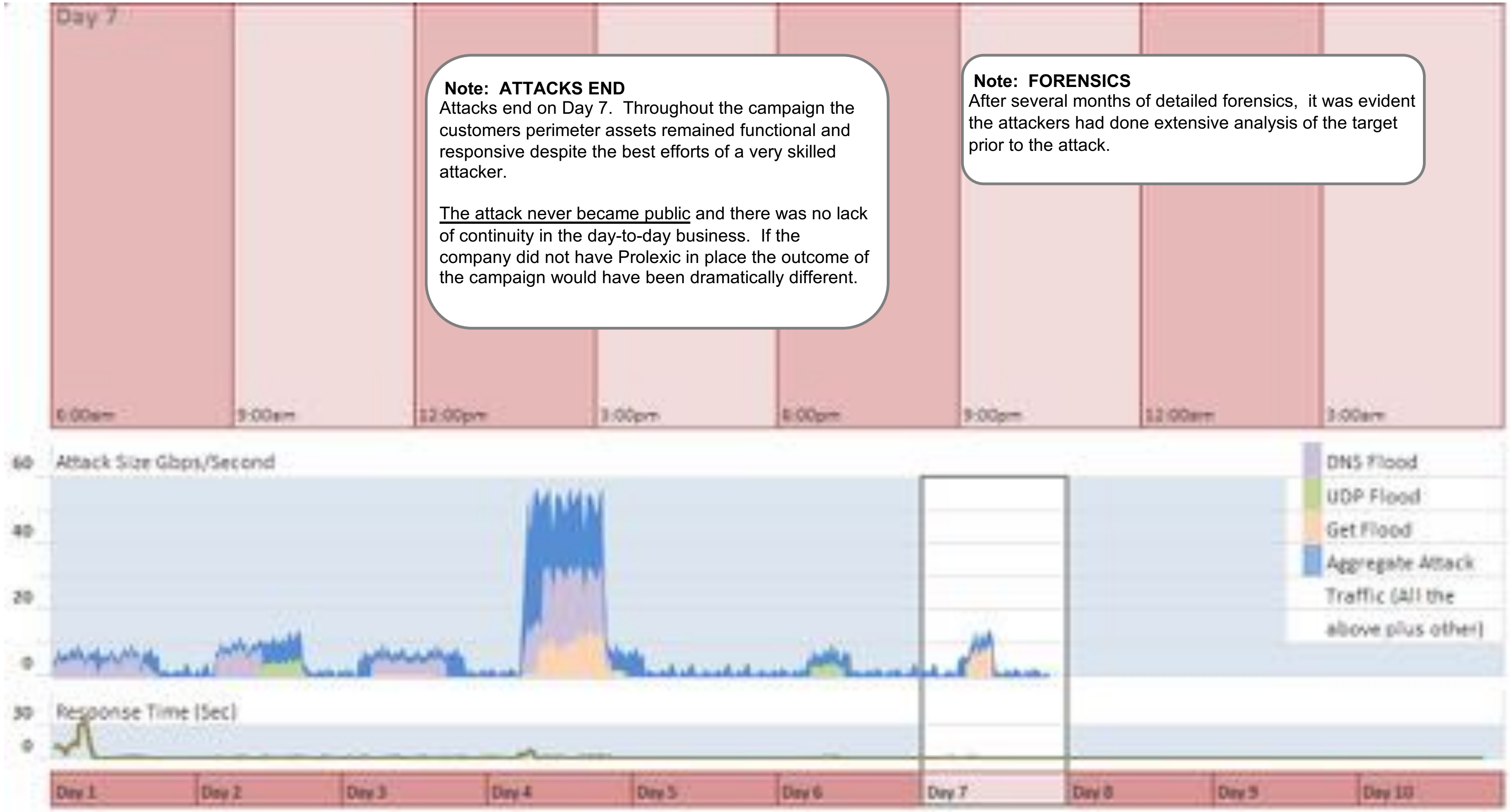
12:00 pm HOME COUNTRY OF ATTACKER IDENTIFIED

Law enforcement narrows down the country origin of the attacker and starts to zero in.

Attacker unsuccessful in impacting customer over several days.

Many attacker C&C's taken down.

DDoS campaign day 7 – large financial customer



Note: ATTACKS END
Attacks end on Day 7. Throughout the campaign the customers perimeter assets remained functional and responsive despite the best efforts of a very skilled attacker.

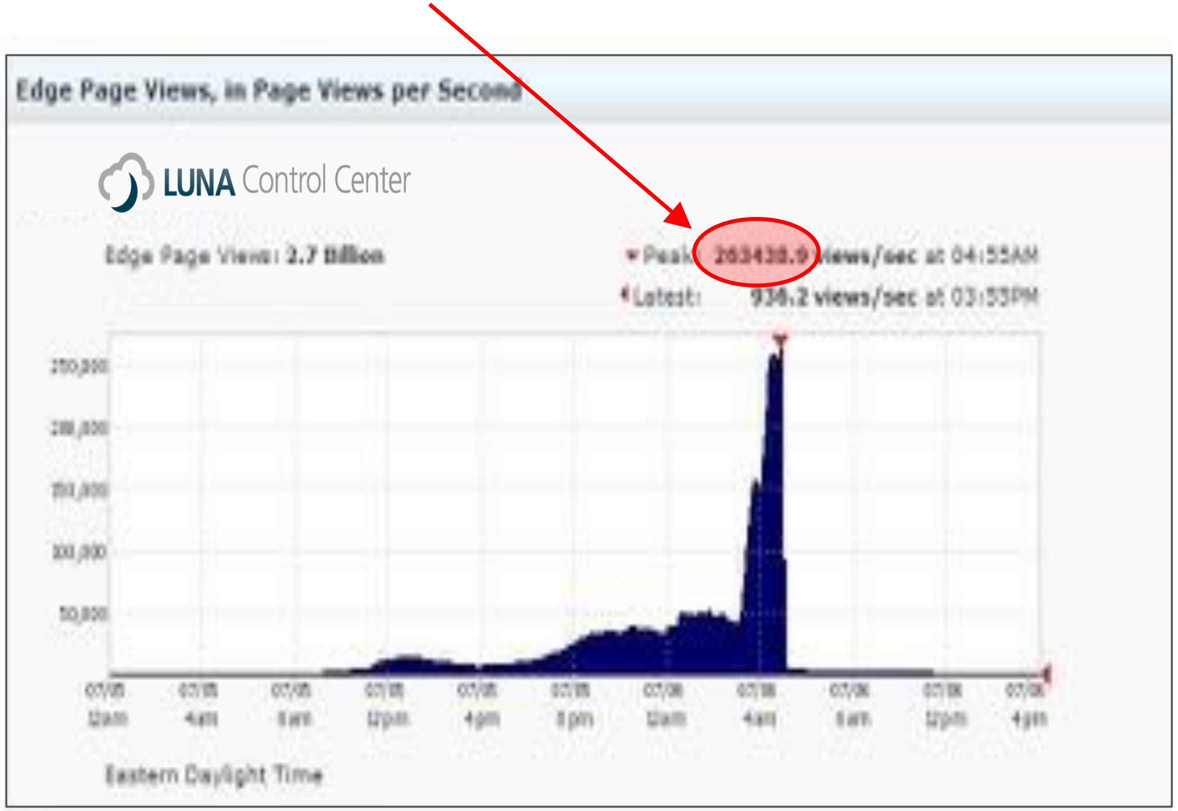
The attack never became public and there was no lack of continuity in the day-to-day business. If the company did not have Prolexic in place the outcome of the campaign would have been dramatically different.

Note: FORENSICS
After several months of detailed forensics, it was evident the attackers had done extensive analysis of the target prior to the attack.

Case Study – Stock Exchange DDoS Attack

Reducing Risk, Protecting the Brand

- Attack on Akamai stock exchange customer.
- Peak attack traffic was 26 Gbps, 170x normal.
- Page Views peaked at over 260,000 per second, 280x normal.



Edge Page Views, in Page Views per Second

Edge Page Views: 2.7 Billion

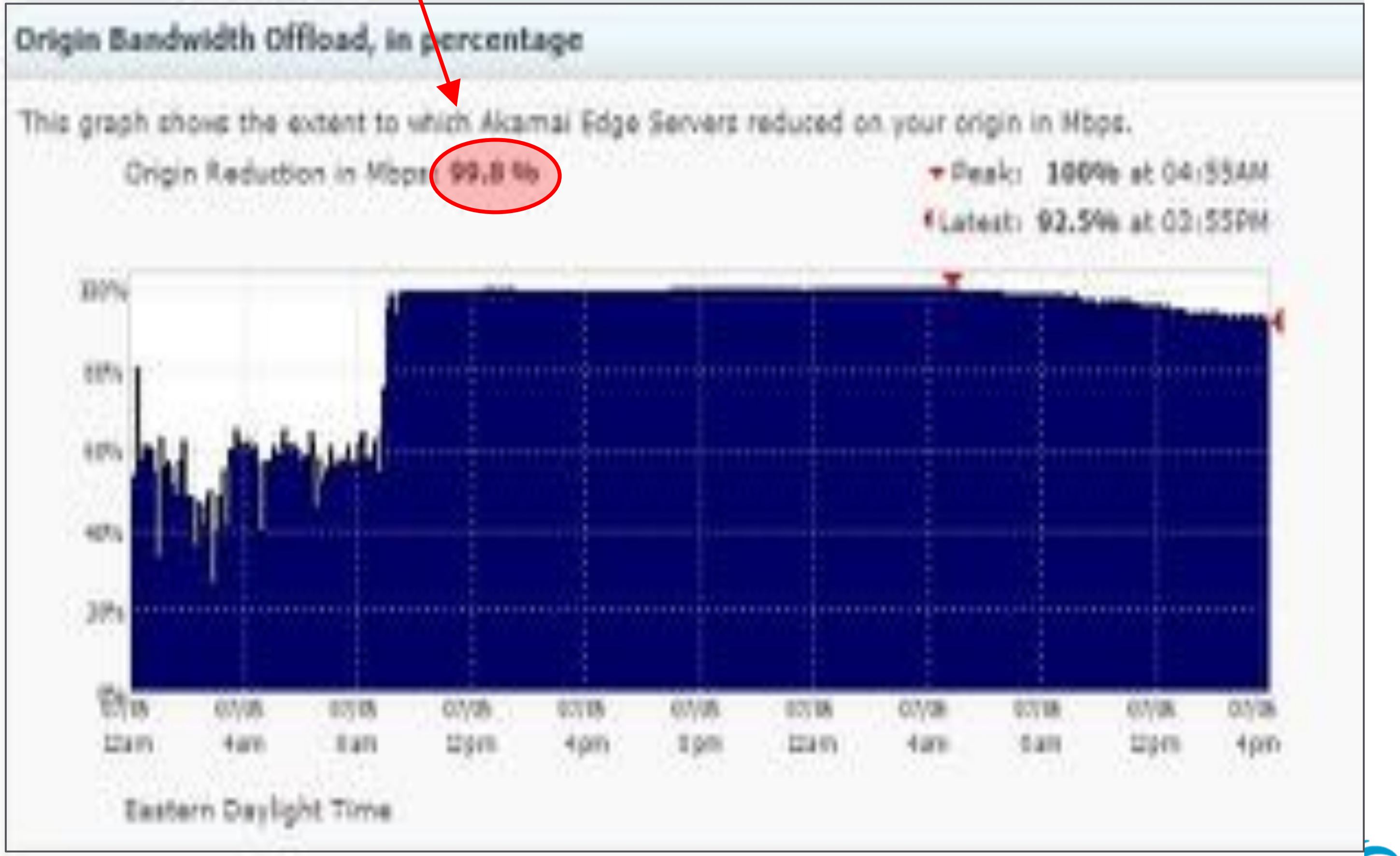
▾Peak: 263430.9 views/sec at 04:55AM

◂Latest: 936.2 views/sec at 03:53PM

Eastern Daylight Time

DDoS Attack – Stock Exchange

- Akamai Offloaded over 99% of bandwidth during the attack, protecting the site.
- Origin bandwidth peaked at only 53 Mbps.



Origin Bandwidth Offload, in percentage

This graph shows the extent to which Akamai Edge Servers reduced on your origin in Mbps.

Origin Reduction in Mbps: 99.8 %

▼Peak: **100%** at 04:55AM

◀Latest: **92.5%** at 03:55PM

Eastern Daylight Time

Operation Ababil

> *“none of the U.S banks will be safe from our attacks”*

Phase 1

Sep 12 – Early Nov 2012

- DNS Packets with “A” payload
- Limited Layer 7 attacks
- Began use of HTTP dynamic content to circumvent static caching defenses

Phase 2

Dec 12, 2012 – Jan 29

- Incorporate random query strings and values
- Additions to bot army
- Burst probes to bypass rate-limiting controls
- Addition of valid argument names, random values

Phase 3

Late Feb 2013 – May 2013

- Increased focus on Layer 7 attacks
- Larger botnet
- Highly distributed
- Target banks where attacks work
- Fraudsters take advantage

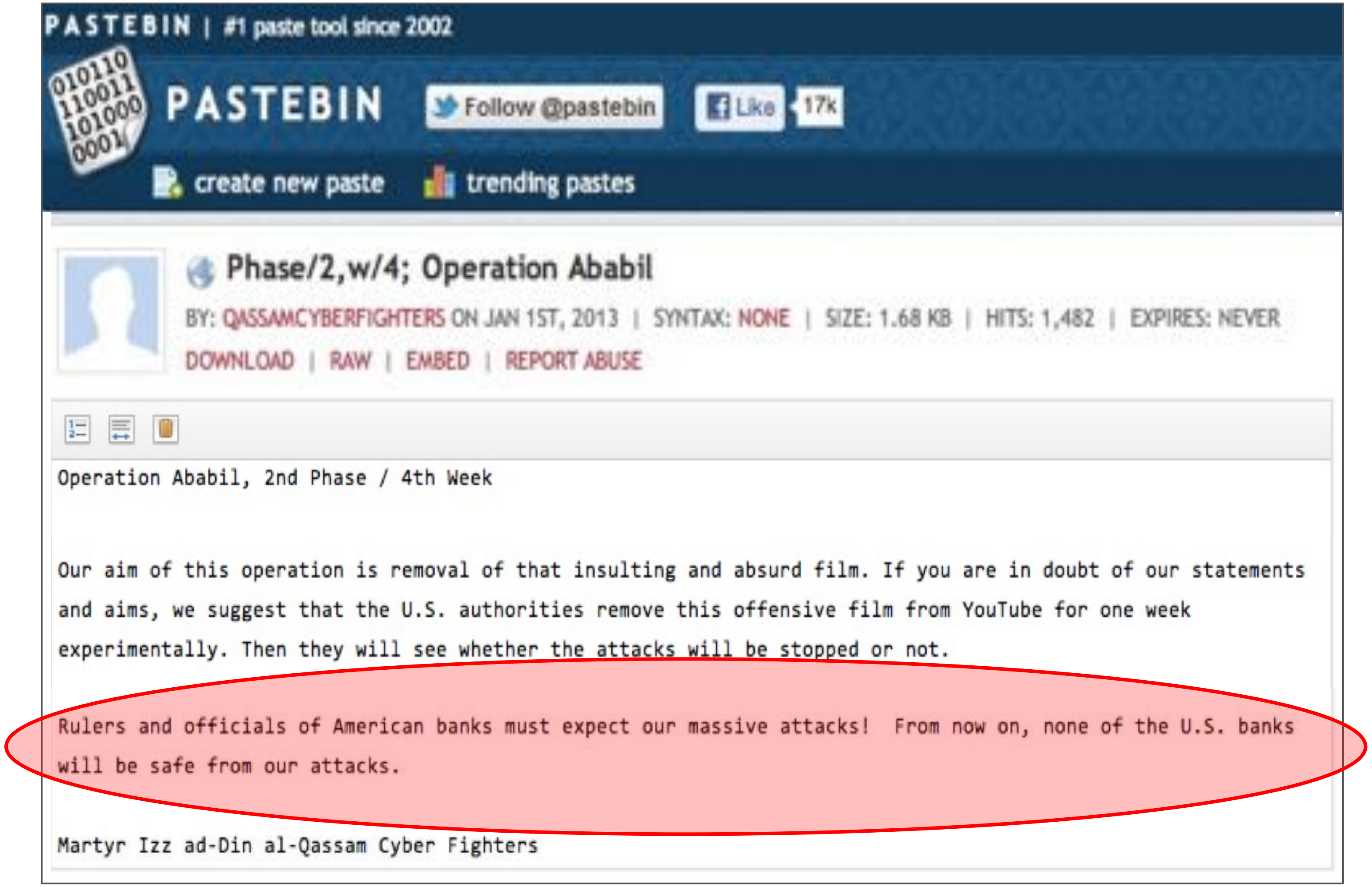
Phase 4

July 2013 – Now

- Updated attack scripts, harder to understand
- Requests look more like normal browsers

Operation Ababil / 2nd Phase / 4th Week

"none of the U.S banks will be safe from our attacks."



Phase/2,w/4; Operation Ababil

BY: QASSAMCYBERFIGHTERS ON JAN 1ST, 2013 | SYNTAX: NONE | SIZE: 1.68 KB | HITS: 1,482 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE

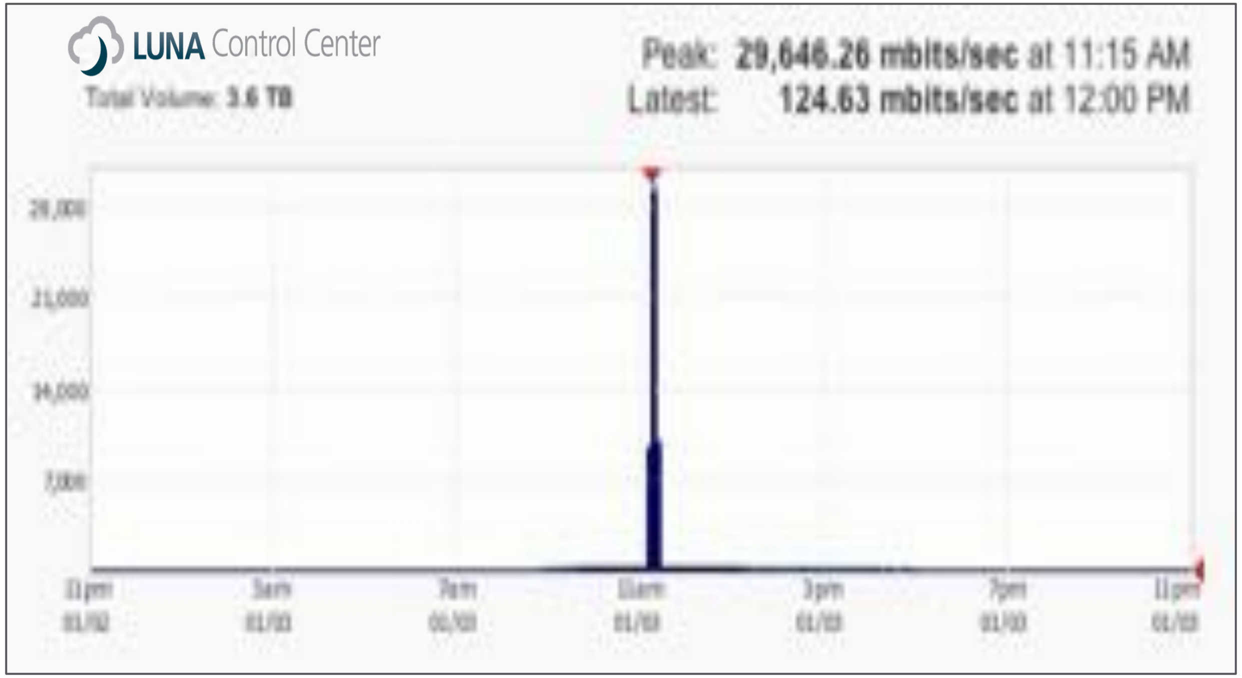
```
Operation Ababil, 2nd Phase / 4th Week


Our aim of this operation is removal of that insulting and absurd film. If you are in doubt of our statements
and aims, we suggest that the U.S. authorities remove this offensive film from YouTube for one week
experimentally. Then they will see whether the attacks will be stopped or not.

Rulers and officials of American banks must expect our massive attacks!  From now on, none of the U.S. banks
will be safe from our attacks.

Martyr Izz ad-Din al-Qassam Cyber Fighters
```

January 3, 2013 – Massive Banking DDoS Attack

Always-on Protection

Bank #1

- Top financial services firm with nearly 10M customers.
- Peak attack traffic was 30 Gbps, 30x normal daily high traffic.
- Attackers gave up after 15 minutes, and moved attack to another bank.
- 100% of the attack was on SSL.



LUNA Control Center

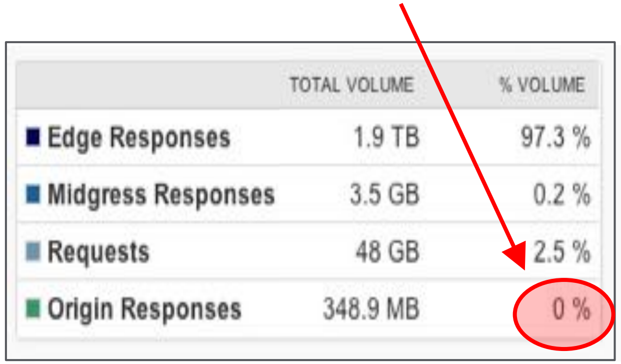
Total Volume: 3.6 TB

Peak: 29,646.26 mbits/sec at 11:15 AM
Latest: 124.63 mbits/sec at 12:00 PM

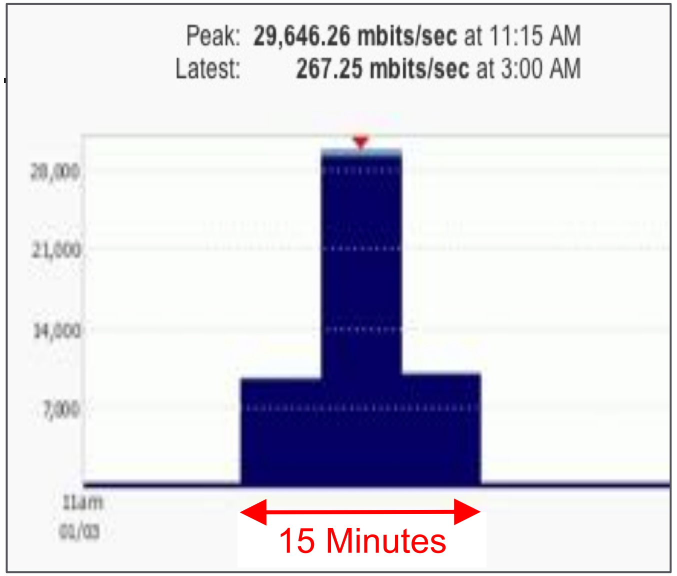
Massive Banking DDoS Attack

Bank #1

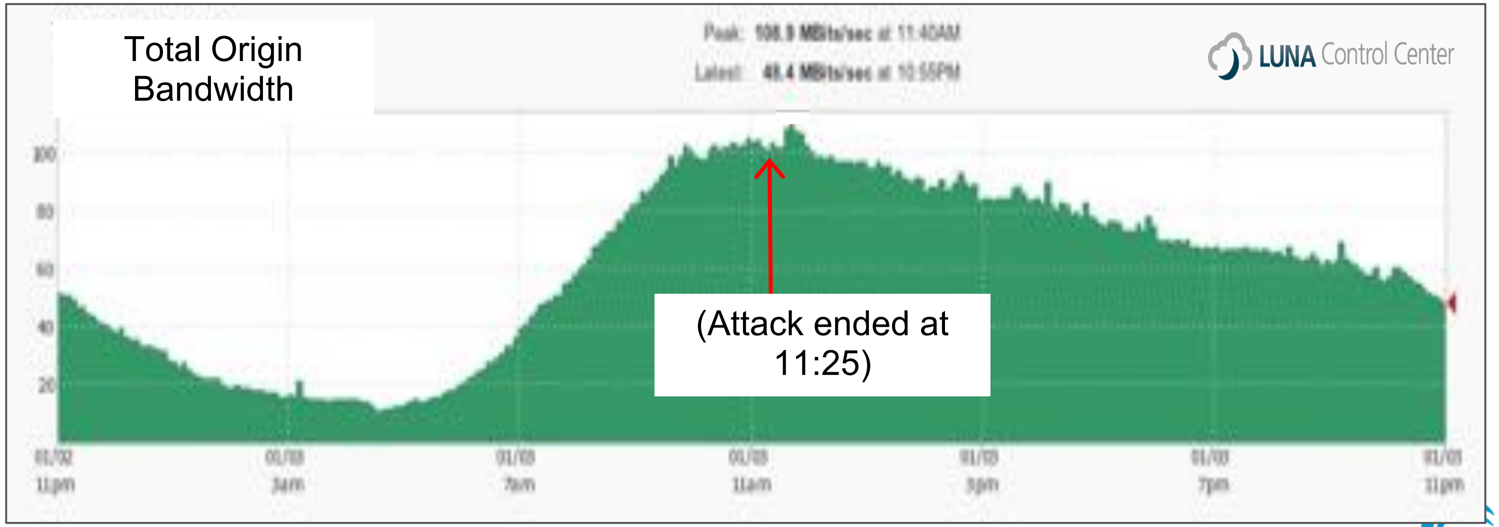
- Akamai offloaded 100% of the attack.



	TOTAL VOLUME	% VOLUME
■ Edge Responses	1.9 TB	97.3 %
■ Midgress Responses	3.5 GB	0.2 %
■ Requests	48 GB	2.5 %
■ Origin Responses	348.9 MB	0 %

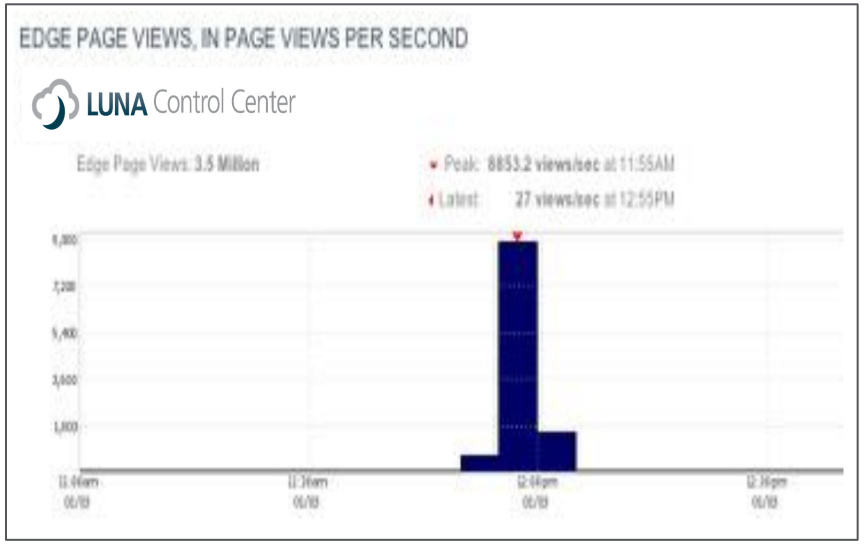


- “A bug impacting our windshield”.



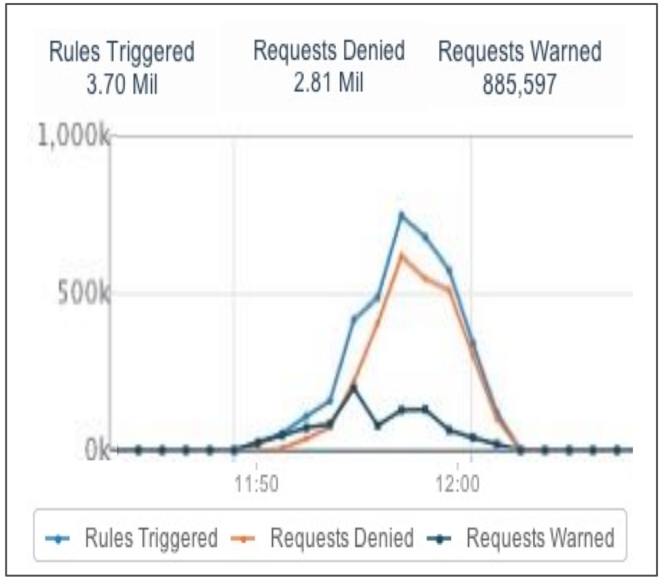
Massive Banking DDoS Attack

- “Probe” attack was then seen at another bank 25 minutes later.



Bank #2

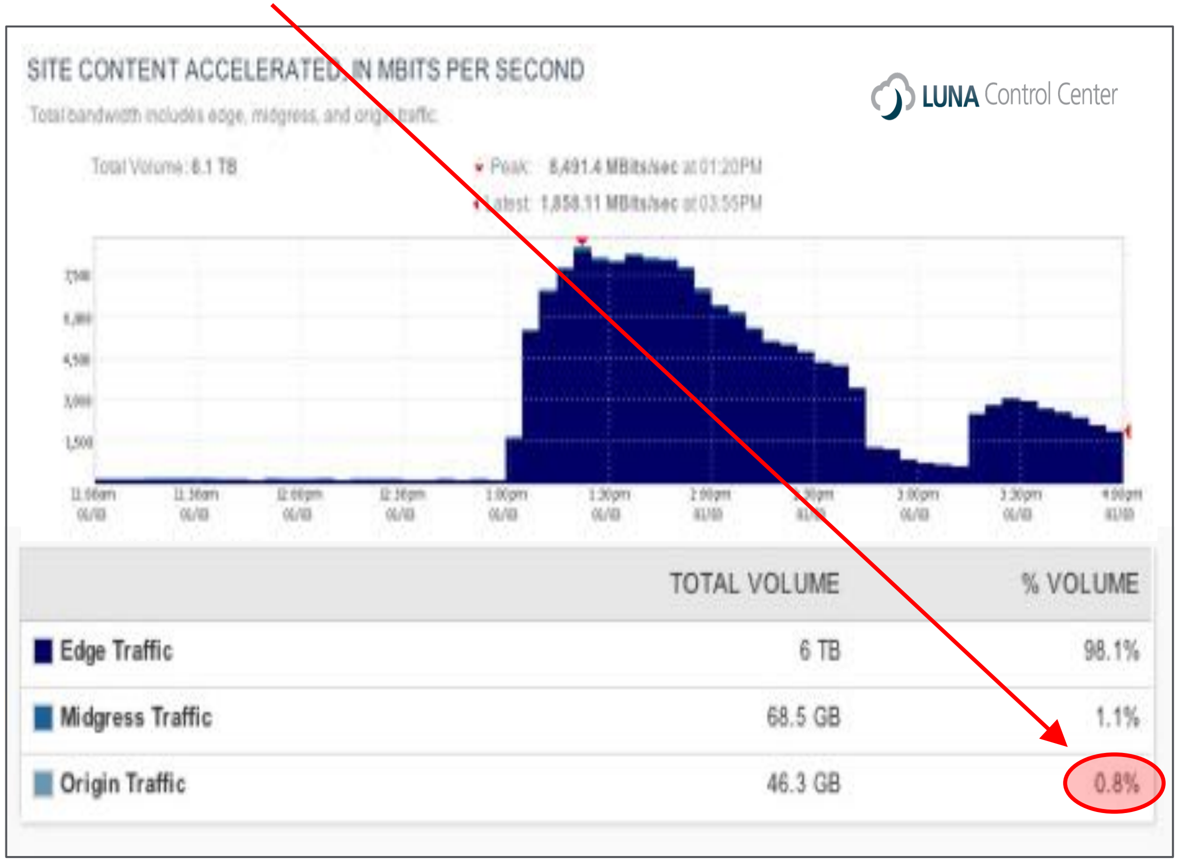
- Akamai Kona in place, and rate controls automatically activated.



Massive Banking DDoS Attack

Bank #3

- 60 minutes later, 8 Gbps attack seen on a 3rd customer.
- 100% of the attack was on SSL.
- Akamai offload was over 99%



SITE CONTENT ACCELERATED IN MBITS PER SECOND

Total bandwidth includes edge, midgress, and origin traffic

Total Volume: 8.1 TB

Peak: 8,491.4 MBits/sec at 01:20PM

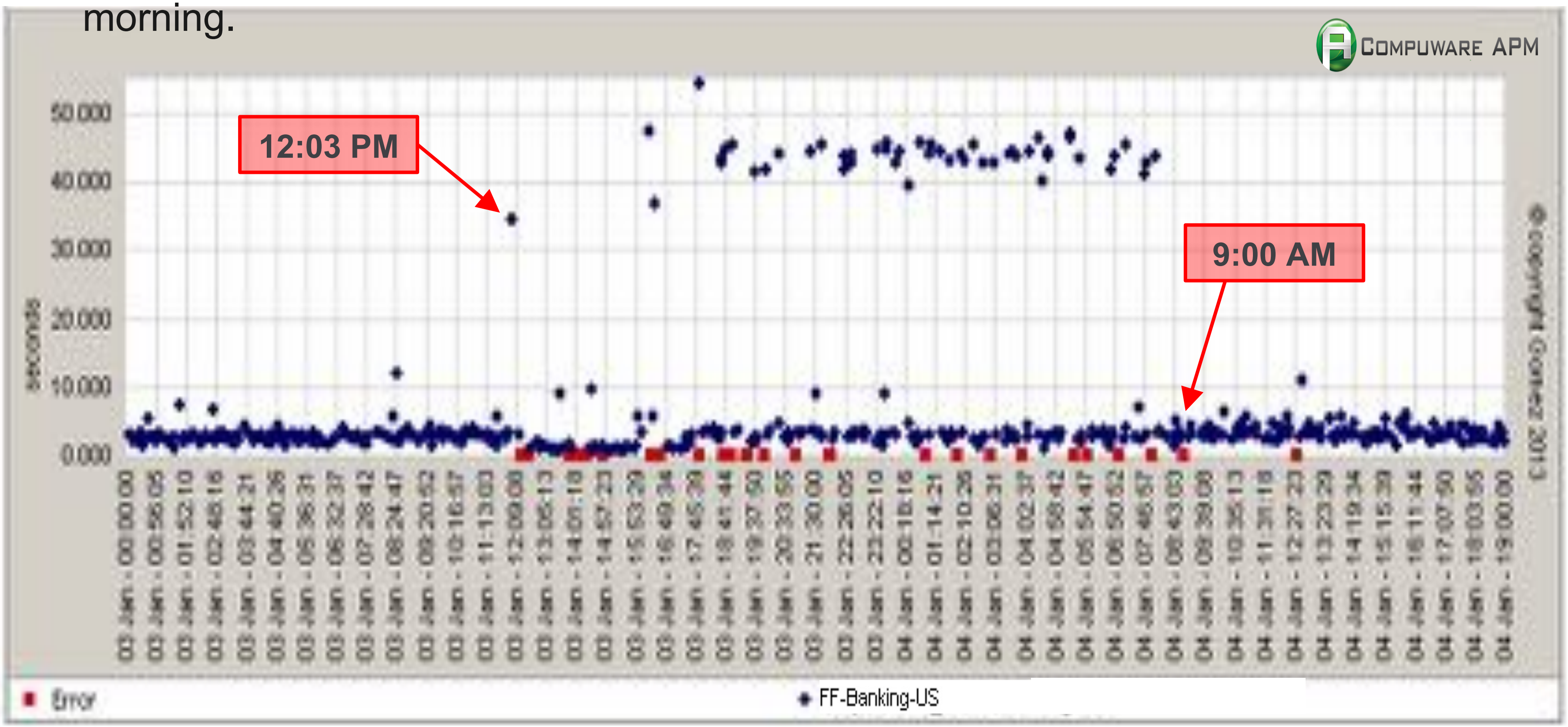
Latest: 1,858.11 MBits/sec at 03:55PM

	TOTAL VOLUME	% VOLUME
■ Edge Traffic	6 TB	98.1%
■ Midgress Traffic	68.5 GB	1.1%
■ Origin Traffic	46.3 GB	0.8%

Non-Akamai bank hit at 12:03 PM

Bank #4

- Compuware benchmark of bank home page, measured from 12 cities 1x p hour.
- First performance hit recorded at 12:03 PM.
- Performance and availability problems continued to 9:00 AM the following morning.



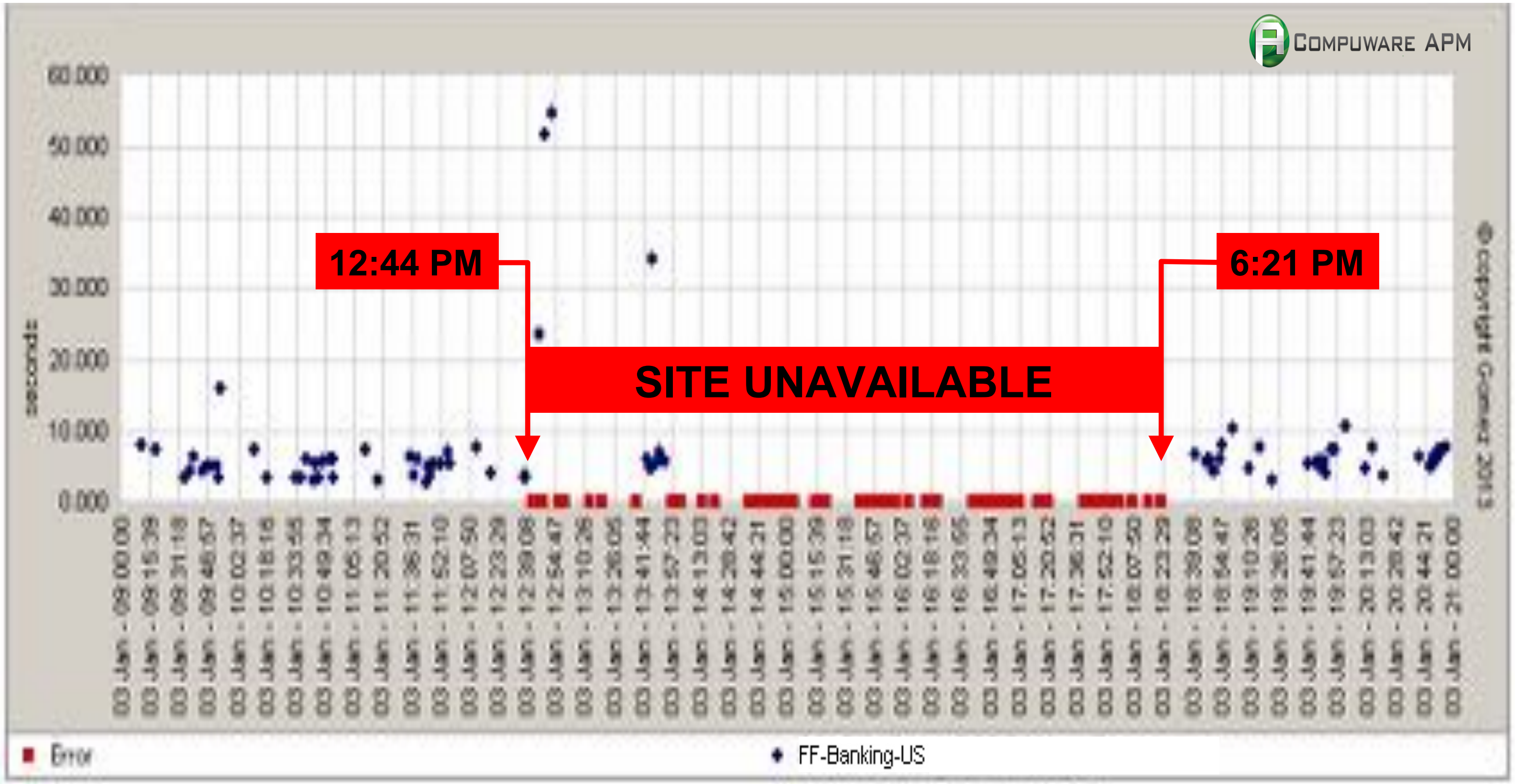
12:03 PM

9:00 AM

Non-Akamai bank attacked at 12:44 PM

Bank #5

- First outage recorded at 12:44 PM.
- Attack continued to 6:21 PM.
- Bank attacked numerous times after January 3.



12:44 PM

SITE UNAVAILABLE

6:21 PM

Questions?

Gracias !

Greivin Viquez
gviqueza@akamai.com
+506 83 28 65 65