Security in a Borderless World

Finding Unknown Risks, 0-day Threats and Measurable Enforcement

Elias Manousos
CTO
RiskIQ
Session Overview

• Online Risk Overview
• Marketing Risks
  – Trademark Abuse, Lead Diversion, Partner/Agent/Affiliate Compliance
• Security, Trust & Safety Risks
  – Account Hijacking, Malware, Phishing, Malvertisements
• Specific Examples
Overview

Today’s attacks exploit vulnerabilities in brands, marketing programs and online business relationships
Online Threats

Target organizations across 3 vectors

**Brand** – Attach to it or use as vehicle

**Customer** – exploit the customer or identity

**Extended Enterprise** – the weakest link: Vendors, Partners, Infrastructure
Staying under the radar

Less risky to “bad guys” and generates significant monthly income

Difficult to prove
- Requires “Big Picture” to make the case
- Seemingly Unconnected: High Frequency, Low Impact Risks

Civil policy violations vs. Criminal
Inexpensive to Operate
- Automated, cookie-cutter
Layers of Complexity

In most cases, US companies fund fraud by purchasing data from the bad guys through a series of middlemen who also benefit.

- Traffic Generators: Source of new users daily
- Buyers: Monetization Sources
- Specialization: Outsourcing lowers the bar
Organizations Suffer

• Stuck in Fire-Fighting Mode

• Operational and Enforcement Costs Increase

• Revolving Door due to Lack of Attribution “who are they?”
The Extended Enterprise

“The related companies, customers, suppliers, service providers, marketing partners and other organizations with which your organization relies on to conduct business.”
Extended Enterprise Examples

The Systems and Partners you can’t live without.....

• Cloud Providers such as Salesforce, Amazon

• Key Services: Ex. Payroll

• Hosted Web Applications

• Marketing Applications: Web Ads, 3\textsuperscript{rd} Party Email Systems

• Web 2.0 Services
  – LinkedIn, Facebook, Twitter
Brand Examples

• Paid Search Violations

• Trademark Infringement to aide Lead Diversion

• Partner Compliance / Misleading Statements
Paid Search Enforcement

Your brand is leveraged to drive targeted, brand-conscious traffic through advertisements, blogs and search results.

Unauthorized advertisers use your trademark in ad copy to lure visitors to their website.
Lead Aggregators

Customers are misled to believe that the website has an official relationship with your business.

Your trademark is used within the website to build user confidence and trust.
Anyone Can Use Your Trademark

Your brand provides credibility to otherwise suspect websites.

Fine print on this page attempts to explain how they will save you 50% on nationwide insurance. This site replaces “nationwide” with any insurance company the user places in the search on the preceding page.
The Bottom Line

It’s up to **you**, the trademark owner, to police the use and abuse of your trademarks across the web.
Social Media

• Social Media represents a new source of traffic
• Better Targeting = better conversions

• COMPANY SPECIFIC CONTENT REMOVED
Purpose of the Tweet

Paid Ads Running on low quality website

A form of web spam

Your Trademark and AD BUDGET provides the monetization

COMPANY SPECIFIC CONTENT REMOVED
Partner Compliance

• False or Misleading Statements
• Using Prizes or Incentives
• Kickbacks
• Territory issues – for example offering a service in another state
Card Affiliates

Online Partners

Debit Cards should not be marketed as Credit

Instant Approval Credit Cards Are sometimes marketed as cash advances

Many Affiliate sell customer information several times = identity theft
Traffic Sources

Search is the single largest traffic source followed by social media

- **Search Engine**
  - Google
  - Yahoo
  - Bing

- **Paid Ads**
  - Paid Search
  - Contextual
  - Banner
  - 3rd Party

- **Affiliate Networks**
  - Commission Junction
  - Linkshare
  - GAN - Google
  - ClickBank

- **Mobile Apps**
  - iPhone
  - Blackberry

- **Social Media**
  - Blogs/RSS
  - Facebook
  - Twitter
  - Digg
  - Social Bookmarks

- **Hacked Legit Sites**
  - Major Brands
  - Mom & Pop
  - Universities
  - Non Profits
  - Abandoned Domains
This Funnel is True for **Good** And **Bad** Traffic.

It is also accurate for different schemes:

- Phish
- Malware
- Lead Diversion
- Affiliate Fraud

**Example**

- 1M Impressions
- 1% have interest
- 10% Click
- 1,000 targets

**Branded Content is the most effective lure to attract users**
Recommendations

• Do you have Policies and Procedures in place?
• Monitor High Traffic Areas: Search, Social
• Develop a scored whitelist of authorized partners
• Understand the financial mechanics of your organization, how can someone make $ off your brand
• Develop countermeasures which increase attackers costs, lower your enforcement costs
Badware

Application acts deceptively or irreversibly.

Application engages in potentially objectionable behavior without:
First, prominently disclosing to the user that it will engage in such behavior, in clear and non-technical language, and then, obtaining the user's affirmative consent to that aspect of the application. [1]
Badware Problem

Malware such as Zeus variants and other coordinated scams are costing Financial Institutions over 1B Annually

FIs calculate losses @ US 5-15M each month

Financial Institutions are the main target of web based malware
Current Approach is Reactive

Malware-based phishing is realized in the form of complaints and losses

Prevention is a difficult problem...

– Legit Partners are Hacked or Fooled by Bad Guys
– Gathering data at Internet Scale across various web properties
– Revolving Door due to lack of attack attribution
– “Fire Fighting mode” takes attention away from big picture
Malware-Based Phishing Overview

1. User's Browser
   - Exploit Shells browser, downloads and installs payload
   - Malicious Payload Server

2. Legitimate Traffic Source
   - My Legit Website
   - http://goodguy.com
   - This is a good site
   - We got Hacked or fooled by a bad guy.
   - We promote various products and services... Poisoned Link
   - We are partners with brands and even use logos... TM Big Bank Logo

3. Exploit Kit
   - Runs various tests to determine best method of infecting users

4. Picks Payload Server

5. Doorway Page
   - Doorway Page
   - http://MyWebsite.com
   - Rendered Page
     - Relevant Content
     - Relevant Content
     - Hidden iFrame...
How it happens...
Infected:

COMPANY SPECIFIC CONTENT REMOVED
Infection Point

• COMPANY SPECIFIC CONTENT REMOVED
Paid Search: (company) loan

• COMPANY SPECIFIC CONTENT REMOVED

• Page 1 on Google!!!

• Possibly a coordinated Adwords Attack

• $11.49 Cost Per Click!

• Scareware
Infected: Fake AV Install

• COMPANY SPECIFIC CONTENT REMOVED
Infected: voraceproductions.com

- Use of redirects through 2 infected hosts
- 2\textsuperscript{nd} infected host acts as the hackers ad server?
- new-av-scannerr.com is the scareware host
# Scope Overview

<table>
<thead>
<tr>
<th>Brand</th>
<th>Brand X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test run timeframe</td>
<td>10 days</td>
</tr>
<tr>
<td>Start date</td>
<td>2010-02-22</td>
</tr>
<tr>
<td>End date</td>
<td>2010-03-05</td>
</tr>
<tr>
<td>Candidate pages</td>
<td>63,377,746</td>
</tr>
<tr>
<td>Total pages picked for analysis</td>
<td>148,543</td>
</tr>
<tr>
<td>Malicious sites containing BofA brand with *reach</td>
<td>740</td>
</tr>
<tr>
<td>% of Malicious sites</td>
<td>0.5%</td>
</tr>
<tr>
<td>Unique Malware resources/URIs (out of the 740)</td>
<td>353</td>
</tr>
<tr>
<td>Unique Malware hosts (out of the 740)</td>
<td>172</td>
</tr>
</tbody>
</table>

*Without reach = 14,577
## Top 10 Distribution Concepts

<table>
<thead>
<tr>
<th>concept</th>
<th>incidentCount</th>
</tr>
</thead>
<tbody>
<tr>
<td>X routing number</td>
<td>97</td>
</tr>
<tr>
<td>bank X loan</td>
<td>79</td>
</tr>
<tr>
<td>bank X home loans</td>
<td>39</td>
</tr>
<tr>
<td>X privacy guard</td>
<td>30</td>
</tr>
<tr>
<td>bank X car loan</td>
<td>29</td>
</tr>
<tr>
<td>bank X interest rates</td>
<td>27</td>
</tr>
<tr>
<td>X logins</td>
<td>24</td>
</tr>
<tr>
<td>bank X routing number</td>
<td>23</td>
</tr>
<tr>
<td>bank X online</td>
<td>21</td>
</tr>
</tbody>
</table>
Calculating Impact & Defining Metrics

Develop your Malware Weather Report....

Research the groups targeting you.

Calculate users exposed or infected.

Distinguish targeted attacks from untargeted.

Store the hosts/exploits/kits forensically for follow on investigation.

Develop metrics to help decide when and what actions to take.
Malvertisements
Malvertising (from "malicious advertising") is the use of online advertising to spread malware.

Because advertising content can be inserted into high-profile reputable websites, malvertising provides malefactors an opportunity to "push" their attacks at cautious web users who would not normally visit unknown external URLs, by exploiting the reputation of the website and the allegedly advertised brands to convince them that they are visiting legitimate advertisements.
Why Worry?

Malvertisements expose vulnerabilities in critical infrastructure

Ability to run Malvertisements lowers the bar for Bad Guys

– Step 1: Buy 0day exploit code.
– Step 2: Buy Botnet/malware in underground forum
– Step 4: Profit.
Malvertisements Status

Ad Networks generally argue their networks are “clean”. Networks have little reason to publicize them. Therefore…..

• Metrics are Lacking – this is similar to Data Breach Events prior to legislation (CA SB 1386)

• Publishers find out via customer complaints (similar to Phishing)

• Malvertisements don’t happen often, this doesn’t mean we don’t have a major problem

• Bad Guy success is measured differently from our idea of success – metrics expose their business model
Overall Trends

Malvertisement Statistics

<table>
<thead>
<tr>
<th>Total Incidents</th>
<th>Unique Publishers</th>
<th>Unique Publishing Ad Networks</th>
<th>Unique Delivering Ad Networks</th>
<th>Unique Blacklisted Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>4036</td>
<td>1142</td>
<td>119</td>
<td>109</td>
<td>1098</td>
</tr>
</tbody>
</table>

Graph showing trends over months.
Publisher Size

Majority of incidents occur on smaller publisher sites

- 46% of incidents are small pubs > 1M Rank
- 32% are top 1M
- 2.58% are top 1000
- .93% are top 100
### But... Big and Small Publishers Impacted

<table>
<thead>
<tr>
<th>Publisher</th>
<th>Rank</th>
<th>Publisher</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>PhotoBucket</td>
<td>24</td>
<td>Ezlaptop.com</td>
<td>445,506</td>
</tr>
<tr>
<td>Huffington Post</td>
<td>32</td>
<td>Thepetrescue.com</td>
<td>417,966</td>
</tr>
<tr>
<td>Digg</td>
<td>62</td>
<td>leechers.info</td>
<td>346,826</td>
</tr>
<tr>
<td>Wikia</td>
<td>88</td>
<td>Zippyshare.com</td>
<td>325,469</td>
</tr>
<tr>
<td>Accuweather</td>
<td>148</td>
<td>Searchreel.com</td>
<td>297,864</td>
</tr>
<tr>
<td>FoxSports</td>
<td>192</td>
<td>glamsham.com</td>
<td>238,705</td>
</tr>
<tr>
<td>Last.fm</td>
<td>250</td>
<td>sushidating.com</td>
<td>221,251</td>
</tr>
<tr>
<td>MensHealth</td>
<td>581</td>
<td>Celebwebnews.com</td>
<td>150,000</td>
</tr>
</tbody>
</table>
Typical Publisher Profile

Ad Publisher: dailyradar.com

Publisher Details
- **Domain:** dailyradar.com
- **Category:** Unknown
- **Alexa Traffic Rank:** Top 10,000 (3,922)
- **Quantcast Traffic Rank:** Top 10,000 (2,452)

Incident Summary
<table>
<thead>
<tr>
<th>Range</th>
<th>Publishing Ad Networks</th>
<th>Delivering Ad Networks</th>
<th>Pages</th>
<th>Incidents</th>
<th>Drive Bys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Month</td>
<td></td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Last 3 Months</td>
<td></td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Last Year</td>
<td>1</td>
<td>1</td>
<td>13</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>Overall</td>
<td>1</td>
<td>1</td>
<td>13</td>
<td>20</td>
<td>20</td>
</tr>
</tbody>
</table>

Monthly Incident Volume

Most Recent Incidents

<table>
<thead>
<tr>
<th>Date</th>
<th>Publishing Ad Network</th>
<th>Delivering Ad Network</th>
<th>Drive By</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-06-06</td>
<td>Doubleclick</td>
<td>Doubleclick</td>
<td>true</td>
<td>/story/the_skeptic_trailers_and_video_clips_on_yahoo_movies/</td>
</tr>
<tr>
<td>2010-06-06</td>
<td>Doubleclick</td>
<td>Doubleclick</td>
<td>true</td>
<td>/story/the-twilight-saga-david-slade-s-note-to-the-fans/</td>
</tr>
<tr>
<td>2010-06-06</td>
<td>Doubleclick</td>
<td>Doubleclick</td>
<td>true</td>
<td>/story/the-twilight-saga-david-slade-s-note-to-the-fans/</td>
</tr>
<tr>
<td>2010-06-06</td>
<td>Doubleclick</td>
<td>Doubleclick</td>
<td>true</td>
<td>/</td>
</tr>
<tr>
<td>2010-06-06</td>
<td>Doubleclick</td>
<td>Doubleclick</td>
<td>true</td>
<td>/</td>
</tr>
<tr>
<td>2010-06-05</td>
<td>Doubleclick</td>
<td>Doubleclick</td>
<td>true</td>
<td>/</td>
</tr>
<tr>
<td>2010-06-05</td>
<td>Doubleclick</td>
<td>Doubleclick</td>
<td>true</td>
<td>/</td>
</tr>
<tr>
<td>2010-06-05</td>
<td>Doubleclick</td>
<td>Doubleclick</td>
<td>true</td>
<td>/</td>
</tr>
<tr>
<td>2010-06-04</td>
<td>Doubleclick</td>
<td>Doubleclick</td>
<td>true</td>
<td>/video/kiss-bei-rock-am-ring-2010/</td>
</tr>
</tbody>
</table>
Ad Network: Clicksor

Organization Details
- Name: Clicksor
- Publishers Tested: N/A
- Abuse Email: -
- Locations: -

Incident Summary

<table>
<thead>
<tr>
<th>Range</th>
<th>Publishers</th>
<th>Incidents</th>
<th>Drive Bys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Month</td>
<td>294</td>
<td>824</td>
<td>633</td>
</tr>
<tr>
<td>Last 3 Months</td>
<td>300</td>
<td>849</td>
<td>658</td>
</tr>
<tr>
<td>Last Year</td>
<td>303</td>
<td>855</td>
<td>659</td>
</tr>
<tr>
<td>Overall</td>
<td>303</td>
<td>855</td>
<td>659</td>
</tr>
</tbody>
</table>

Weekly Incident Volume

- Incidents
- Drive Bys

Tracking Hosts - 1 Found

<table>
<thead>
<tr>
<th>Host</th>
<th>Incidents</th>
<th>Drive Bys</th>
</tr>
</thead>
<tbody>
<tr>
<td>clicksor.com</td>
<td>823</td>
<td>627</td>
</tr>
</tbody>
</table>

Publishers Affected - More than 15 Found

<table>
<thead>
<tr>
<th>Domain</th>
<th>Alexa Rank</th>
<th>Quantcast Rank</th>
<th>Incidents</th>
<th>Drive Bys</th>
</tr>
</thead>
<tbody>
<tr>
<td>bikini--models.co.cc</td>
<td>-</td>
<td>953,310</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>fulldownload.mu</td>
<td>-</td>
<td>305,597</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>magazine-models.co.cc</td>
<td>-</td>
<td>990,004</td>
<td>27</td>
<td>27</td>
</tr>
<tr>
<td>bikiniswimsuit.co.cc</td>
<td>-</td>
<td>-</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>gadis-models.co.cc</td>
<td>-</td>
<td>-</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>esure--car--insurance.blogspot.com</td>
<td>-</td>
<td>-</td>
<td>15</td>
<td>14</td>
</tr>
<tr>
<td>netne.net</td>
<td>34,043</td>
<td>136,348</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>thedownloadforum.com</td>
<td>870,930</td>
<td>-</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>xtremehost.com</td>
<td>14,874</td>
<td>560,013</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>indomedia.us</td>
<td>-</td>
<td>-</td>
<td>12</td>
<td>12</td>
</tr>
</tbody>
</table>

Most Recent Incidents

- 2010-09-16 clicksor.com neurosoftware.ro true
- 2010-09-16 clicksor.com dlarena.com true
- 2010-09-16 clicksor.com onlinenigeria.com true
- 2010-09-16 clicksor.com onlinenigeria.com true
- 2010-09-15 clicksor.com downloadconvertvideo.com true
- 2010-09-15 clicksor.com downloadconvertvideo.com true
- 2010-09-15 clicksor.com downloadconvertvideo.com true
Ad Network: Doubleclick

Organization Details
Name: Doubleclick
Publishers Tested: N/A
Abuse Email: -
Locations: -

Incident Summary

<table>
<thead>
<tr>
<th>Range</th>
<th>Publishers</th>
<th>Incidents</th>
<th>Drive Bys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Month</td>
<td>64</td>
<td>136</td>
<td>104</td>
</tr>
<tr>
<td>Last 3 Months</td>
<td>72</td>
<td>151</td>
<td>109</td>
</tr>
<tr>
<td>Last Year</td>
<td>81</td>
<td>169</td>
<td>114</td>
</tr>
<tr>
<td>Overall</td>
<td>81</td>
<td>169</td>
<td>114</td>
</tr>
</tbody>
</table>

Weekly Incident Volume

Tracking Hosts - Displaying 1 of 3

<table>
<thead>
<tr>
<th>Host</th>
<th>Incidents</th>
<th>Drive Bys</th>
</tr>
</thead>
<tbody>
<tr>
<td>doubleclick.net</td>
<td>168</td>
<td>113</td>
</tr>
</tbody>
</table>

Most Recent Incidents

<table>
<thead>
<tr>
<th>Date</th>
<th>Host</th>
<th>Publisher</th>
<th>Drive By</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-09-16</td>
<td>doubleclick.net</td>
<td>mixtapekings.com</td>
<td>true</td>
</tr>
<tr>
<td>2010-09-16</td>
<td>doubleclick.net</td>
<td>closecombattraining.com</td>
<td>-</td>
</tr>
<tr>
<td>2010-09-16</td>
<td>doubleclick.net</td>
<td>perfectconnectionongolfswing.com</td>
<td>-</td>
</tr>
<tr>
<td>2010-09-15</td>
<td>doubleclick.net</td>
<td>projectcoreconnect.com</td>
<td>-</td>
</tr>
<tr>
<td>2010-09-11</td>
<td>doubleclick.net</td>
<td>shopping.yahoo.com</td>
<td>-</td>
</tr>
<tr>
<td>2010-09-09</td>
<td>doubleclick.net</td>
<td>protection-av63.co.cc</td>
<td>-</td>
</tr>
<tr>
<td>2010-09-06</td>
<td>doubleclick.net</td>
<td>allseasonspools.com</td>
<td>-</td>
</tr>
</tbody>
</table>

Publishers Affected - More than 15 Found

<table>
<thead>
<tr>
<th>Domain</th>
<th>Alexa Rank</th>
<th>Quantcast Rank</th>
<th>Incidents</th>
<th>Drive Bys</th>
</tr>
</thead>
<tbody>
<tr>
<td>dailyradar.com</td>
<td>3,922</td>
<td>2,452</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>menshealth.com</td>
<td>2,446</td>
<td>581</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>womenshealthmag.com</td>
<td>8,849</td>
<td>1,519</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>wikia.com</td>
<td>199</td>
<td>88</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>freepayingsurveys.com</td>
<td>386,099</td>
<td>29,229</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>ctv.ca</td>
<td>4,216</td>
<td>3,494</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>bottomdollar.com</td>
<td>55,057</td>
<td>3,300</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>huffingtonpost.com</td>
<td>154</td>
<td>32</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>85.12.24.41</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>playlist.com</td>
<td>2,557</td>
<td>255</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
Incident Example

Incident: foxsports.com

<table>
<thead>
<tr>
<th>Summary</th>
<th>Matched Blacklists</th>
<th>Page Thumbnail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id: 1244415</td>
<td>GSB Malware Match: decoy56.info/</td>
<td><img src="image" alt="Page Thumbnail" /></td>
</tr>
<tr>
<td>Found On Date: 2010-07-10 12:50:34.0</td>
<td>GSB Phishing Match:</td>
<td></td>
</tr>
<tr>
<td>Publishing Ad Network: Fox Networks</td>
<td>Subbl Match Lists:</td>
<td></td>
</tr>
<tr>
<td>Delivering Ad Network: Right Media</td>
<td>PhishTank:</td>
<td></td>
</tr>
<tr>
<td>Drive-By Malware: true</td>
<td>Internet Identity:</td>
<td></td>
</tr>
<tr>
<td>Publisher: foxsports.com</td>
<td>RiskIQ Zero Day:</td>
<td></td>
</tr>
<tr>
<td>Publisher Page URL: <a href="http://man.foxsports.com/foxASC">http://man.foxsports.com/foxASC</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blacklisted URL: <a href="http://decoy56.info/a5z/">http://decoy56.info/a5z/</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Embedded Objects:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cause: iframe.src</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content Type:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP Response Code: 0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Overview</th>
<th>URL</th>
<th>Ad Network</th>
<th>Cause</th>
<th>Response Code</th>
<th>Frame</th>
<th>Window</th>
<th>Parent Window</th>
<th>Lost Referrer</th>
<th>Referrer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><a href="http://man.foxsports.com/foxASC">http://man.foxsports.com/foxASC</a></td>
<td>parentPage</td>
<td>200</td>
<td>true</td>
<td>true</td>
<td>TopLevel@4b900a</td>
<td>false</td>
<td><a href="http://noticias.latam.man.com/">http://noticias.latam.man.com/</a>...</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><a href="http://ad.foxnetworks.com/iframe3?yyAAAAVYCBoxVYAAAAAsQFw">http://ad.foxnetworks.com/iframe3?yyAAAAVYCBoxVYAAAAAsQFw</a>...</td>
<td>Fox Networks</td>
<td>frame.arc</td>
<td>302</td>
<td>false</td>
<td>false</td>
<td>Frame@42c1260e</td>
<td>false</td>
<td><a href="http://man.foxsports.com/foxASC">http://man.foxsports.com/foxASC</a>...</td>
</tr>
<tr>
<td>3</td>
<td><a href="http://ad.yieldmanager.com/iframe3?yyAAAAVYCBoxVYAAAAAsQFw">http://ad.yieldmanager.com/iframe3?yyAAAAVYCBoxVYAAAAAsQFw</a>...</td>
<td>Right Media</td>
<td>redirect</td>
<td>200</td>
<td>true</td>
<td>true</td>
<td>Frame@42c1260e</td>
<td>false</td>
<td><a href="http://man.foxsports.com/foxASC">http://man.foxsports.com/foxASC</a>...</td>
</tr>
<tr>
<td>4</td>
<td><a href="http://content.twitstastical.com/track?UglvDQ4RAkC5XVQBZDVMvs">http://content.twitstastical.com/track?UglvDQ4RAkC5XVQBZDVMvs</a>...</td>
<td>Right Media</td>
<td>frame.arc</td>
<td>302</td>
<td>false</td>
<td>false</td>
<td>Frame@32b587ae</td>
<td>false</td>
<td><a href="http://ad.yieldmanager.com/iframe">http://ad.yieldmanager.com/iframe</a>...</td>
</tr>
<tr>
<td>5</td>
<td><a href="http://decoy56.info/a5z/">http://decoy56.info/a5z/</a></td>
<td>redirect</td>
<td>200</td>
<td>true</td>
<td>false</td>
<td>Frame@32b587ae</td>
<td>false</td>
<td><a href="http://ad.yieldmanager.com/iframe">http://ad.yieldmanager.com/iframe</a>...</td>
<td></td>
</tr>
</tbody>
</table>
WHY....
Painting the Big Picture

• All fraudulent schemes begin with Traffic

• The amount of initial traffic a bad guy can receive defines the size of the market

• Larger brands or brands that have not been targeted recently face increased risk
Why these problems exist

• Zero-hour, rapidly changing infrastructure and content

• Lack of Attribution or Identity

• Bad Guy Countermeasures

• Manipulated Trust Metrics
The Zero-Hour

• Real-time indexing, ad exchanges, syndication, Kits

• Moves faster than security filters

• “Under the radar”
  – Fast Flux
  – High Frequency, Low Impact
  – Targets large numbers of users from many hosts
Online Commerce - Trust Issues

• Relative anonymity
• Churn - New players have no track record
• Traffic Transparency
• Transaction Repudiation / Verification – “No Smoking Gun”
Bad Guys Manipulate Trust Metrics

• Maintain impression / click ratios
• Blank or falsify referrers
• Use “threat detectors” to avoid crawlers and manual investigation
• Distribute fraud across multiple personas/accounts/networks
• Operate legit sites & use fraud to gain comp advantage
• Purchase valid traffic – fraud supported arbitrage
Conclusion

• Take **Ownership** of your IP Online – if you don’t someone else will

• **Develop Policies** – Have a general plan/Whitelists

• Understand the **Incentives & Motives** driving fraud, policy violations, Malware

• Develop tests for “**under the radar**” events

• Managing Online Risks is an **opportunity**
Thank you

• RiskIQ:
• 123Tenth Street, San Francisco, Ca 94103
• elias@riskiq.com, gerry@riskiq.com