War Stories from the Cloud:
Rise of the Machines

John Summers
VP Security Products
The Platform
- 175,000+ Servers
- 2,300+ Locations
- 750+ Cities
- 92 Countries
- 1,227+ Networks

The Data
- 2 trillion hits per day
- 780 million unique IPv4 addresses seen quarterly
- 13+ trillion log lines per day
- 260+ terabytes of compressed daily logs

15 - 30% of all web traffic
Avoid data theft and downtime by extending the security perimeter outside the data center and protect from increasing frequency, scale and sophistication of web attacks.

The Akamai Solution – Kona Site Defender + Prolexic
In Q2 2015, DDoS attacks were less powerful, but longer and more frequent

Traditional DDoS attacks harness the scale of global botnets

Newer attacks target protocol vulnerabilities to amplify size
- SNMP (6x)
- DNS (28x-54x)
- CHARGEN (358x)
- NTP (556x)
DDoS Mega Attacks > 100 Gbps in Q2 2015

Twelve mega-attacks in Q2 2015 vs. six in Q2 2014. Most targeted Internet/Telecom. Two targeted Gaming.
DDoS Mega Attacks > 50 Mpps in Q2 2015

A 214 million packets per second (Mpps) DDoS attack was among the highest ever recorded. Such attacks can take out tier 1 routers, such as used by Internet service providers (ISPs).
Avoid data theft and downtime by extending the security perimeter outside the data center and protect from increasing frequency, scale and sophistication of web attacks.

Most Commonly DDoS’ed Verticals – Q1 2015

- Education: Q1 2015 - 4.93%, Q2 2015 - 2.50%
- Financial Services: Q1 2015 - 8.40%, Q2 2015 - 8.19%
- Gaming: Q1 2015 - 35.32%, Q2 2015 - 35.20%
- Hotel & Travel: Q1 2015 - 0.87%, Q2 2015 - 0.41%
- Internet & Telecom: Q1 2015 - 13.77%, Q2 2015 - 12.90%
- Media & Entertainment: Q1 2015 - 7.45%, Q2 2015 - 9.41%
- Public Sector: Q1 2015 - 1.82%, Q2 2015 - 1.05%
- Retail & Consumer Goods: Q1 2015 - 2.25%, Q2 2015 - 2.60%
- Software & Technology: Q1 2015 - 25.19%, Q2 2015 - 27.74%
Avoid data theft and downtime by extending the security perimeter outside the data center and protect from increasing frequency, scale and sophistication of web attacks.

Top 10 Source Countries for DDoS Attacks in Q2 2015

- China 37.01%
- US 17.88%
- UK 10.21%
- India 7.43%
- Spain 6.03%
- Russia Federation 4.45%
- Korea 4.53%
- Germany 4.29%
- Australia 4.18%
- Taiwan 4%

Note: The pie chart illustrates the source countries with the largest percentage of DDoS attacks in Q2 2015.
Web Application Attack Vectors, Q2 2015

SQLi and LFI were the most prevalent attack vectors over HTTP.
Attacks Over HTTPS, Q2 2015

Shellshock accounted for 49% of web application attacks in Q2, largely due to a persistent, multi-week campaign against a single customer.

Shellshock attacks shifted the balance of attacks to HTTPS (56%). Last quarter, only 9% of attacks were over HTTPS.
Top 10 Source Countries for Web Application Attacks, Q2 2015

- China: 51%
- US: 15%
- Brazil: 11%
- Russia: 6%
- Germany: 7%
- Taiwan: 3%
- Netherlands: 2%
- Ukraine: 2%
- Indonesia: 2%
- Ireland: 1%
Top 10 Target Countries for Web Application Attacks, Q2 2015

- US: 81%
- Brazil: 7%
- China: 4%
- Spain: 2%
- Sweden: 1%
- Canada: 1%
- Australia: 1%
- UK: 1%
- India: 1%
- Germany: 1%
Data excludes Shellshock, which primarily targeted a single financial services organization. 95% of the Shellshock attacks were directed at the one company.
Leveraging Big Data to Understand Attacks

The following slides are based on a real event on January 5th 2014....

“Akamai, we are under attack!...”
Ad-Hoc Attack Analysis

An attempt to exploit an old (2007) WordPress Remote File Inclusion vulnerability. The victim application was running ASP.NET.

HTTP/1.1
Host: www.vulnerable.site
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4)

Attacked parameter: wpPATH
Malicious payload: http://www.google.com/humans.txt
What Else Did This Attacker Do On This Site?

Same attacker Sent 2122 different RFI exploit attempts
34 different sites were attacked by the same attacker with a total of 24,301 attacks
Was There Similar Activity Going On At The Same Time?

Attacks originated from a **botnet** containing **272** attacking machines

**1,358,980** attacks were launched during the campaign

The campaign lasted for **2** weeks
Security Big Data at Akamai: Cloud Security Intelligence

20 Terabytes of daily attack data
2 Petabytes of security data stored
Up to 90 days retention
600K log lines/sec. indexed by 30 dimensions
8000 queries daily scanning terabytes of

Benefits

Unrivaled Web Security visibility
• Perform WAF accuracy analysis on any customer at any time
• Detect new attacks, including 0-day and quickly issue new protections

• A powerful web security research tool
• Improve WAF Accuracy
• Behavioral analytics platform
Behavioral Analytics & The Akamai Intelligent Platform
Proactive Security using Behavioral Analytics

DATA SOURCES

- Kona WAF Triggers
- Akamai Logs – “WAF Light”
- Akamai Logs – Behavioral

CSI Platform

HEURISTICS

- Attack Patterns
- Client Behavior
- Application Profiling
- NAT Detection
- False Positive Reduction

IPs
Risk score decay
Grow revenue opportunities with fast, personalized web experiences and manage complexity from peak demand, mobile devices and data collection.

1549 SQL injection attempts w/37 unique payloads
Grow revenue opportunities with fast, personalized web experiences and manage complexity from peak demand, mobile devices and data collection.

691 SQL injection attempts w/18 unique payloads
232 SQL injection attempts w/9 unique payloads
## Client Reputation Details

### Reputation Over Time
- **Time Range:** 05/26/2014, 07:35:36 PM - 05/28/2014, 07:35:36 PM

### Score Changing Events

<table>
<thead>
<tr>
<th>Time</th>
<th>Category</th>
<th>Before</th>
<th>After</th>
<th>Reasoning</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/28/2014 - 08:19:06 AM</td>
<td>Web Attackers</td>
<td>10</td>
<td>9</td>
<td>Client risk score decay</td>
</tr>
<tr>
<td>05/27/2014 - 05:20:06 PM</td>
<td>Web Attackers</td>
<td>9</td>
<td>10</td>
<td>Client performed 1549 SQL injection attempts using 37 unique attack payloads</td>
</tr>
<tr>
<td>05/27/2014 - 11:19:06 AM</td>
<td>Web Attackers</td>
<td>8</td>
<td>9</td>
<td>Client performed 691 SQL injection attempts using 18 unique attack payloads</td>
</tr>
<tr>
<td>05/27/2014 - 10:22:00 AM</td>
<td>Web Attackers</td>
<td>4</td>
<td>8</td>
<td>Client performed 232 SQL injection attempts using 9 unique attack payloads</td>
</tr>
<tr>
<td>05/27/2014 - 06:19:06 AM</td>
<td>Web Attackers</td>
<td>3</td>
<td>4</td>
<td>Client risk score decay</td>
</tr>
</tbody>
</table>
A Year in the Life of a Botnet

In January 2014 we published a blog on a global botnet:

Exploiting Joomla Content Editor vulnerability to install backdoors

Began as a “single event” analysis of the exploit

“Zoomed out” and discovered an entire botnet mining the web for vulnerable Joomla servers
Avoid data theft and downtime by extending the security perimeter outside the data center and protect from increasing frequency, scale and sophistication of web attacks.

A Truly Global Botnet

Botnet Machine Distribution by Country (Top 10)

- USA: 352
- Germany: 200
- France: 98
- Russia: 83
- Brazil: 68
- UK: 48
- Italy: 46
- Netherlands: 45
- Poland: 42
- Canada: 39

Botnet Machine Distribution by Continent

- Europe: 54%
- North America: 25%
- Asia: 13%
- South America: 7%
- Africa: 1%
And a Very Active Botnet

- 43,000 malicious HTTP requests seen over the month
- 2008 different web applications were targeted
10 months later, the Botnet lives on…

In Nov. 2014, the team began a 3 month follow on analysis

The botnet now contains 1037 members.

All members are compromised public Web servers, mostly running Joomla and WordPress CMS

The Botnet has targeted more than 7800 applications over the period

Note – the data is only based on Akamai customers – probably targeted many more applications
Active Members Over Time
New Botnet Members Over Time
Activity Duration of Botnet Members and Evolution

On average, Joomla botnet members spurted malicious traffic over 29 days.

To compare, compromised web servers running other Web platforms, were maliciously active for 10 days on average.

- The reason for the difference between Joomla and the rest of the servers is unclear
- Likely related to the massive exploitation of the Joomla vulnerability

The Botnet evolved over time to attempt to also exploit other vulnerabilities:

- Remote File Inclusion (RFI) on the TimThumb image resizer WordPress module
- Remote Code Execution (RCE) on the Open Flash Chart library
Longevity of Members

Comparing the active Botnet members from 9 months ago to now

- 43 of the botnet members were also maliciously active 9 months ago.
- 4% of botnet members have not been “cleaned up” for 9 months

Surprising, given that:

- The botnet targets a 3-year old vulnerability. Vulnerable web servers should have been upgraded with newer software ages ago
- The awareness for the usage of this vulnerability in the wild. This is not the first publication of a JCE vulnerability exploitation
- The botnet activity is visible and loud, targeting many applications across the Internet, making it easy to be detected.
Avoid data theft and downtime by extending the security perimeter outside the data center and protect from increasing frequency, scale and sophistication of web attacks.

How many bots does Akamai see IN ONE DAY?

8.01 BILLION
Bot requests in 24-hours

Bots on the Akamai Platform

Data Collected
April 1-2, 2015
Total Requests: 85,475,034,620

Bots were 9.4% of all requests
Avoid data theft and downtime by extending the security perimeter outside the data center and protect from increasing frequency, scale and sophistication of web attacks.

Bots on the Akamai Platform

- **Crawlers, Spiders & Scrapers**: 42%
- **API Engines**: 26%
- **Search engines & site indexers**: 24%
- **Other Bots**: 6%
- **Security scanning**: 1%

8.01 Billion requests
Avoid data theft and downtime by extending the security perimeter outside the data center and protect from increasing frequency, scale and sophistication of web attacks.

Bots on the Akamai Platform

- **Crawlers, Spiders & Scrapers:** 42%
  - Content Scrapers: 24%
  - Advertising: 7%
  - Data Aggregators: 3%
  - Web Archivers: 2%
  - Search engines & site indexers: 1%
  - SEO Analyzers: 1%
  - Social Media: 1%

- **API Engines:** 26%
  - API Engines: 6%
  - Other Bots: 24%

- **Security scanning:** 1%

Total requests: 8.01 billion
Avoid data theft and downtime by extending the security perimeter outside the data center and protect from increasing frequency, scale and sophistication of web attacks.

Bots – The Akamai Viewpoint

Common bot challenges
- Stolen intellectual property
- Increased price competition
- Additional bandwidth costs
- IT infrastructure overhead
- DDoS and application downtime

42% Crawford, Spiders & Scrapers
26% Search engines & site indexers
6% API Engines
24% Other Bots
1% Security scanning

8.01 Billion requests
Avoid data theft and downtime by extending the security perimeter outside the data center and protect from increasing frequency, scale and sophistication of web attacks.

Bots – The Akamai Viewpoint

Bot management needs

- Bot detection and identification
- Advanced bot responses
- Report on bot activity and mitigations applied
- Policies to enable business-level protection

8.01 Billion requests
Allow customers to manage the load on their infrastructure from Bots and protect their Web content from being scraped

- Detect if human or not
- Manage Good and Bad Bot Traffic
- Business Oriented Policies – Apply actions based on importance of the traffic to business:
  - Slow it down
  - Feed fake / stale data
  - Challenge it
  - Deny it
  - Etc.
Closing Thoughts

Bots and automation are an increasing problem for the web.

Simply exposing a botnet and its tactics has little impact.

Shutting down members of a Botnet only causes it to breed faster.

Effective detection requires many techniques, but especially behavioral analytics.

Effective mitigation requires a variety of responses that keep the bot unaware that they have been detected.
War Stories from the Cloud: Rise of the Machines

John Summers
VP Security Products