Beyond DDoS: Case Studies on Attack Mitigation for Financial Services

Mike Kun and Patrick Laverty, Akamai CSIRT
Akamai CSIRT: What We Do

Akamai Customer Security Incident Response Team:
• Incident Response for 30% of the web
• We only do web, DNS, and the infrastructure
• No: APT, endpoints, email, Active Directory
• Lots of:
  • Threat intelligence
  • OSINT
  • Coordination with peer CERT/CSIRT
  • Discussions with policy-makers
  • Customer outreach
Login Abuses

Rules Triggered(7,632) Requests Denied(3,590) Requests Warned(4,042)

STATS BY GEOGRAPHY

STATS BY RULE ID

STATS BY CLIENT IP

Block IPs

STATS BY MESSAGE

MESSAGE
RULES TRIGGERED REQUESTS DENIED REQUESTS WARNED
LOGIN/FAIL:73.181.22 4,042 0 4,042
IP 69.73.181.22 recent:click(3,LoginFailures) 3,590 3,590 0

©2013 AKAMAI | FASTER FORWARD™
Login Abuses – TTPs and Defenses

• Rate controls to block fast moving scripts
  • Attack relies on being able to check thousands of accounts quickly
  • Blocking aggressive scripts prevents login exploitation
• Internal monitoring for changes to customer accounts
  • Email address
  • Shipping address
  • Same email on multiple accounts
• Geo blocklists for areas where there is no business
  • Cuts down on the places attackers can launch from
  • Do cloud server providers need to access your webpage?
• Custom rules to block User-Agent strings (or lack thereof)
  • Attack scripts are often simple and will contain only “curl” or “wget”
  • Sometimes none at all
Domain Hijacking

- Attackers gain credentials via phishing
- Attack can be against domain owner or registrar
- Domain maliciously redirected
- DNS settings updated at registrar
- Preventions include properly trained users against social engineering and domain locks
Domain Hijacking – TTPs and Countermeasures

DNS Locking – Two Levels

ClientUpdateProhibited
ClientTransferProhibited
ClientDeleteProhibited

ServerUpdateProhibited
ServerTransferProhibited
ServerDeleteProhibited

.com

ICANN
Scrapers and Bots

[Diagram showing statistics for requests warned, triggered, and denied, with geographical and rule-specific data visualizations.]
Scrapers and Bots
Scrapers and Bots

Rules Triggered (86,023)  Requests Denied (26,008)  Requests Warned (60,015)

Stats by Geography

Stats by Client IP

<table>
<thead>
<tr>
<th>CLIENT IP</th>
<th>RULES Triggered</th>
<th>REQUESTS Denied</th>
<th>REQUESTS Warned</th>
</tr>
</thead>
<tbody>
<tr>
<td>46.47.226.210</td>
<td>77,887</td>
<td>26,008</td>
<td>51,859</td>
</tr>
<tr>
<td>137.117.160.87</td>
<td>2,203</td>
<td>0</td>
<td>2,203</td>
</tr>
<tr>
<td>168.63.93.0</td>
<td>2,196</td>
<td>0</td>
<td>2,196</td>
</tr>
<tr>
<td>63.128.163.20</td>
<td>885</td>
<td>0</td>
<td>885</td>
</tr>
<tr>
<td>137.135.168.19</td>
<td>732</td>
<td>0</td>
<td>732</td>
</tr>
<tr>
<td>85.70.234.114</td>
<td>389</td>
<td>0</td>
<td>389</td>
</tr>
</tbody>
</table>

Stats by Rule ID

Stats by ARL

<table>
<thead>
<tr>
<th>ARL</th>
<th>RULES Triggered</th>
<th>REQUESTS Denied</th>
<th>REQUESTS Warned</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.somesite.com/en/light/">www.somesite.com/en/light/</a></td>
<td>734</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><a href="http://www.somesite.com/fr/light">www.somesite.com/fr/light</a></td>
<td>734</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><a href="http://www.somesite.com/en/light/">www.somesite.com/en/light/</a></td>
<td>734</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><a href="http://www.somesite.com/fr/light/">www.somesite.com/fr/light/</a></td>
<td>732</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><a href="http://www.somesite.com/light/">www.somesite.com/light/</a></td>
<td>732</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Scrapers and Bots
Scrapers and Bots – TTPs and Countermeasures

- Reduce Efficiency
- Reduce Impact
- Client Validation
- Welcome Bots

Aggressiveness vs. Desirability Matrix
Hacktivists - TTPs

Attack types are all across the board:

- DDoS
- SQL Injection
- Defacement/Cross-Site Scriping (XSS)
- Local File Include (LFI)
- Social Engineering
- In-person protests
Hacktivists - Countermeasures

DDoS – Rate Controls
## Hacktivists - Countermeasures

### DDoS – Rate Controls

<table>
<thead>
<tr>
<th>RATE POLICIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>RATE CATEGORY</td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>Page view request rate v5 (Currently Active)</td>
</tr>
<tr>
<td>Origin error rate (v3) (Currently Active)</td>
</tr>
</tbody>
</table>
Hacktivists - Countermeasures

SQL Injection – WAF Rules
Hacktivists - Countermeasures

Defacement/Cross Site Scripting (XSS) – WAF Rules
Hacktivists - Countermeasures

Local File Include (LFI) – WAF Rules
Reflection and Amplification Attacks
Reflection and Amplification Attacks - Analysis

Reflection:

- Uses UDP packets with forged source headers
- Attacker targets in intermediate server: DNS, NTP, etc
- Server replies to the forged source, sending traffic to the victim
- Victim does not know the source of the attack

Amplification

- Attacker makes a query to the intermediate server
- The query is small but the answer is large
- The difference allows a small botnet to send lots of small queries and still hit with a lot of traffic
Reflection and Amplification Attacks - Analysis

Amplification Factors:

- BitTorrent: 3.8
- SNMP: 6.3
- DNS: 28-54
- QOTD: 140.3
- CharGEN: 358.8
- NTP: 556.9
Flash Crowds vs. DDoS

- Both have large number of requests
  - Flash crowd has low requests per source IP address
  - DDoS has high requests per source IP address

- Other differentiators
  - Referrers
  - URL pattern
  - User demographics
  - Blacklists
  - DDoS bot signatures
  - Session tokens

- Responses differ greatly
  - Block a malicious DDoS
  - Allow a flash crowd
Flash Crowds

Akamai Delivered Sochi Traffic Trend

* This graph represents HTTP, HTTPS, live video streaming, and video-on-demand for a subset of properties and should not be used to represent total viewership or traffic, but rather the trend of viewership through the event.
Questions?