War Stories from the Cloud –
Going Behind the Web Security Headlines

Emmanuel Mace
Security Expert

Akamai
FASTER FORWARD

The leading cloud platform for enabling secure, high-performing user experiences on any device, anywhere.

ABOUT US:

- Distributed cloud platform, on-demand scale
- Delivering 15-30% of all daily web traffic
- 2 trillion cloud interactions daily
- 150M mobile apps delivered daily
- Defending against attacks over 200Gbps
- Enabling >$250 billion in annual e-commerce
- A single network hop from 90% of internet users

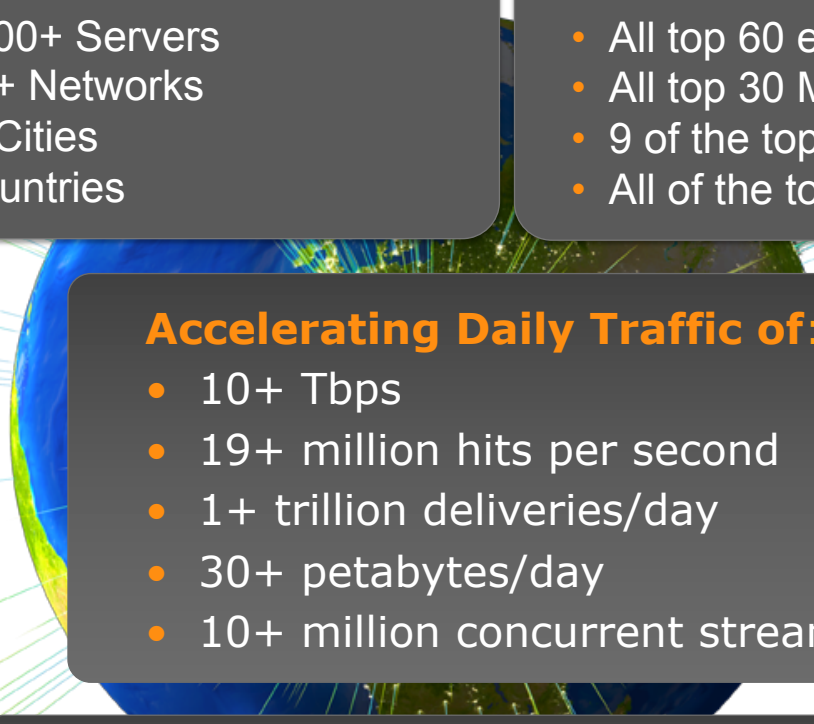
CORP STATS:

$1.3B Revenue	2,000 Locations	4,000 Customers	3,000 Employees

OUR HISTORY:

Founded 1998 and rooted in MIT technology—solving Internet congestion with math not hardware.

The Akamai Intelligent Platform



A Global Platform:

- 147,000+ Servers
- 1,100+ Networks
- 650+ Cities
- 82 Countries

Delivering 130,000+ Domains

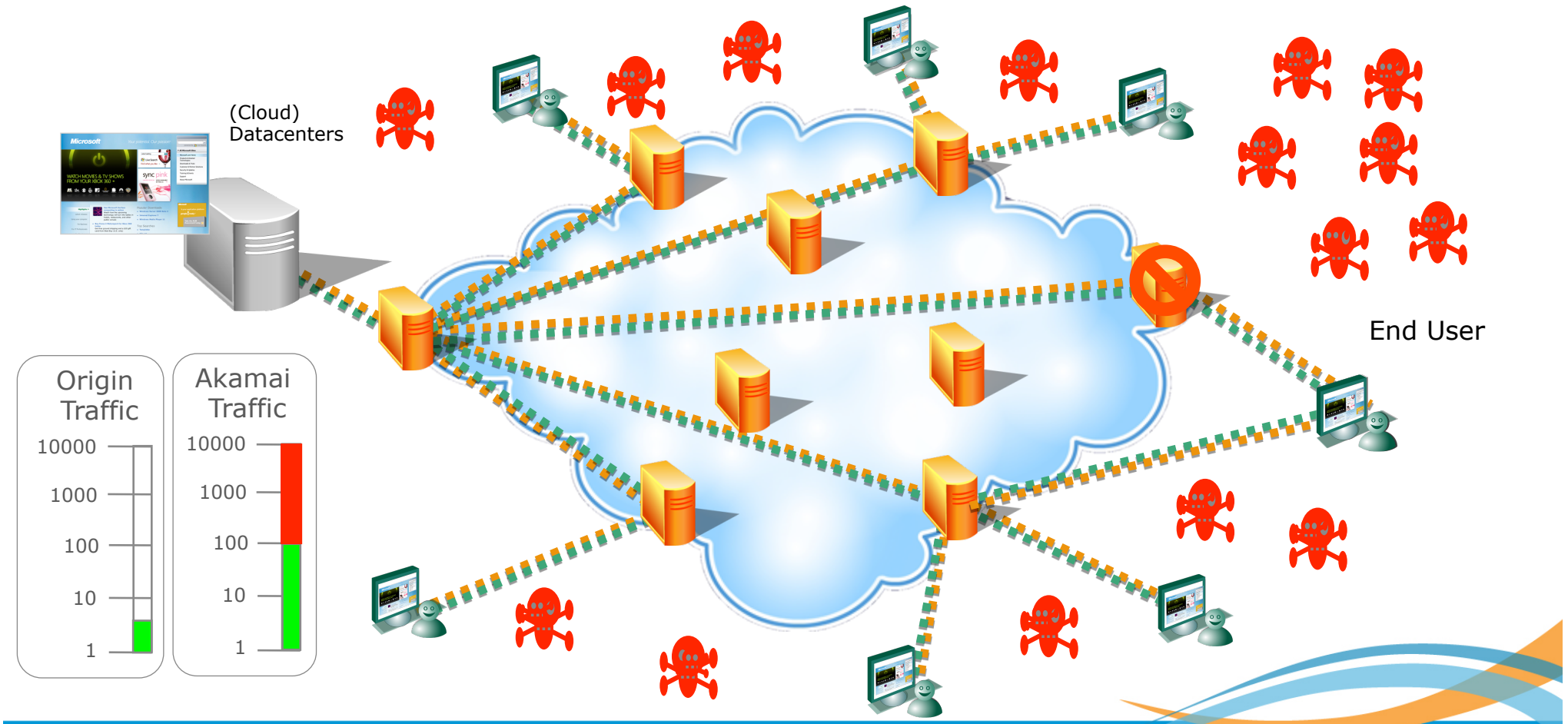
- All top 60 eCommerce sites
- All top 30 M&E companies
- 9 of the top 10 banks
- All of the top Internet portals

Accelerating Daily Traffic of:

- 10+ Tbps
- 19+ million hits per second
- 1+ trillion deliveries/day
- 30+ petabytes/day
- 10+ million concurrent streams

15–30+% of Web Traffic

The Akamai Platform Provides a Perimeter Defense



Attacks on Akamai Customers

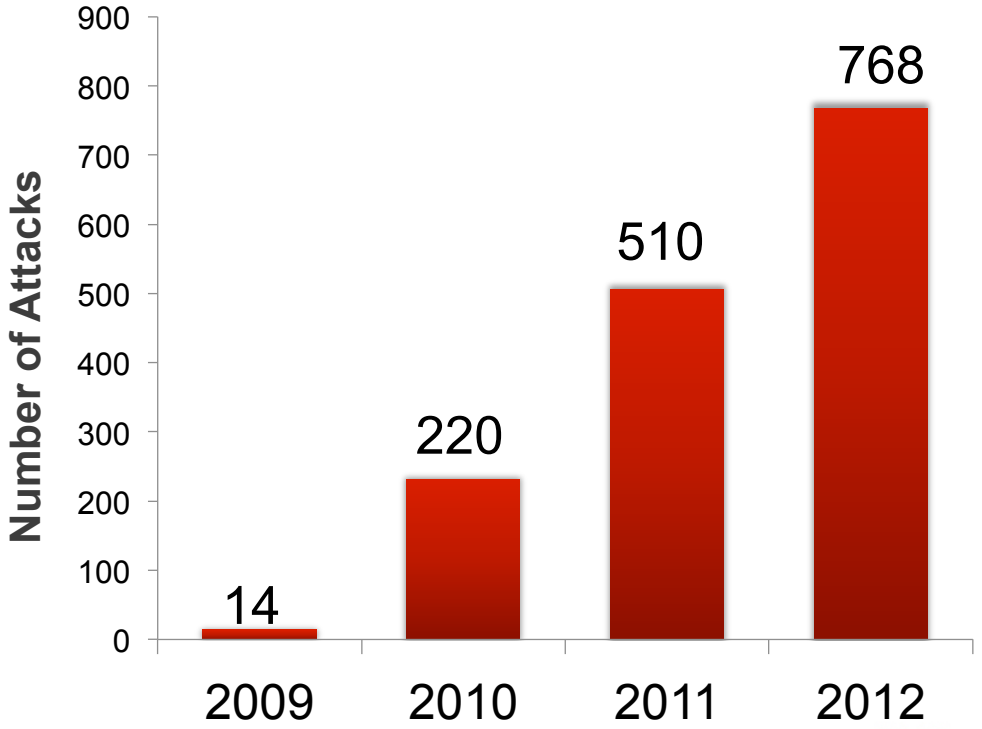
Typical Attack Size

10 Gbps

Large Attack Size

100+ Gbps

Attacks are originating from all geographies and are moving between geographies during the attack



Attack Trends in 2013

DDoS attacks have evolved

- "Volumetric" to "low & slow"

Volumetric attacks are more sophisticated

More attacks focus on the application

Application attacks evolve to look more like real users

More Attacks

Smarter Attacks

Better Reconnaissance

Better Targeting

Operation Ababil

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

Phase 1	Phase 2	Phase 3	Phase 4
Sep 12 – Early Nov 2012	Dec 12, 2012 – Jan 29	Late Feb 2013 – May 2013	July 2013 – Now
• DNS Packets with "A" payload • Limited Layer 7 attacks • Began use of HTTP dynamic content to circumvent static caching defenses	• Incorporate random query strings and values • Additions to bot army • Burst probes to bypass rate-limiting controls • Addition of valid argument names, random values	• Increased focus on Layer 7 attacks • Larger botnet • Highly distributed • Target banks where attacks work • Fraudsters take advantage	• Updated attack scripts, harder to understand • Requests look more like normal browsers

Phase 1 Attack – Sept 2012

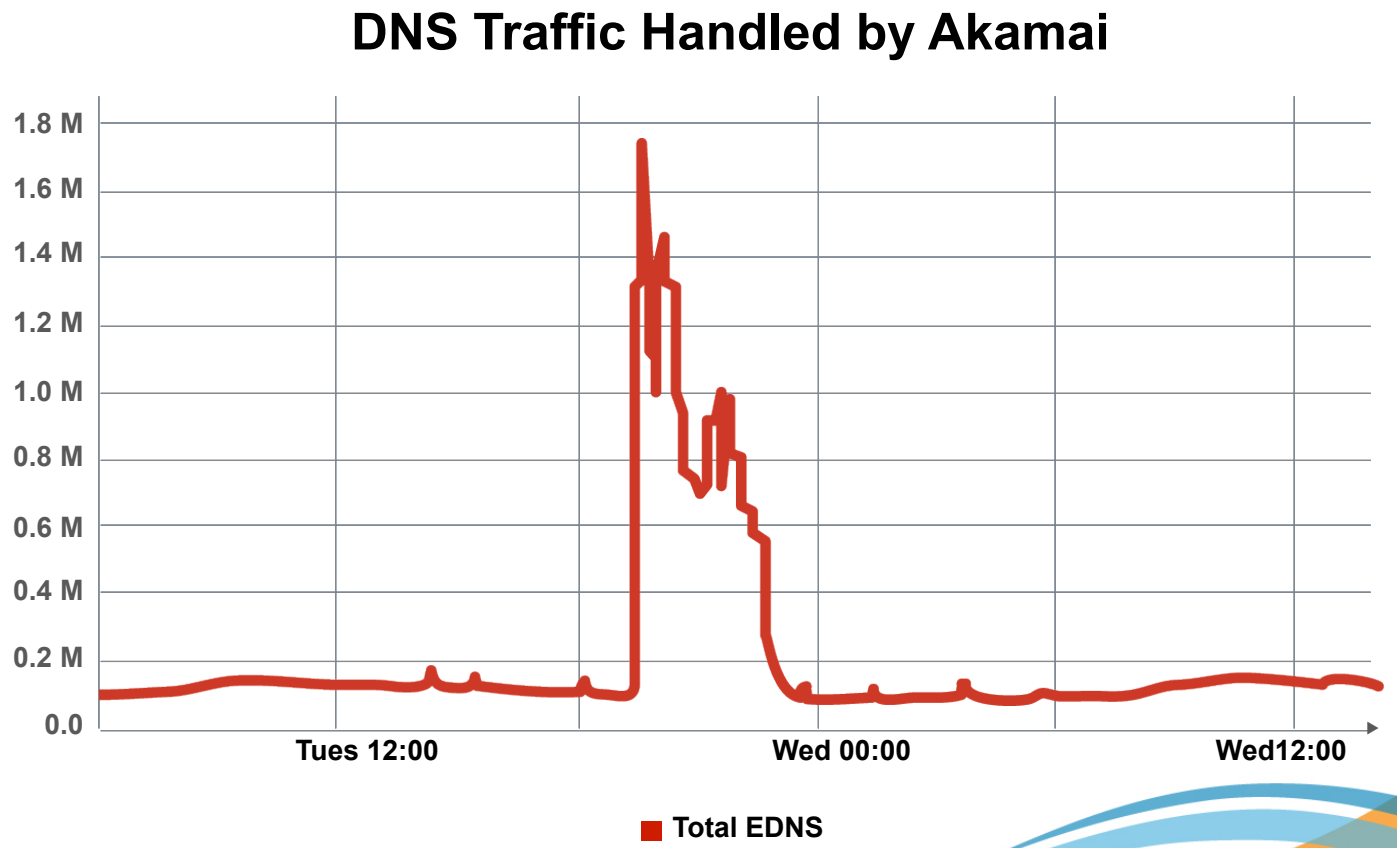
Attack Traffic:

23 Gbps

(10,000X normal)

Duration:

4.5 Hours



Phase 2 Attacks - January 2nd, 2013

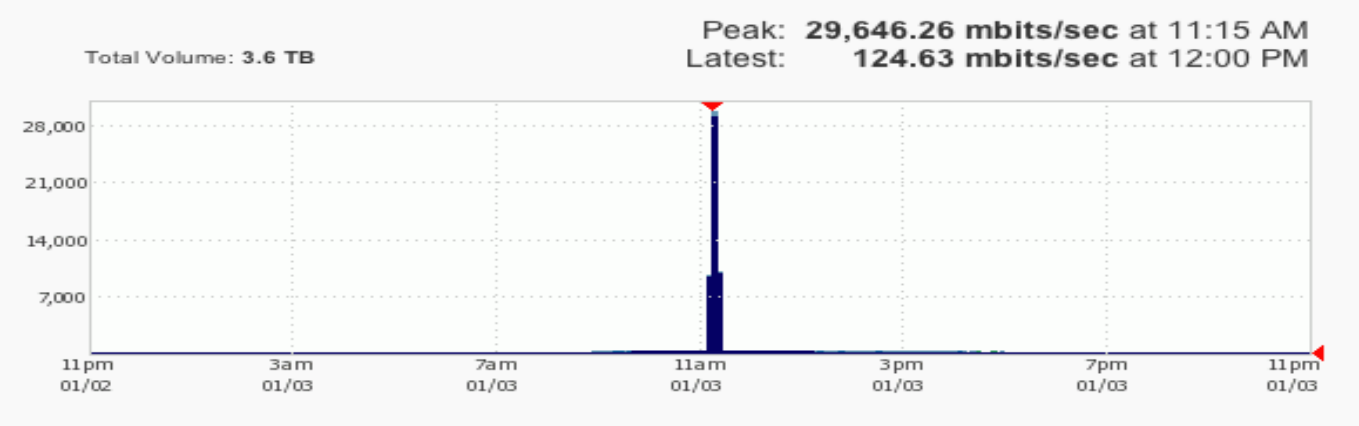
Bank #1

Bank #2

Bank #3

Bank #4

Bank #5



QCF targeted PDF files

Akamai Dynamic Caching Rules offloaded 100% of the traffic

No Origin Impact

	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 %

Phase 2 Attacks - January 2nd, 2013

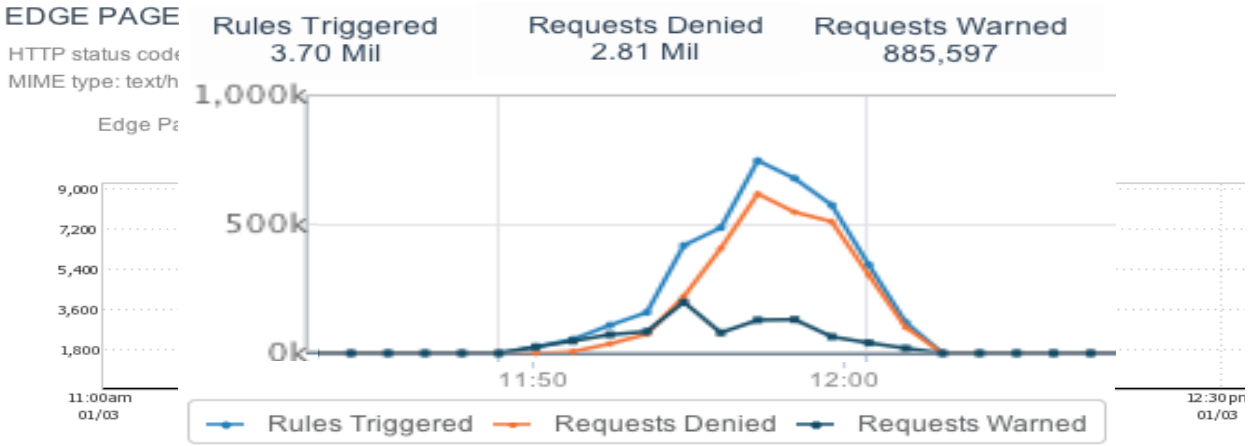
Bank #1

Bank #2

Bank #3

Bank #4

Bank #5



QCF targeted marketing web pages

Rate controls automatically activated
Attack was deflected, far from bank's datacenter

No Origin Impact

Phase 2 Attacks - January 2nd, 2013

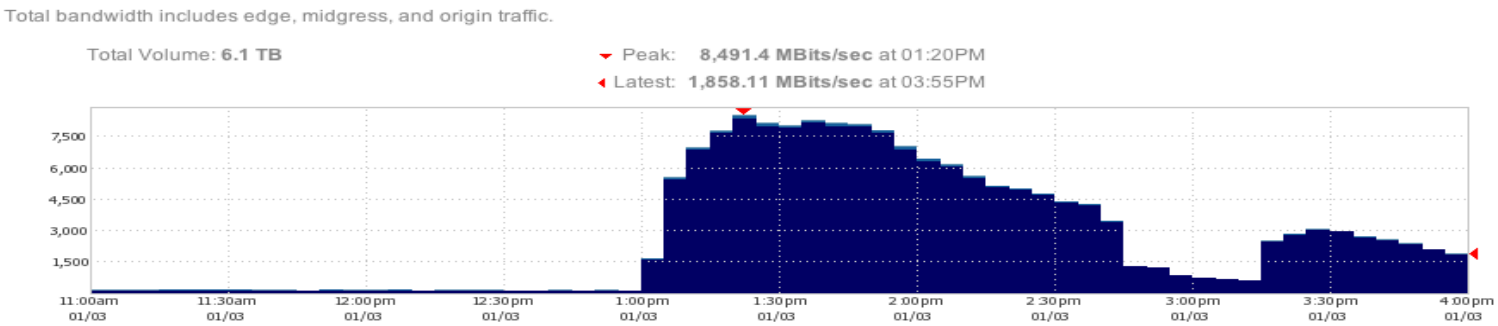
Bank #1

Bank #2

Bank #3

Bank #4

Bank #5



QCF targeted SSL

Akamai offloaded 99% of the traffic

No Origin Impact

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

Phase 2 Attacks - January 2nd, 2013

Bank #1

Bank #2

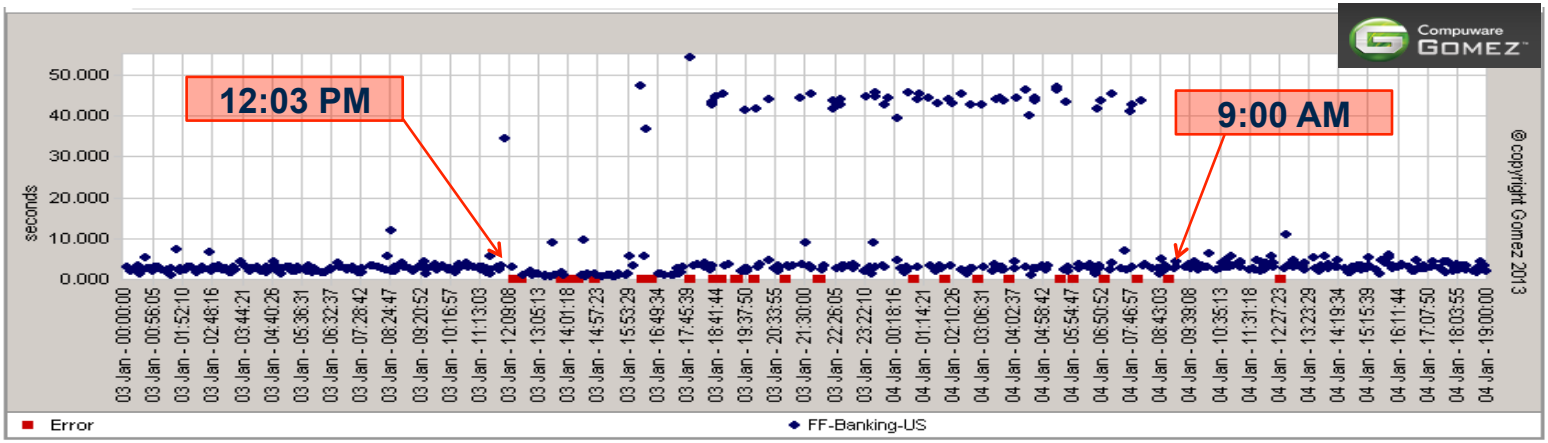
Bank #3

Bank #4

Bank #5

NOT on Akamai

Gomez agents in 12 cities measuring hourly



Error/Outage—site not responding

Phase 2 Attacks - January 2nd, 2013

Bank #1

Bank #2

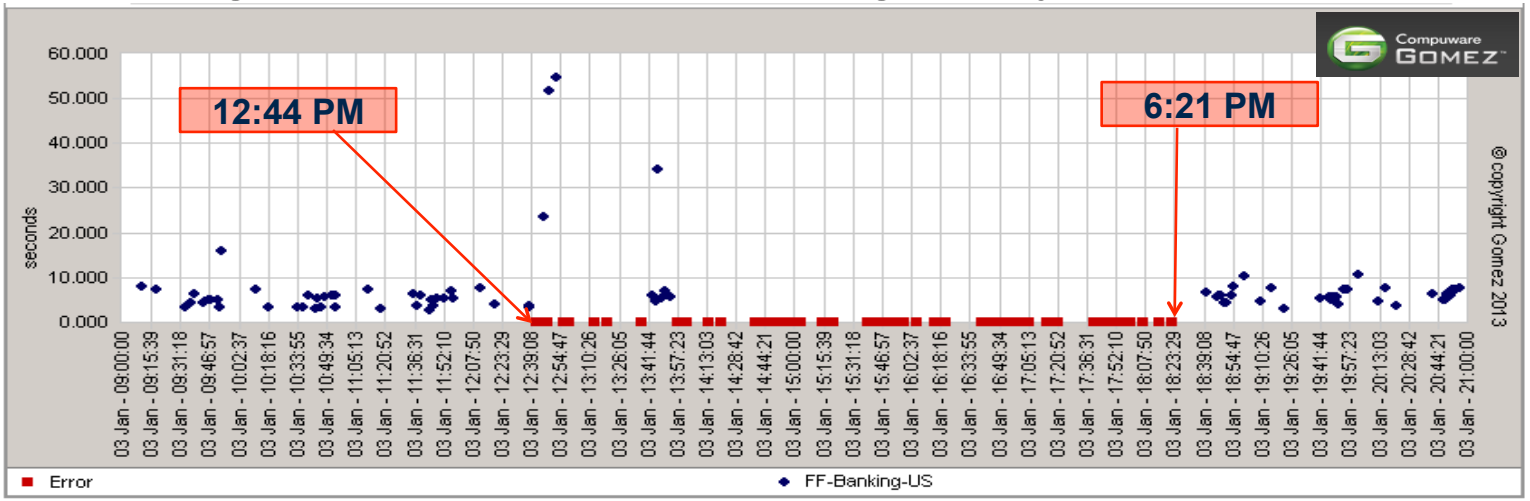
Bank #3

Bank #4

Bank #5

NOT on Akamai

Gomez agents in 12 cities measuring hourly

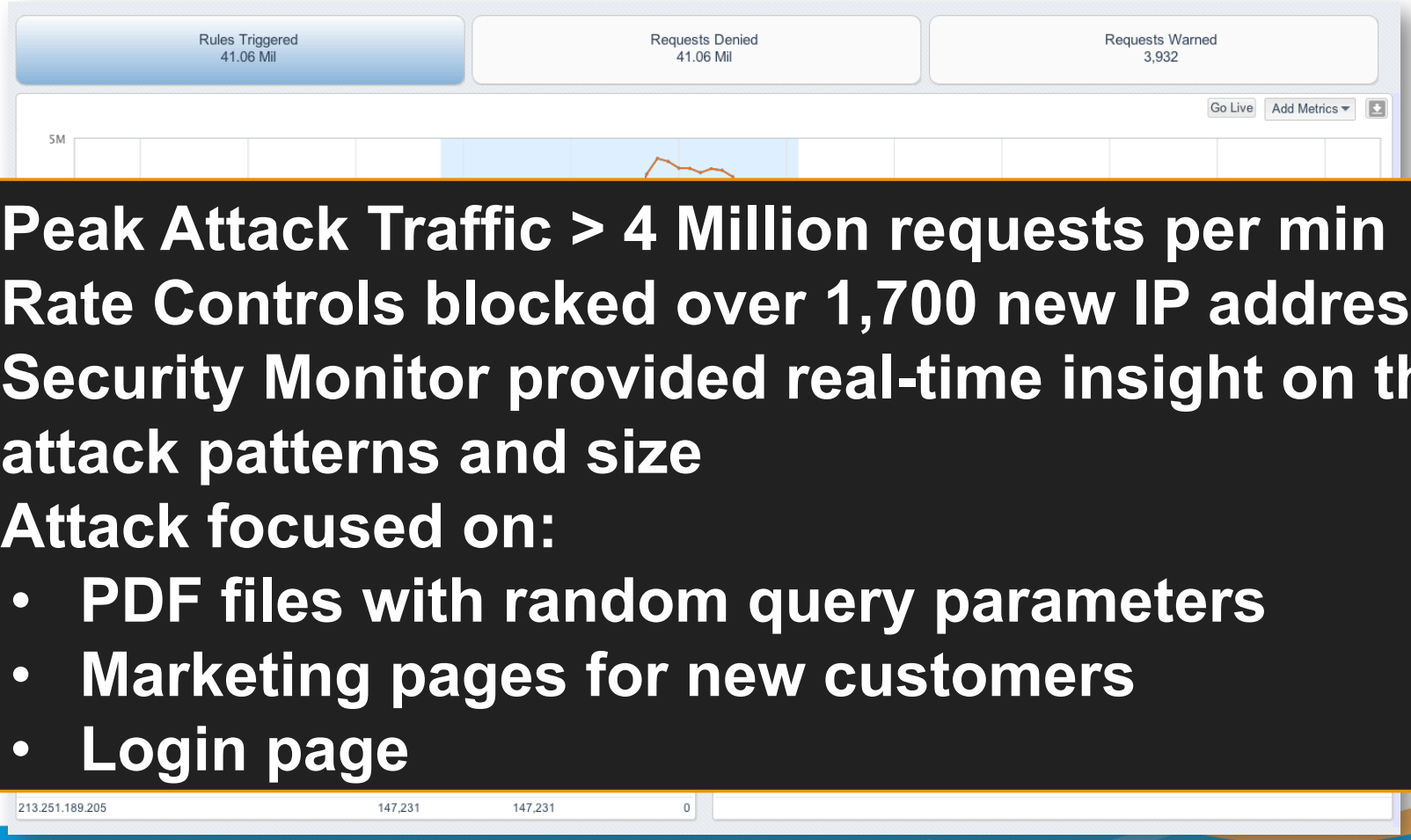


- Error/Outage—site not responding

Phase 3 Attack Example

- Attack started at March 5, 2013 morning
- Peak Attack Traffic > 4 Million requests per min
- 70x normal Edge Bandwidth
  - Origin Traffic stayed at normal levels
- ~2000 Agents participated in the 20 minute assault
  - 80% of the agents were new IP addresses that had not participated in earlier campaigns

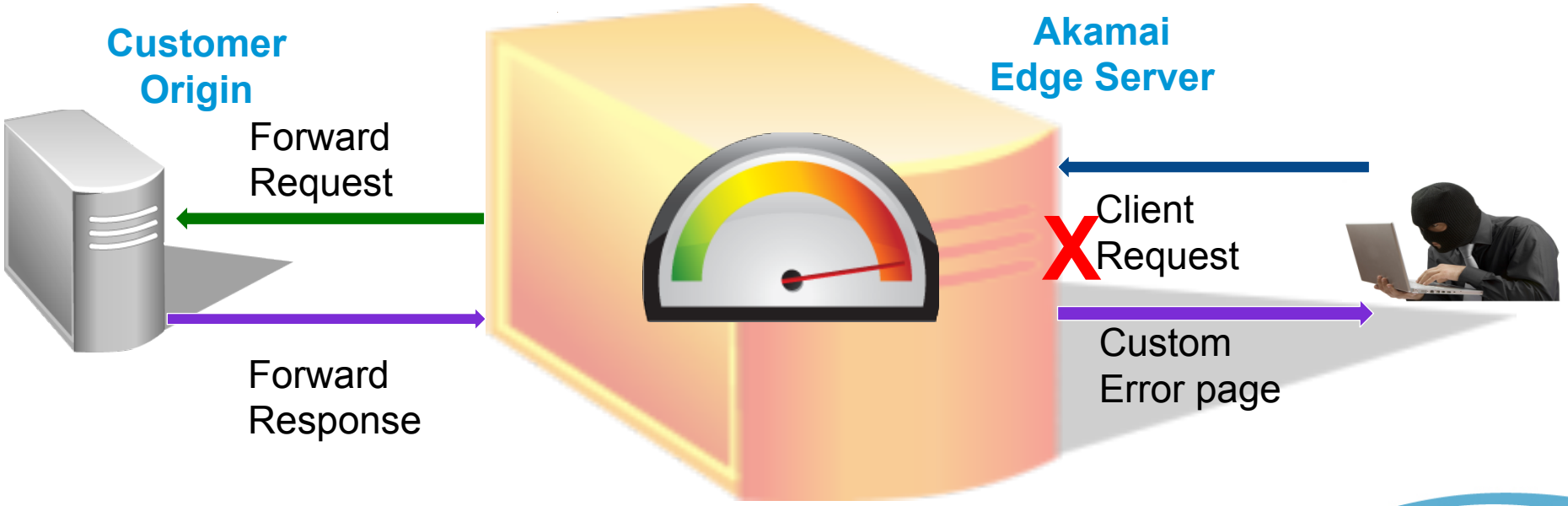
Security Monitor – Visualizing Attack Traffic in Real Time



- **Peak Attack Traffic > 4 Million requests per min**
- **Rate Controls blocked over 1,700 new IP address**
- **Security Monitor provided real-time insight on the attack patterns and size**
- **Attack focused on:**
  - **PDF files with random query parameters**
  - **Marketing pages for new customers**
  - **Login page**

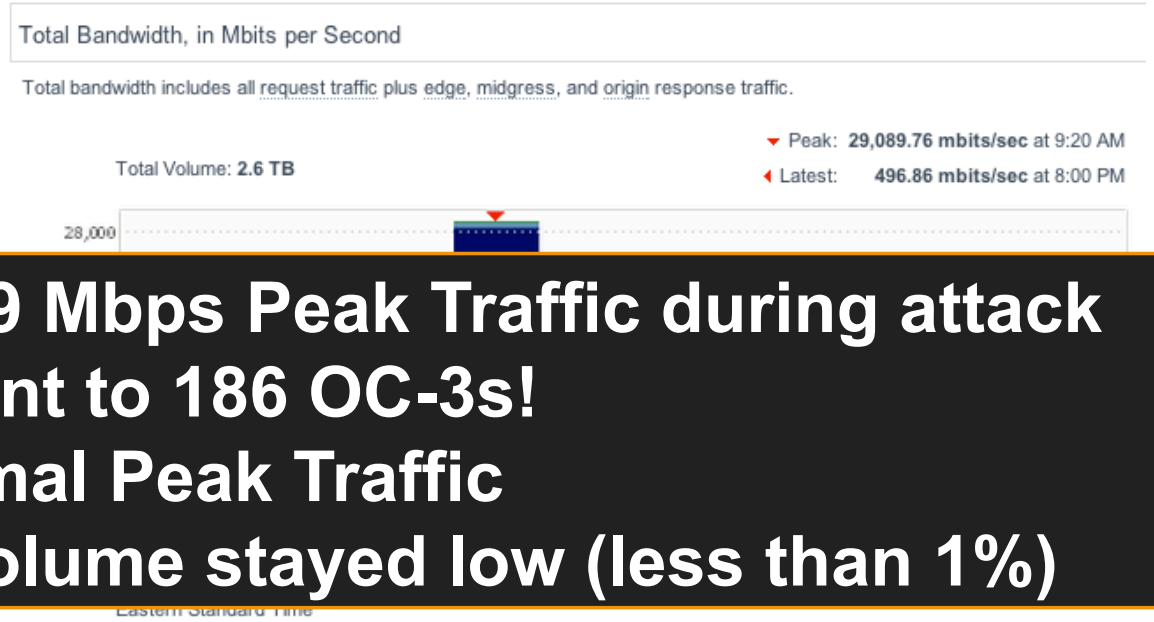
Defeating HTTP flooding attacks – Rate Controls

1. Count the number of Forward Requests
2. Block any IP address with excessive forward requests



Automatic Origin Overload Prevention!

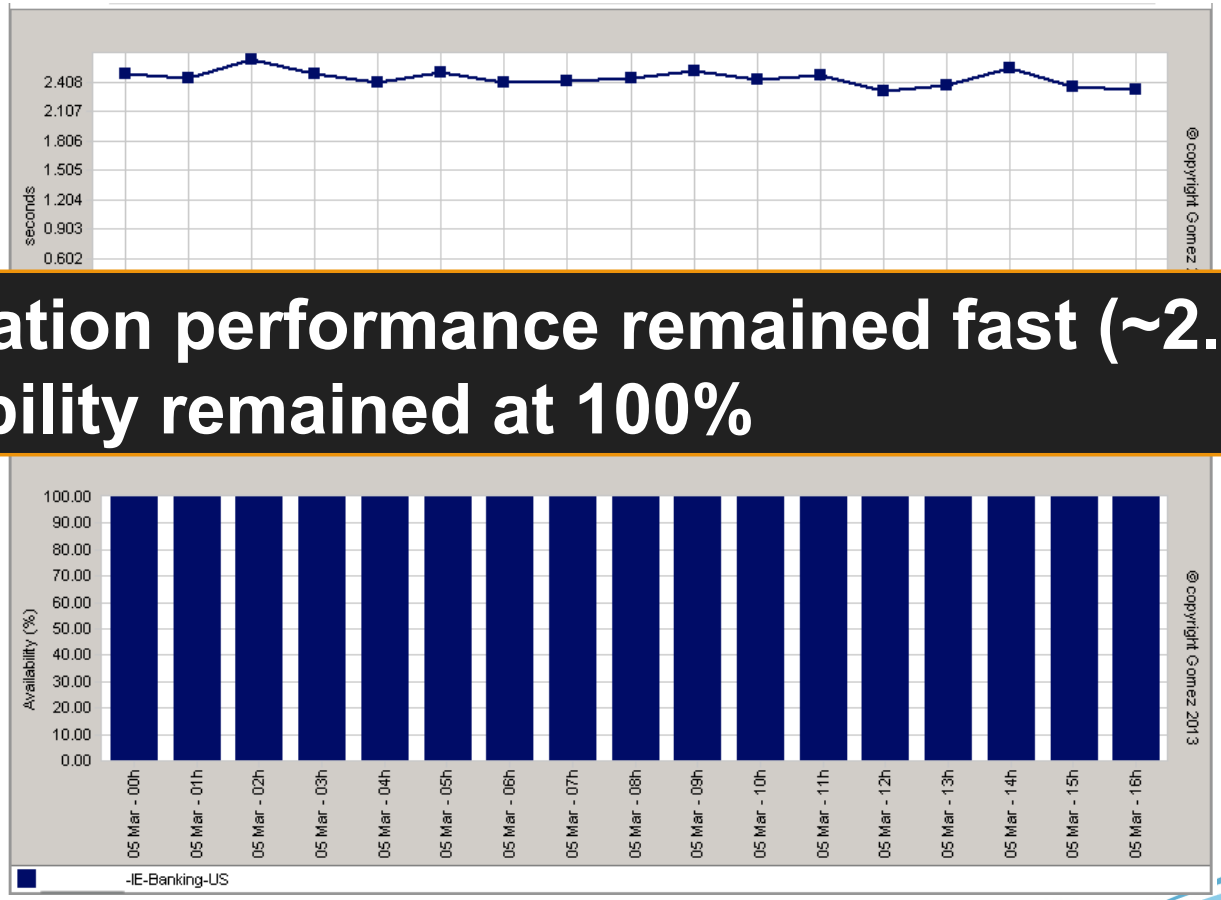
Visualizing Traffic Bandwidth



- **29,013.99 Mbps Peak Traffic during attack**
- **Equivalent to 186 OC-3s!**
- **70x Normal Peak Traffic**
- **Origin Volume stayed low (less than 1%)**

	TOTAL VOLUME	% VOLUME
Edge Responses	2.4 TB	94.2 %
Midgress Responses	31.7 GB	1.2 %
Requests	92.5 GB	3.6 %
Origin Responses	25.4 GB	1 %

Origin Performance and Availability

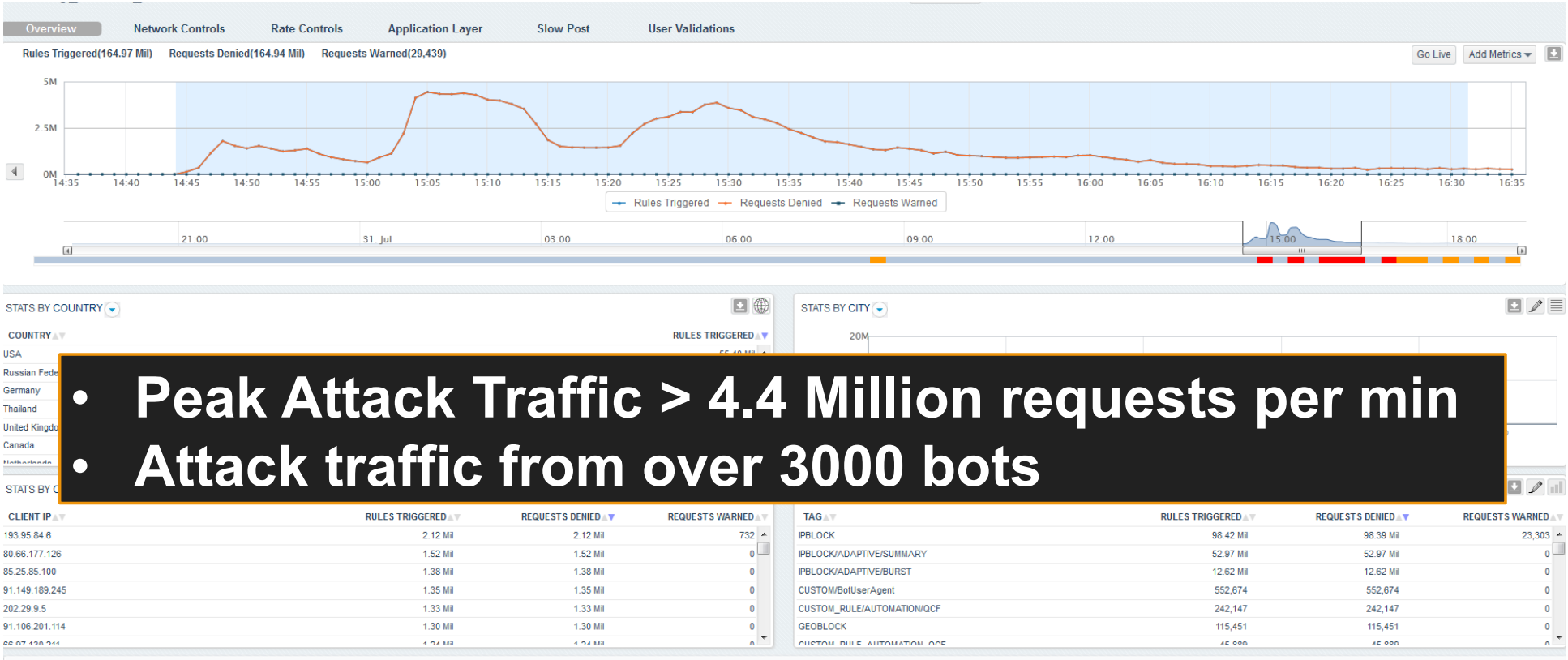


- **Application performance remained fast (~2.5 sec)**
- **Availability remained at 100%**

Phase 4 Attack Example

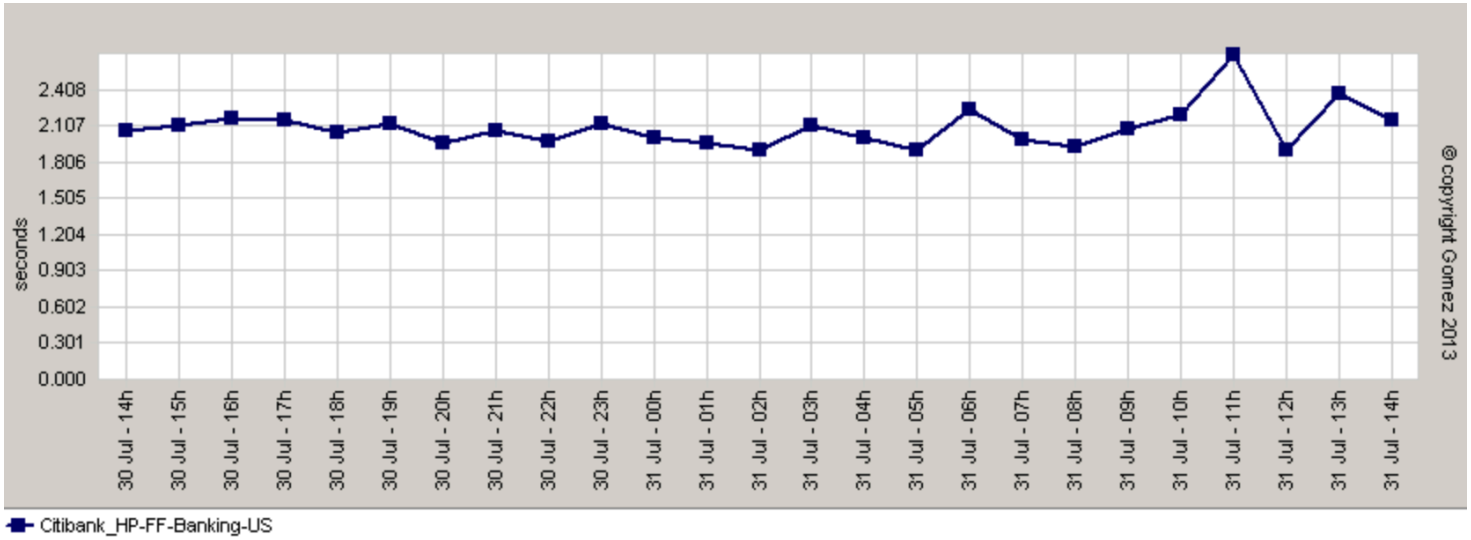
- Attack started at 14:46 GMT, July 31, 2013
- Peak HTTP Attack Traffic > 4.4 Million requests per min
- 30x normal traffic (130,000+ request per second)
- Search and Detail.do (Marketing) webpages were targeted
- No negative availability impact
- No negative performance impact
- Akamai worked with Customer to monitor attack patterns and share intelligence
- Additional IP Blocks for the new bots have been deployed
- DNS infrastructure was also targeted

Akamai Security Monitor – Attack Traffic



- **Peak Attack Traffic > 4.4 Million requests per min**
- **Attack traffic from over 3000 bots**

Performance Impact – Fast as always

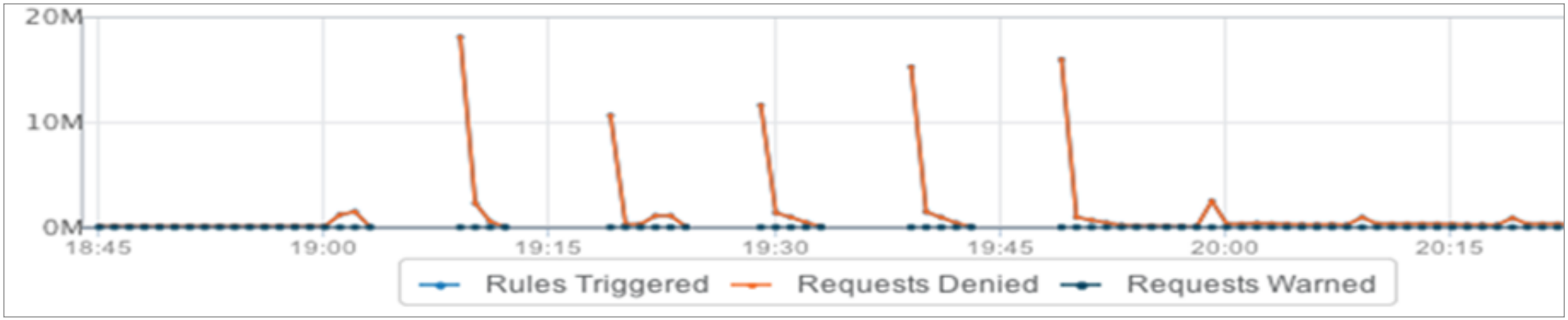


- **100% Availability**
- **Average Response Time ~ 2 seconds**

Attack Tactics - Pre-attack Reconnaissance

Attackers test the site with short burst high speed probes

- Short bursts of attack requests on non-cacheable content every 10 minutes
- Peak of 18 million requests per minute



Rapid burst capability makes “always-on” defenses critical

Application Attacks - Account Checkers

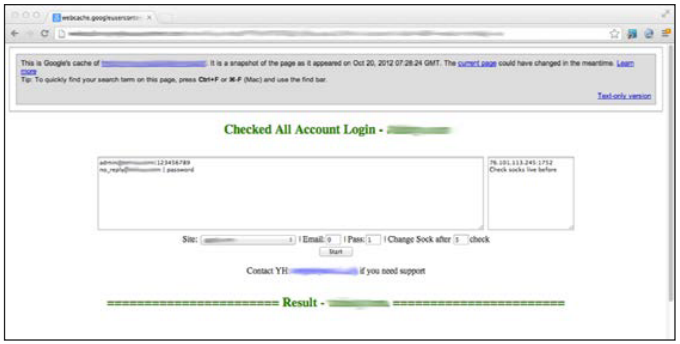
Attackers acquire a list of names and passwords

Use automated tools to test them on a range of web sites

Brute force attack on the login page

- Revenue/Data loss if the account is successfully compromised
  - 1 in 12 chance of success!
- DoS attack on the site since processing the login is resource intensive

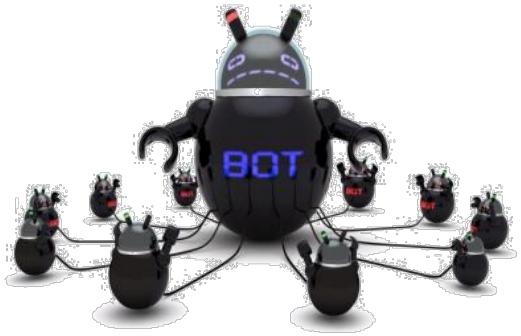
Attack on Multi-Channel eCommerce Customer



Mitigation Process

1. Network Controls:

- Attacker consistently used the same user-agent string
- Detect when the user-agent was seen and collect the source IP addresses
- Block the source IP addresses
- Some benefit – but too manual
- Abandoned as attacker began using more new nodes



2. Rate Controls:

- Block IP addresses that were hitting the targeted URIs at an excessive rate
- Not very effective as the request rate was low, 1 per second or less, but still impacting to the origin authentication infrastructure

Mitigation Process

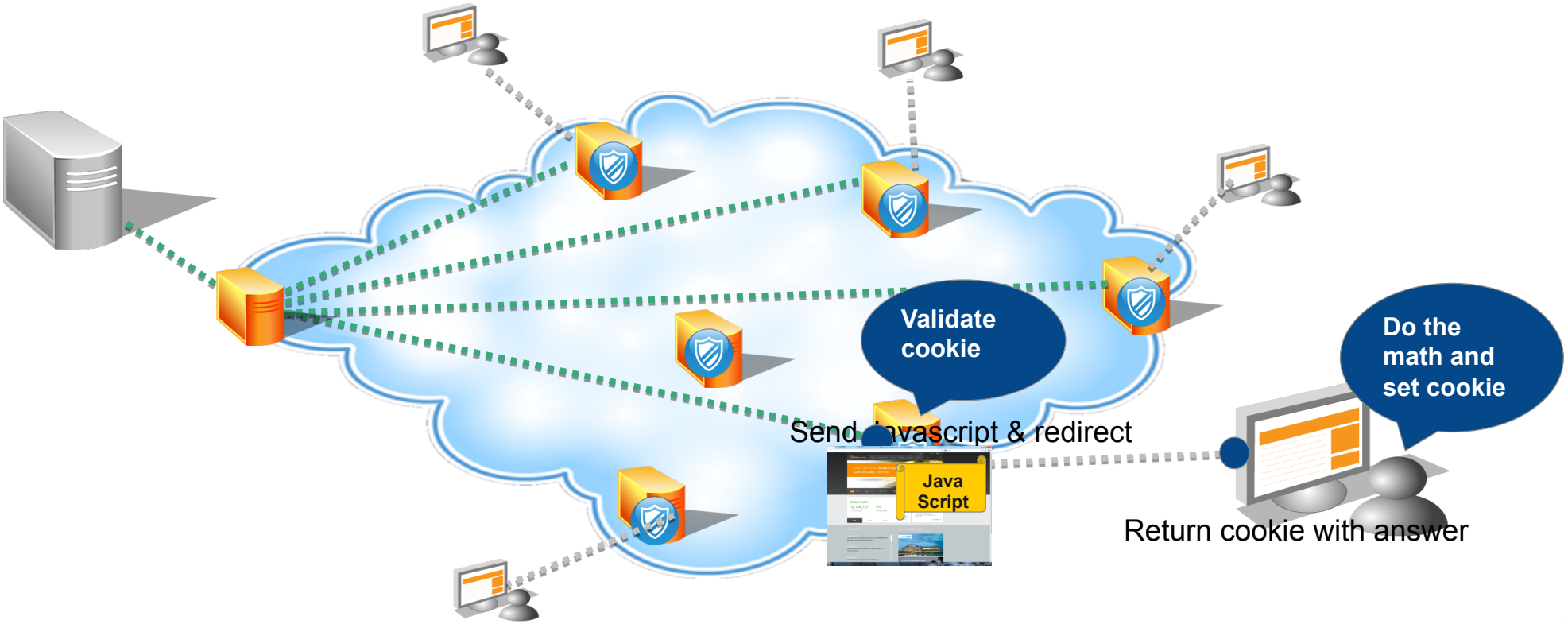
3. Application controls:

- Attack began from international sites (Japan, Italy, Romania) with out passing the correct session information
- Block requests to the target URIs with a missing JSESSIONID cookie
  - Mitigated the attack for ~8 hours until the attacker started sending the correct cookie
- Block requests to the target URIs from non-US based geographies
  - Mitigated the attack for ~24 hours until the attacker shifted to US based addresses
- Block requests with a missing dc cookie
  - Mitigated the attack for 8 hours and was once more circumvented

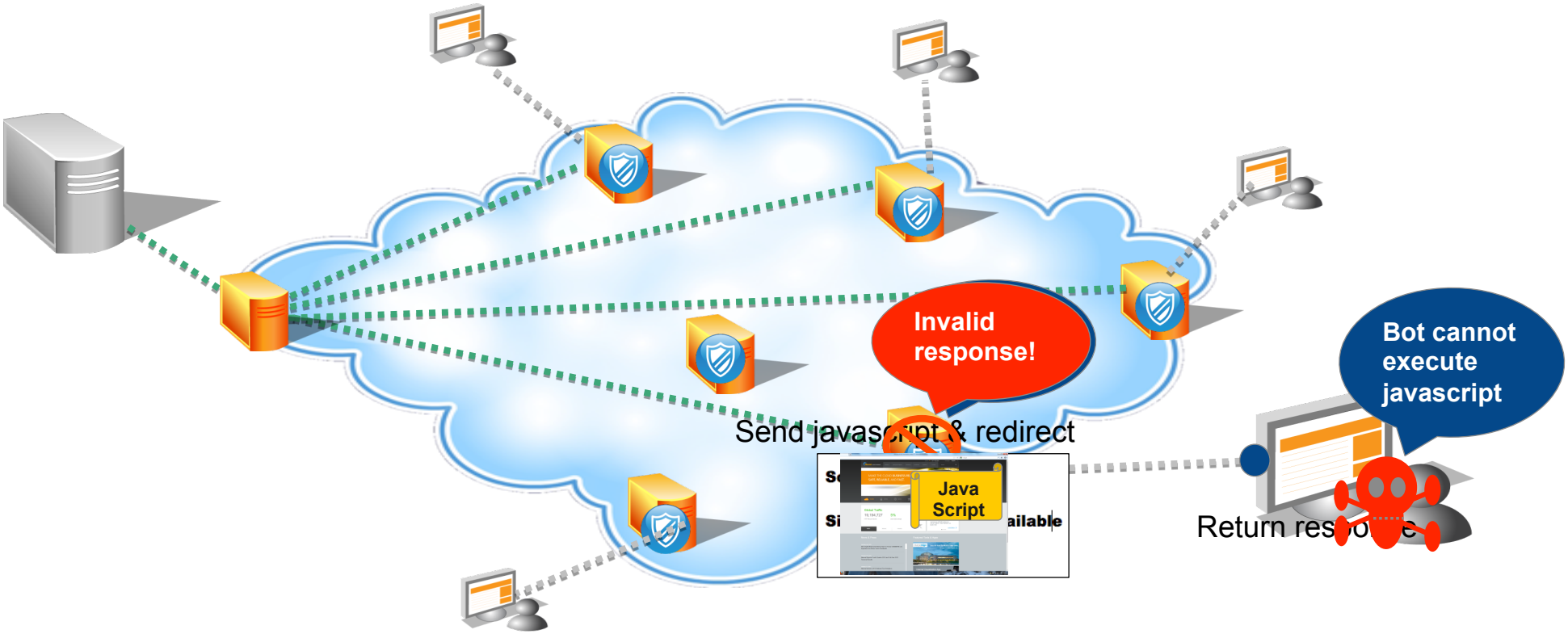
4. User Validation

- Is it a real browser or a bot?

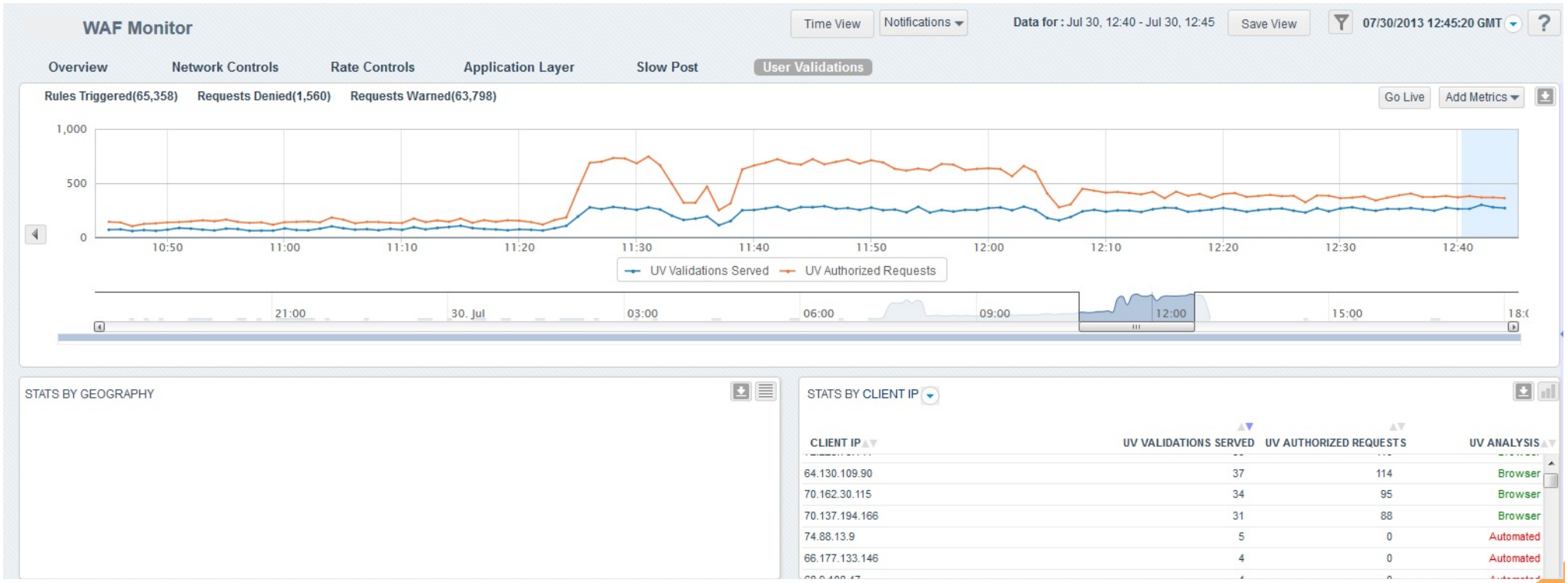
User Validation to Defeat Account Checkers



Failed Validation



User Validation Blocking Account Checkers



Conclusions and Recommendations

Due to recent attack sizes, infrastructure capacity build out is not economical, and may not work anyway

- Attacks range from 13X to 70X normal traffic, 25X to 120X normal request volume

A cloud-based security layer is critical

The burst speed of attacks has become too fast for reactive mitigation – it requires proactive “always-on” defense

Attack resilience requires increased visibility and fluency with layer 7 attack techniques and defenses – network layer defenses are not enough

Thank you

emmace@akamai.com