Good Bot, Bad Bot, Ugly Bot. Battle of the Bots!

John Ellis – 周由安
Chief Strategist, Cyber Security (APJ)
Akamai Technologies
@zenofsecurity
About me

- Kiwi (New Zealander)
- 20+ years experience in IT security (trained sheep to hack)
- Have worked in defence, telecommunications and banking
- Consider myself a student, but love to share what I know
- 9 years in Singapore, and see we’re still trying to find the Asian solution to the Asian problem (talk to me afterwards if you want to know more).
- Still ‘trying’ to learn Mandarin….might one day get there
## Cyber ‘buzz’ bingo

<table>
<thead>
<tr>
<th>Cyber</th>
<th>SaaS</th>
<th>Threat Intel</th>
<th>Cloud</th>
<th>BOYD</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT</td>
<td>Cyber Kill Chain</td>
<td>Innovation</td>
<td>Big Data</td>
<td>Breach</td>
</tr>
<tr>
<td>TTPs</td>
<td>Signal to noise</td>
<td>Cross-Platform</td>
<td>SMAC</td>
<td>Next-gen</td>
</tr>
<tr>
<td>APT</td>
<td>China</td>
<td>Data Driven</td>
<td>Thought Leaders</td>
<td>Cyber Attack</td>
</tr>
<tr>
<td>BOT</td>
<td>Game Changer</td>
<td>PaaS</td>
<td>Cyber Crime</td>
<td>Hacktivist</td>
</tr>
</tbody>
</table>
What is a bot?

A software application that automates tasks that are simple and structurally repetitive at much higher rates or precision than a human.
Bot trends & environment

**Good**
- Human traffic: 44%
- Partner bots
- Search engine, crawlers, spider bots
- Vulnerability scanner, Site performance bots

**Bad**
- Bot traffic: 56%
- Scraper bots
- Hacker, Fraud bots
- DDoS bots
- Spam bots

-_bad Bots: Account for 29% of all website visits, 22% fraud activity
- Good Bots: Account for 27% of all website visits

**Source:** Incapsula / Akamai
Good bots

Vulnerability Scanners

Search engine optimization (SEO)

Performance analysis tools
Bad bots

- Fraud
- Malware
- Spam (it ain’t ham)
- Vulnerability scanners
- Scrapers (your competitors)
- DDoS attacks
- Did I mention malware?
Ugly ‘naughty’ bots

Scrapers

Want to know everything about you

Price Aggregators

Crawlers

Too Friendly

Malicious? Maybe, Maybe not
SPAM Bots

Target marketing

Improve SEO

Malware distribution

Fraud
Scraper Bots (an example)
Commercial Scraping Services / Tools

OUTwit Technologies
import io
80legs
kimonono
scrape.it
Scrape Box
mozenda
UiPath
Akamai
The BOT evolution

Desktop

Server

Cloud

Mobile

Internet of Things (IoT)
DDoS Bots

DDoS attacks instances plotted over time Q1 2013-Q1 2015

Source: Akamai SOTI Security Report Q1 2015
Top 10 Source Countries for DDoS Attacks

1. China
   - 1.4 billion people
   - 642 million people online
   - Over 50% of systems infected with viruses
   - 9 out of 10 Windows systems pirated
   - 70% of Windows systems never patched

2. Germany
   - 17.3%

3. Russia
   - 5.95%

4. France
   - 6.03%

5. U.K.
   - 6.17%

6. Korea
   - 6.23%

7. India
   - 6.93%

8. Spain
   - 7.29%

9. Italy
   - 8.38%

10. U.S.
    - 12.18%

China has 23.45% of DDoS attacks.
DDoS 4 Bitcoin (DD4BC)

Who, What, Where & How

- DD4BC (DDoS For Bitcoins)
- Online ransom group
- Not ransomware
- No other attribution
- Publicly available DDoS toolkits & rented botnets in the underground

Who are the targets?

- Banking & Credit Unions: 74%
- Gaming: 15%
- Media & Entertainment: 4%
- Payment Processing: 7%
Great Canon (GC) of China

A path system, capable of injecting traffic and directly suppressing traffic. Acting as a full “man-in-the-middle” for targeted flows. ‘Harnesses’ legitimate web browsing traffic for attack capability and capacity. Example of a cat and mouse game. Targets of HTTP get flood DDoS attack. Coding error provides clue as to how to detect and filter traffic.


Coding error provides clue as to how to detect and filter traffic. Example of cat and mouse game.
Value of a hacked PC (Brian Kerbs)

Using Botnets to access market insights

- **Legal** return on investment
- **Illegal** access to information

Source: Interpol
Account checkers and Fraud

How does this evil deed typically happen?

1. Builds tools server
2. Cultivate list of open proxies
3. Acquire compromised logins
4. Check / alter compromised accounts
5. Make fraudulent purchase

Account checkers and Fraud

British Airways suspended a frequent flyer account after
an Andromeda Botnet Used to Deliver New GamaPoS Malware

By Eduard Kovacs on July 17, 2015

Researchers at Trend Micro have conducted an analysis of GamaPoS, a new point-of-sale (PoS) malware that has made its way onto the systems of United States organizations with the aid of the notorious Andromeda botnet.
How to manage em’ BOTS
Block, Mitigate or Manage?

Blocking BOTS causes them to go underground, mutate and harder to detect.

Management strategies vary depending on the nature of the BOT and it’s goal.

Not sure if bot......or

Stupid human?
TTPs for the Good, Bad and Ugly

<table>
<thead>
<tr>
<th>Aggressiveness</th>
<th>Degrees of Desirability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Desirable</td>
</tr>
<tr>
<td>Reduce Impact</td>
<td>Welcome Bots</td>
</tr>
<tr>
<td>Terminate with extreme prejudice</td>
<td>Client Validation</td>
</tr>
</tbody>
</table>

- Aggressiveness: Reducer Impact, Terminate with extreme prejudice
- Degrees of Desirability: Desirable, Undesirable
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.

Solution Landscape (what can you buy)

From a technology perspective:

BOT Detection Methods
- No BOT Detection
- Rate Based Detection
- Cross Customer Header/IP Based Tracking
- Cross Customer Fingerprint Based Tracking
- Advanced BOT Evasion Traps

BOT Response Methods
- Alert/Deny
- CAPTCHA
- HTML Obscuring/Rewriting
- Slow BOT/Serve Alt./etc.
- BOT Obfuscation

Cloud BOT Mgt.
Cooking your BOT management program

Detection

Learnings

Mitigation

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.
Bot Detection Methods

- Client reputation
- Client and browser fingerprinting
- HTTP header anomaly detection
- JavaScript Injection
- JS BOT evasion traps
- Behavioral Analysis
Bot Response Methods

- IP blocking
- Geo blocking
- Rate controls
- Web Application Firewall Rules
- Obfuscation for HTML, JS, URL and Form
- Serve slow, stale, alternate, tar pit
- CAPTCHA challenge
Bot Learnings

- BOT scoring, categorization and trends
- Crowd sourcing of new BOTS [www.botopedia.org](http://www.botopedia.org)
- Resource usage by BOT
- Input into evolving your detection and mitigation tactics
- Understand the cost of your mitigation strategies
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.

7 Key Ingredients to Succeed (today)

1. **Scale your defenses with a Cloud WAF**
   Extend your perimeter beyond your site

2. **Reverse Proxy**
   Automatically drops traffic not on port 80 or port 443

3. **Geo-based blocking**
   Refuse requests from customer-selected list of countries

4. **Validate against known list of attackers**
   Positive or negative security model (black or white lists)

5. **Rate Controls**
   Block requests that are too fast or too slow (anomaly scoring)

6. **Data driven WAF**
   WAF rules continuously refined based on visibility into web

7. **Caching**
   Dynamic and static caching to serve requests
Looking ahead

- Good Bots are an essential part of our Internet ecosystem
- It’s an arms race, and you need to have a clear strategy
- If you don’t have a WAF….get one!!!
- Threat intel (bingo) is vital in understanding. Learn from others
- Now you’ve got a strategy, have a plan and rehearse it!
- It’s hard…but understand what normal looks like (try..please)
- Think active defense…be smart in how you operate
Friend or Foe? You need to decide
I would like to thank

- Mike Smith (Akamai APJ Security CTO)
- Patrick Laverty (Akamai CSIRT)
- Mike Kun (Akamai CSIRT)
- Dave Lewis (Akamai Global Security Advocate)
- …and Akamai’s customers and competitors (they keep me honest)
- 我也感谢我的太太（大熊猫）