Security in a Borderless World

Finding Unknown Risks, 0-day Threats and Measurable Enforcement

Elias Manousos
CTO
RiskIQ

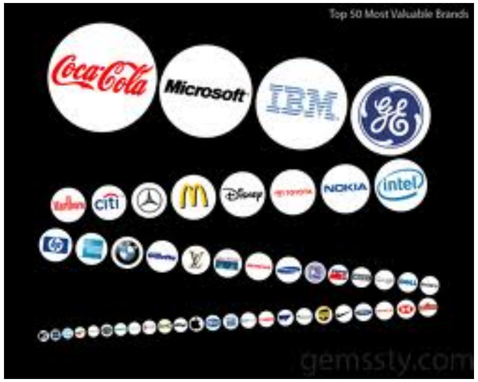
Session Overview

- 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, 3rd Party Email Systems
- Web 2.0 Services
  - LinkedIn, Facebook, Twitter

Brand Examples

- Paid Search Violations

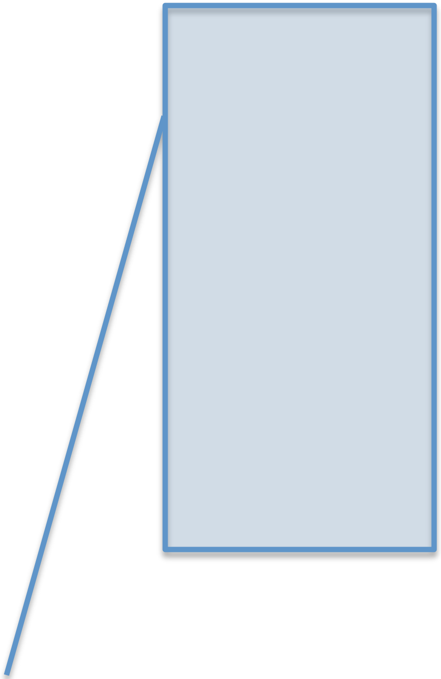
- Trademark Infringement to aide Lead Diversion

- Partner Compliance / Misleading Statements

Paid Search Enforcement

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

COMPANY SPECIFC CONTENT REMOVED



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.

COMPANY SPECIFC CONTENT REMOVED

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.

COMPANY SPECIFC CONTENT REMOVED

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.

COMPANY SPECIFC CONTENT REMOVED

Social Media

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

- COMPANY SPECIFC 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 SPECIFC
CONTENT REMOVED

Partner Compliance

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

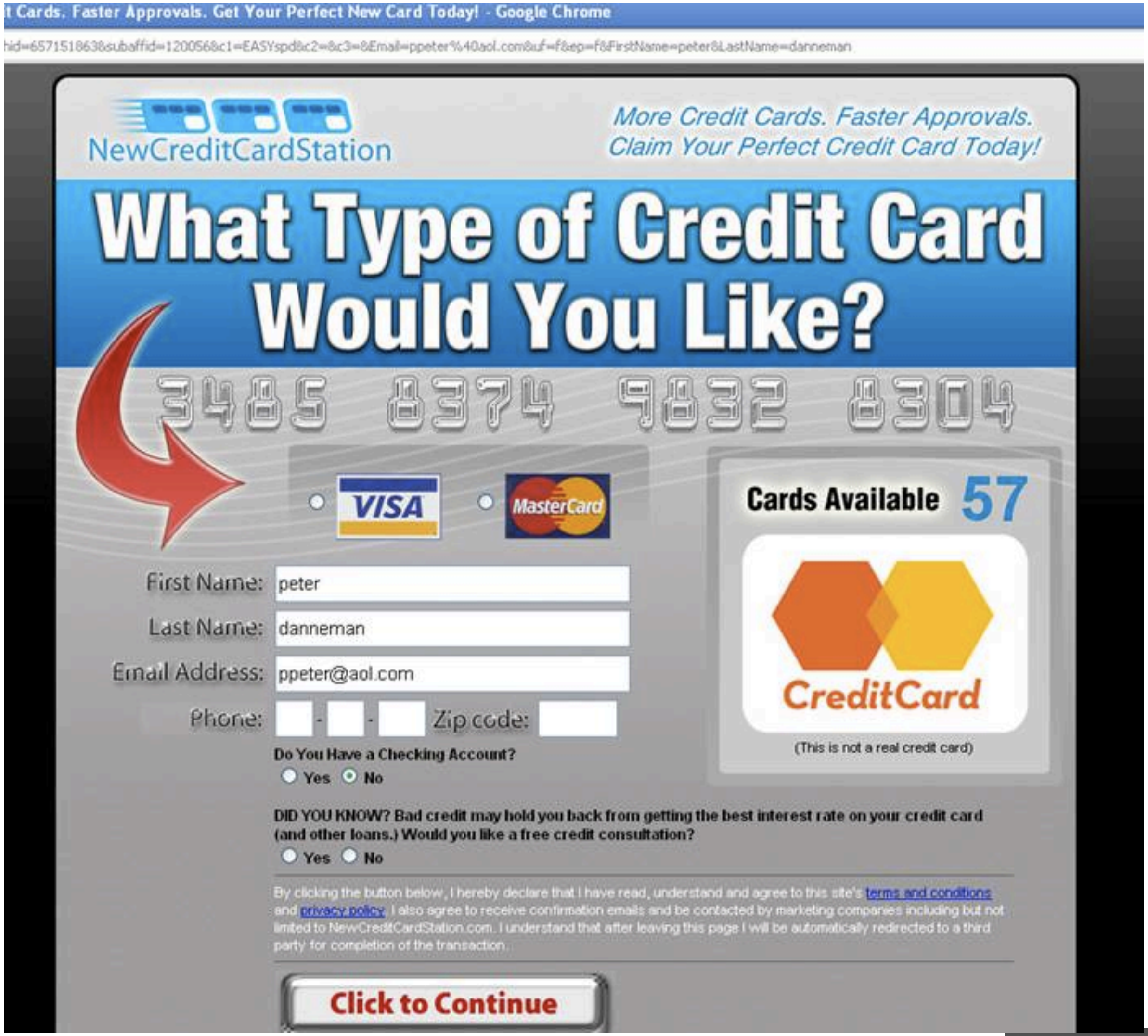
Card Affiliates

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



t Cards. Faster Approvals. Get Your Perfect New Card Today! - Google Chrome

hid=6571518638subaffid=120056&c1=EASYspd&c2=&c3=&Email=ppeter%40aol.com&uf=f&ep=f&FirstName=peter&LastName=danneman

NewCreditCardStation
More Credit Cards. Faster Approvals.
Claim Your Perfect Credit Card Today!
What Type of Credit Card Would You Like?
3485 8374 9832 8304
VISA
MasterCard
Cards Available 57
CreditCard

○ VISA ○ MasterCard

First Name: peter

Last Name: danneman

Email Address: ppeter@aol.com

Phone: - - Zip code:

(This is not a real credit card)

Do You Have a Checking Account?
○ Yes ● No

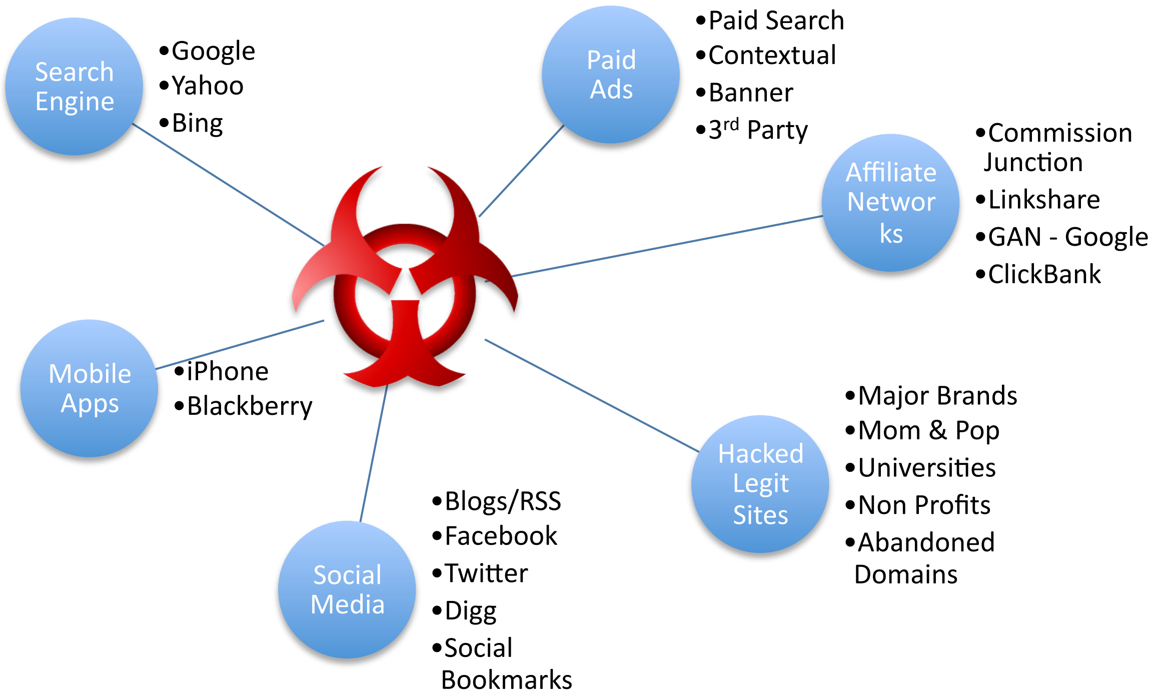
DID YOU KNOW? Bad credit may hold you back from getting the best interest rate on your credit card (and other loans.) Would you like a free credit consultation?
○ Yes ○ No

By clicking the button below, I hereby declare that I have read, understand and agree to this site's terms and conditions and privacy policy. I also agree to receive confirmation emails and be contacted by marketing companies including but not limited to NewCreditCardStation.com. I understand that after leaving this page I will be automatically redirected to a third party for completion of the transaction.

Click to Continue

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 Networ ks
- Commission Junction
- Linkshare
- GAN - Google
- ClickBank

Mobile Apps
- iPhone
- Blackberry

Hacked Legit Sites
- Major Brands
- Mom & Pop
- Universities
- Non Profits
- Abandoned Domains

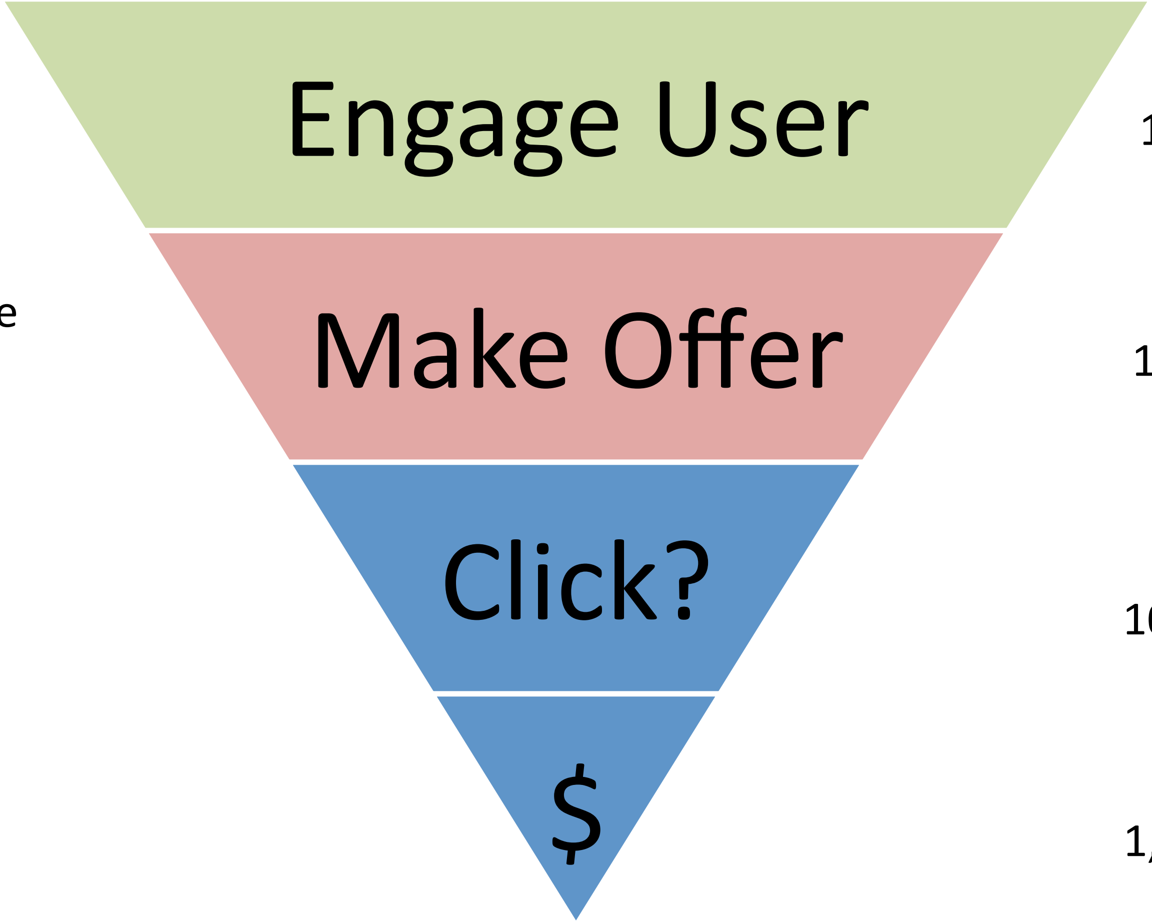
Social Media
- Blogs/RSS
- Facebook
- Twitter
- Digg
- Social Bookmarks

Funnel to Capture Users

This Funnel is True for **Good** And **Bad** Traffic.

It is also accurate for different schemes:

Phish, Malware, Lead Diversion, Affiliate Fraud….



Engage User

Make Offer

Click?

$

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

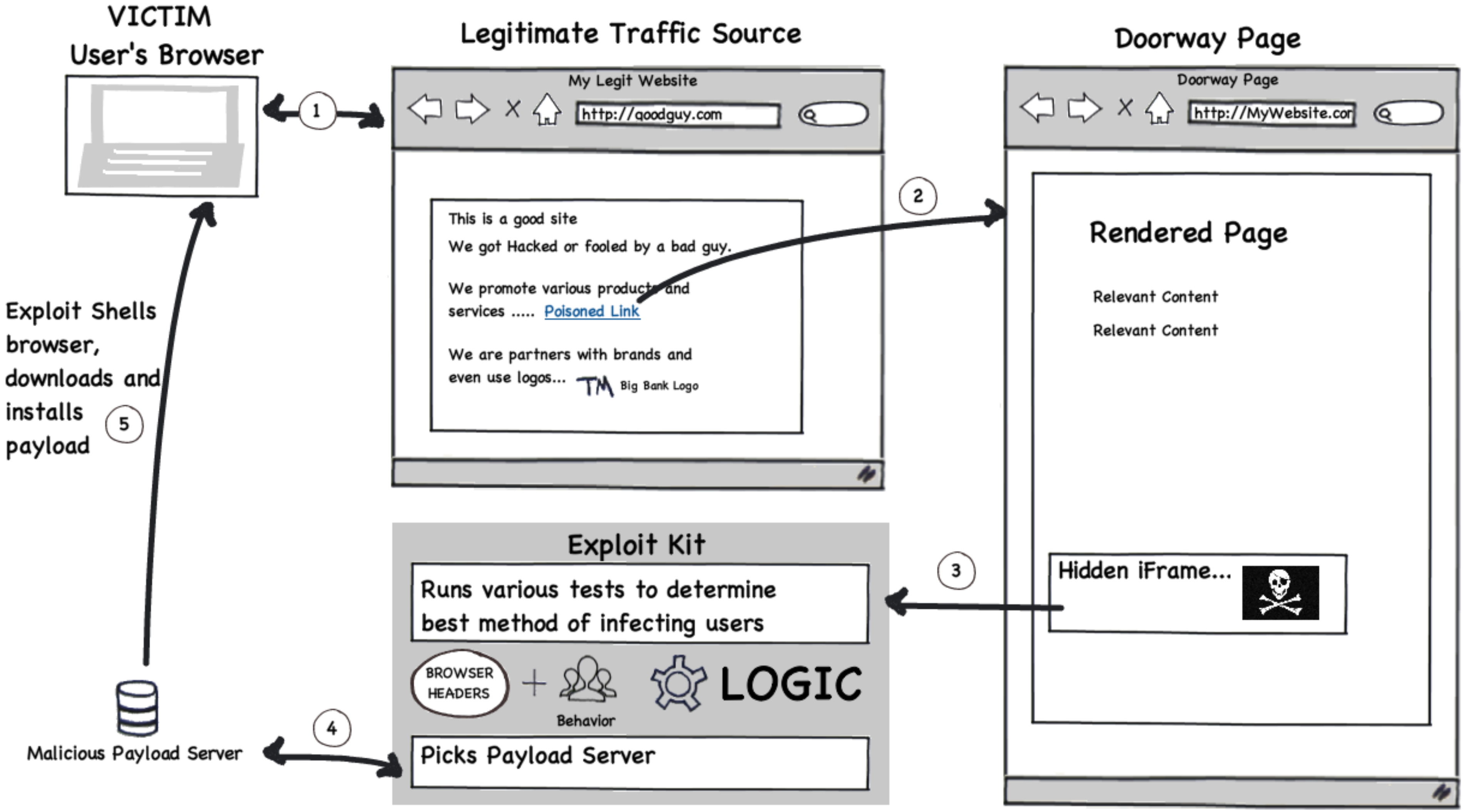
Current Approach is Reactive

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



VICTIM
User's Browser

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

Doorway Page

Doorway Page

http://MyWebsite.cor

Rendered Page

Relevant Content

Relevant Content

Hidden iFrame...

Exploit Kit

Runs various tests to determine best method of infecting users

BROWSER HEADERS + Behavior LOGIC

Picks Payload Server

Malicious Payload Server

Exploit Shells browser, downloads and installs payload

How it happens…

COMPANY SPECIFC CONTENT REMOVED

INFECTED SITE

Infected:

COMPANY SPECIFC CONTENT REMOVED

Infection Point

- COMPANY SPECIFC CONTENT REMOVED

Paid Search: (company) loan

- COMPANY SPECIFC CONTENT REMOVED

INFECTED SITE

- Page 1 on Google!!!
- Possibly a coordinated Adwords Attack
- $11.49 Cost Per Click!
- Scareware

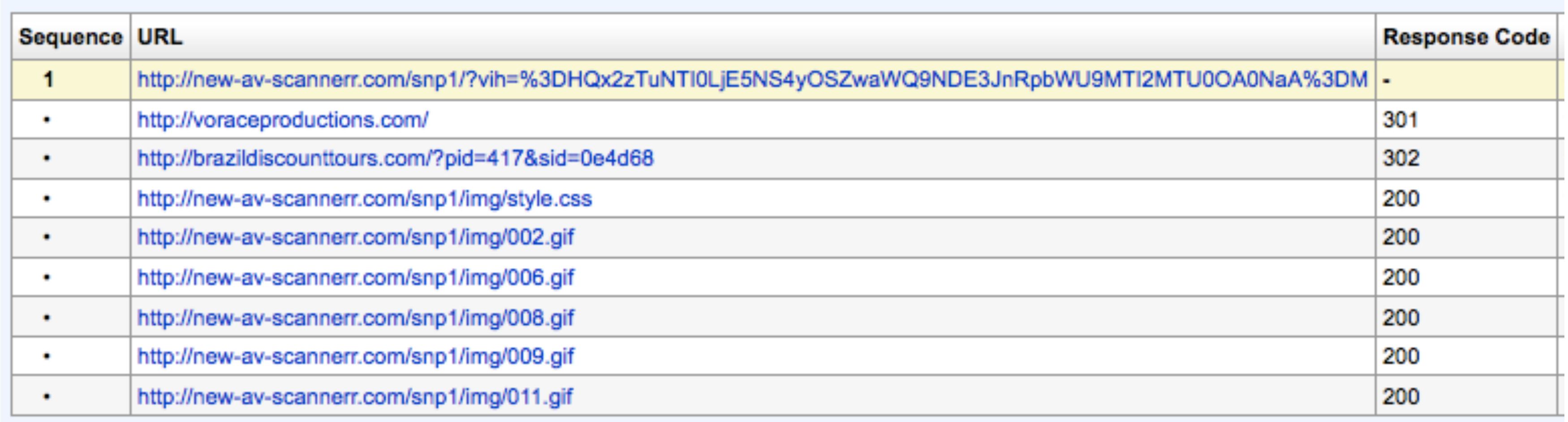
Infected: Fake AV Install

- COMPANY SPECIFC CONTENT REMOVED

↓

Infected: voraceproductions.com

- Use of redirects through 2 infected hosts
- 2nd infected host acts as the hackers ad server?
- new-av-scannerr.com is the scareware host



Sequence	URL	Response Code
1	http://new-av-scannerr.com/snp1/?vih=%3DHQx2zTuNTI0LjE5NS4yOSZwaWQ9NDE3JnRpbWU9MTI2MTU0OA0NaA%3DM	-
•	http://voraceproductions.com/	301
•	http://brazildiscounttours.com/?pid=417&sid=0e4d68	302
•	http://new-av-scannerr.com/snp1/img/style.css	200
•	http://new-av-scannerr.com/snp1/img/002.gif	200
•	http://new-av-scannerr.com/snp1/img/006.gif	200
•	http://new-av-scannerr.com/snp1/img/008.gif	200
•	http://new-av-scannerr.com/snp1/img/009.gif	200
•	http://new-av-scannerr.com/snp1/img/011.gif	200

Scope Overview

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

* Without reach = 14,577

Top 10 Distribution Concepts

```
+---------------------------------+---------------+
| concept                         | incidentCount |
+---------------------------------+---------------+
| X routing number                |            97 |
| bank X loan                     |            79 |
| bank X home loans               |            39 |
| X privacy guard                 |            30 |
| bank X car loan                 |            29 |
| bank X interest rates           |            27 |
| X logins                        |            24 |
| bank X routing number           |            23 |
| bank X online                   |            21 |
+---------------------------------+---------------+
```

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

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 exploting 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

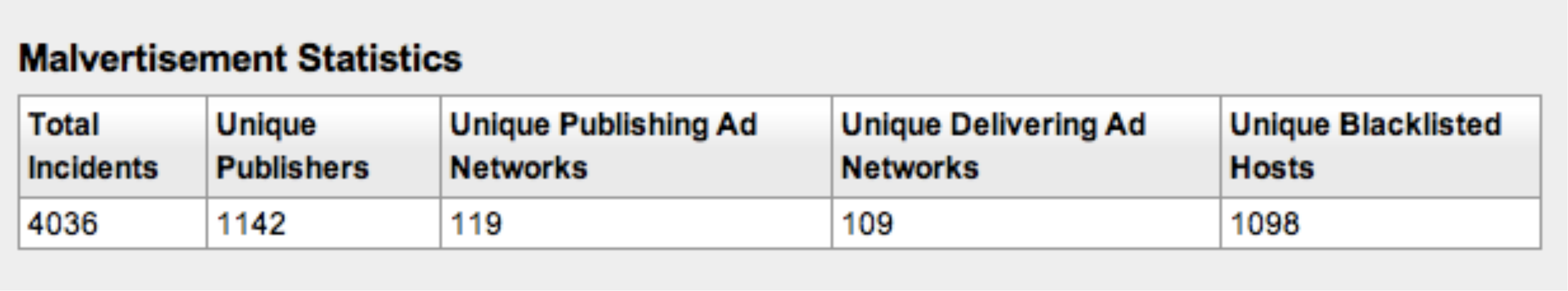
- Step 1: Buy 0day exploit code.
- Step 2: Buy Botnet/malware in underground forum
- Step 3: Buy Malvertisements. Distribute Malware.
- Step 4: Profit.

Malvertisements Status

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

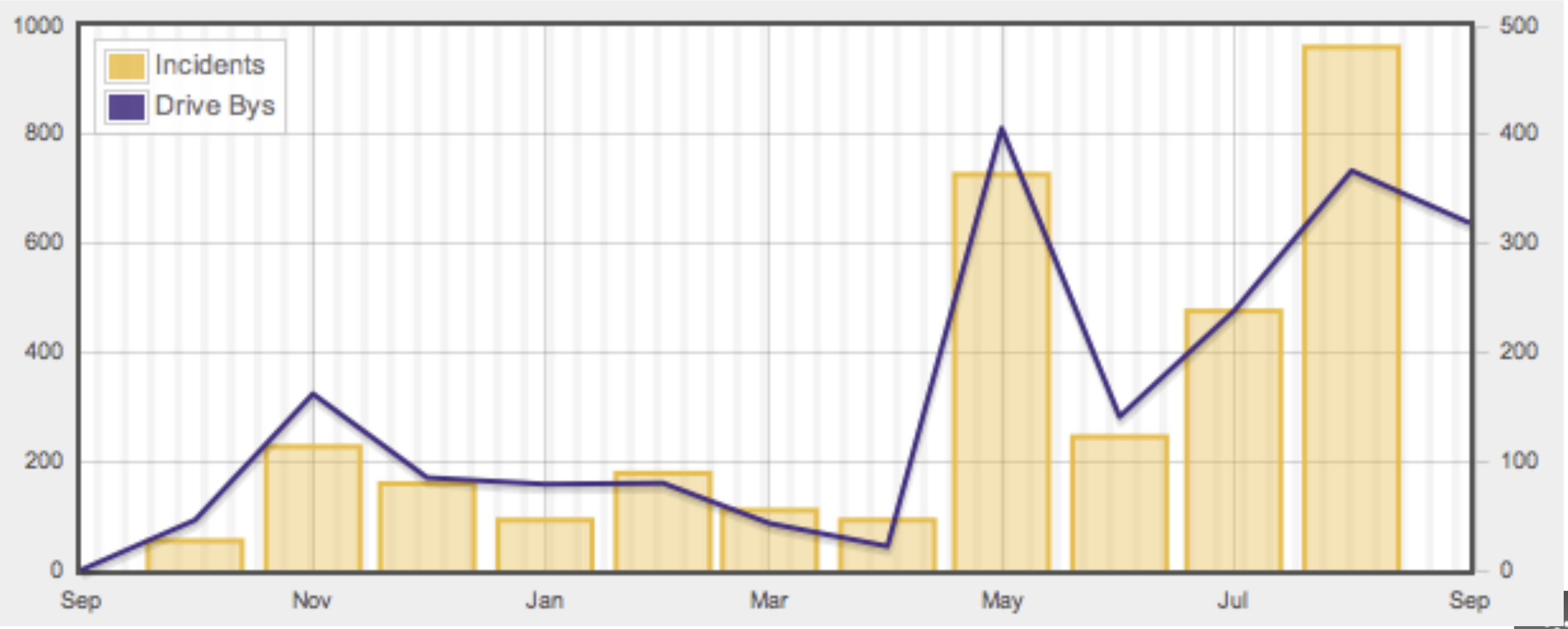
- Metrics are Lacking – this is similar to Data Breach Events prior to legislation (CA SB 1386)
- Publishers find out via customer complaints (similar to Phishing)
- Malvertisements don’t happen often, this doesn’t mean we don’t have a major problem
- Bad Guy success is measured differently from our idea of success – **metrics** expose their business model

Overall Trends

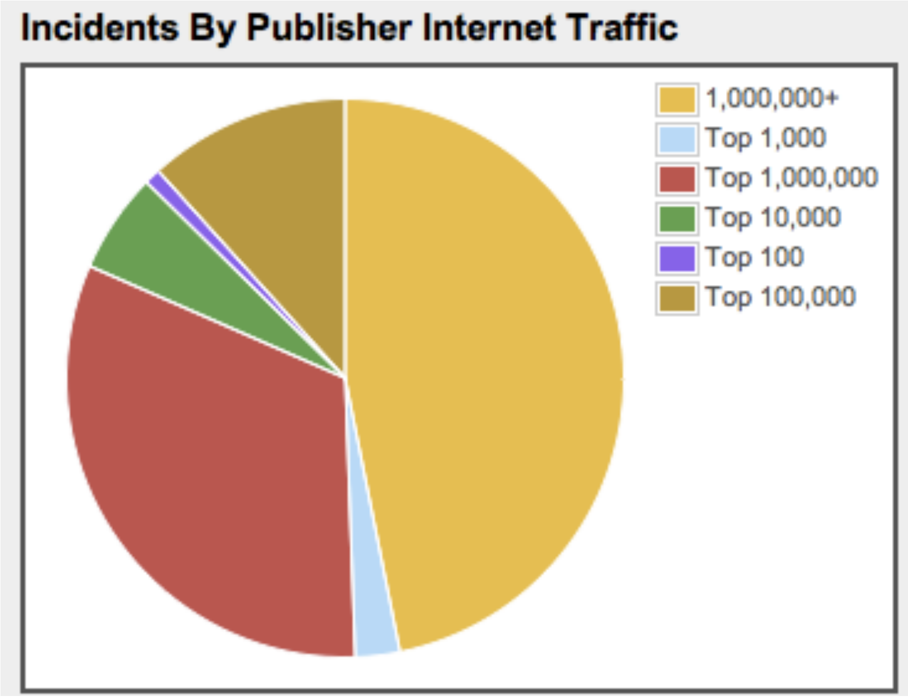


Malvertisement Statistics

Total Incidents	Unique Publishers	Unique Publishing Ad Networks	Unique Delivering Ad Networks	Unique Blacklisted Hosts
4036	1142	119	109	1098



Publisher Size



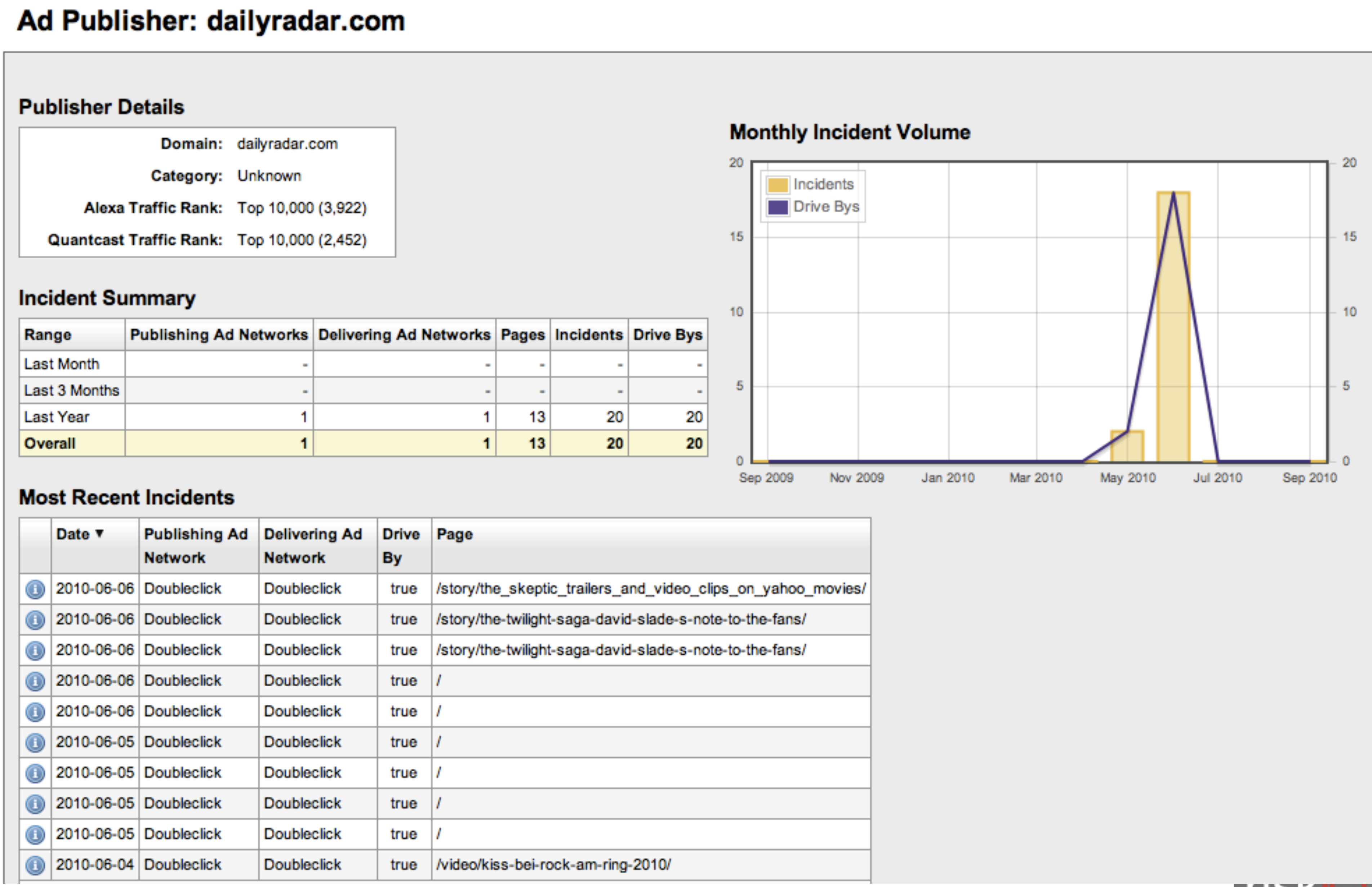
Majority of incidents occur on smaller publisher sites

- 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

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

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)

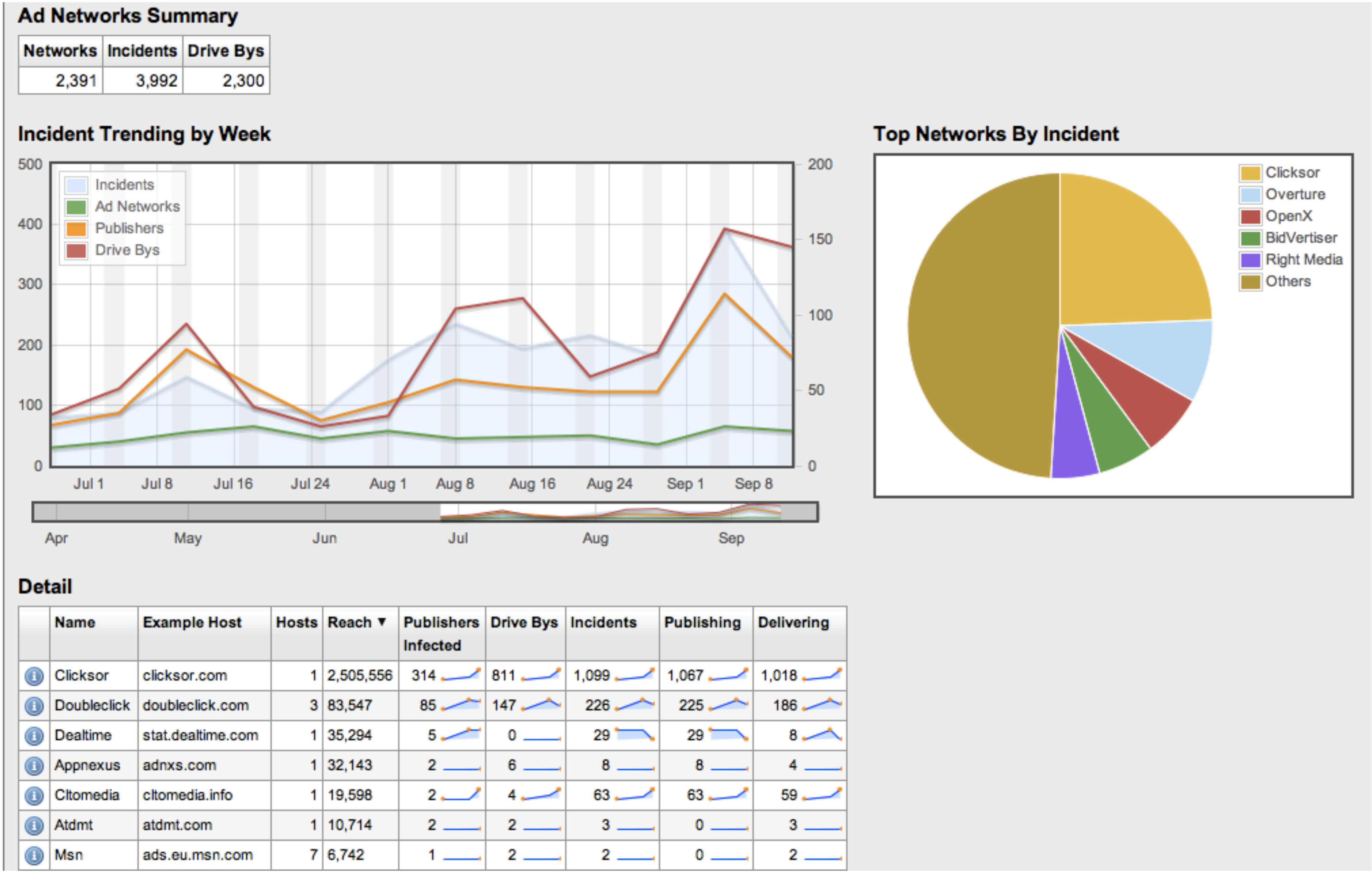
Incident Summary

Range	Publishing Ad Networks	Delivering Ad Networks	Pages	Incidents	Drive Bys
Last Month	-	-	-	-	-
Last 3 Months	-	-	-	-	-
Last Year	1	1	13	20	20
Overall	**1**	**1**	**13**	**20**	**20**

Monthly Incident Volume

Most Recent Incidents

	Date ▼	Publishing Ad Network	Delivering Ad Network	Drive By	Page
ⓘ	2010-06-06	Doubleclick	Doubleclick	true	/story/the_skeptic_trailers_and_video_clips_on_yahoo_movies/
ⓘ	2010-06-06	Doubleclick	Doubleclick	true	/story/the-twilight-saga-david-slade-s-note-to-the-fans/
ⓘ	2010-06-06	Doubleclick	Doubleclick	true	/story/the-twilight-saga-david-slade-s-note-to-the-fans/
ⓘ	2010-06-06	Doubleclick	Doubleclick	true	/
ⓘ	2010-06-06	Doubleclick	Doubleclick	true	/
ⓘ	2010-06-05	Doubleclick	Doubleclick	true	/
ⓘ	2010-06-05	Doubleclick	Doubleclick	true	/
ⓘ	2010-06-05	Doubleclick	Doubleclick	true	/
ⓘ	2010-06-05	Doubleclick	Doubleclick	true	/
ⓘ	2010-06-04	Doubleclick	Doubleclick	true	/video/kiss-bei-rock-am-ring-2010/



Ad Networks Summary

Networks	Incidents	Drive Bys
2,391	3,992	2,300

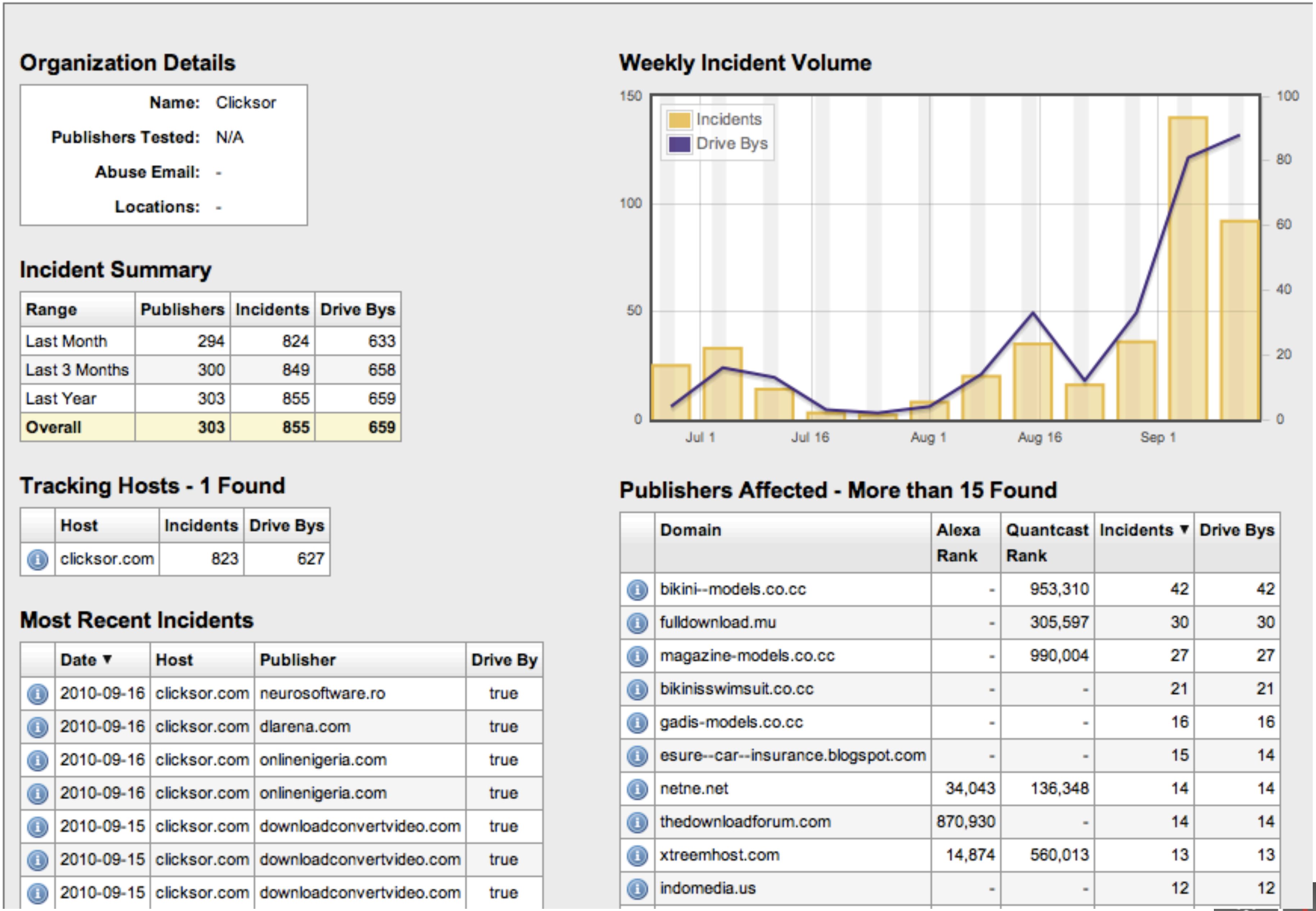
Incident Trending by Week

Top Networks By Incident

Detail

	Name	Example Host	Hosts	Reach ▼	Publishers Infected	Drive Bys	Incidents	Publishing	Delivering
ⓘ	Clicksor	clicksor.com	1	2,505,556	314	811	1,099	1,067	1,018
ⓘ	Doubleclick	doubleclick.com	3	83,547	85	147	226	225	186
ⓘ	Dealtime	stat.dealtime.com	1	35,294	5	0	29	29	8
ⓘ	Appnexus	adnxs.com	1	32,143	2	6	8	8	4
ⓘ	Cltomedia	cltomedia.info	1	19,598	2	4	63	63	59
ⓘ	Atdmt	atdmt.com	1	10,714	2	2	3	0	3
ⓘ	Msn	ads.eu.msn.com	7	6,742	1	2	2	0	2

Ad Network: Clicksor



Organization Details

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

Incident Summary

Range	Publishers	Incidents	Drive Bys
Last Month	294	824	633
Last 3 Months	300	849	658
Last Year	303	855	659
Overall	**303**	**855**	**659**

Tracking Hosts - 1 Found

	Host	Incidents	Drive Bys
ⓘ	clicksor.com	823	627

Most Recent Incidents

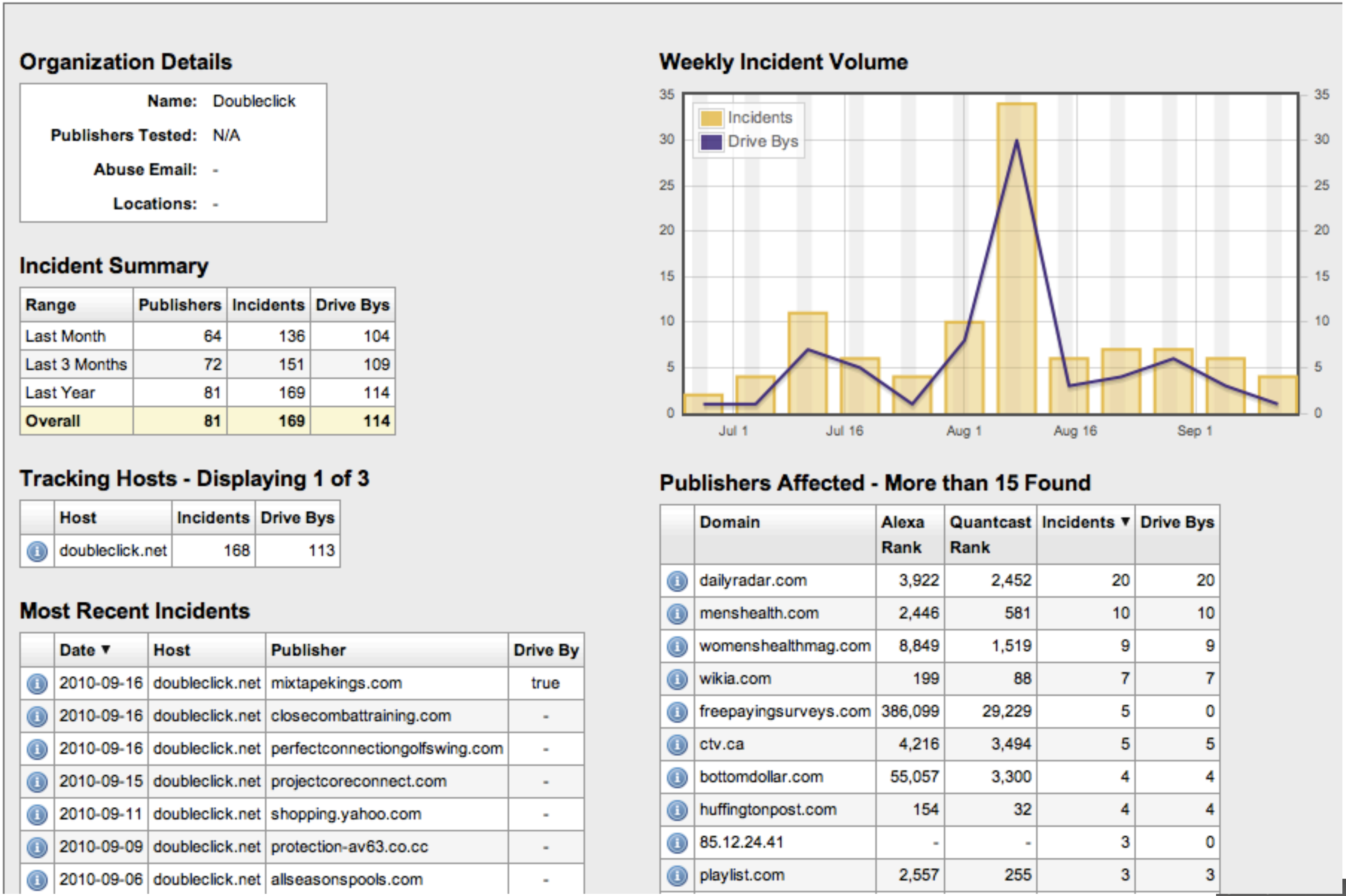
	Date ▼	Host	Publisher	Drive By
ⓘ	2010-09-16	clicksor.com	neurosoftware.ro	true
ⓘ	2010-09-16	clicksor.com	dlarena.com	true
ⓘ	2010-09-16	clicksor.com	onlinenigeria.com	true
ⓘ	2010-09-16	clicksor.com	onlinenigeria.com	true
ⓘ	2010-09-15	clicksor.com	downloadconvertvideo.com	true
ⓘ	2010-09-15	clicksor.com	downloadconvertvideo.com	true
ⓘ	2010-09-15	clicksor.com	downloadconvertvideo.com	true

Weekly Incident Volume

Publishers Affected - More than 15 Found

	Domain	Alexa Rank	Quantcast Rank	Incidents ▼	Drive Bys
ⓘ	bikini--models.co.cc	-	953,310	42	42
ⓘ	fulldownload.mu	-	305,597	30	30
ⓘ	magazine-models.co.cc	-	990,004	27	27
ⓘ	bikinisswimsuit.co.cc	-	-	21	21
ⓘ	gadis-models.co.cc	-	-	16	16
ⓘ	esure--car--insurance.blogspot.com	-	-	15	14
ⓘ	netne.net	34,043	136,348	14	14
ⓘ	thedownloadforum.com	870,930	-	14	14
ⓘ	xtreemhost.com	14,874	560,013	13	13
ⓘ	indomedia.us	-	-	12	12

Ad Network: Doubleclick



Organization Details

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

Incident Summary

Range	Publishers	Incidents	Drive Bys
Last Month	64	136	104
Last 3 Months	72	151	109
Last Year	81	169	114
Overall	**81**	**169**	**114**

Tracking Hosts - Displaying 1 of 3

	Host	Incidents	Drive Bys
ⓘ	doubleclick.net	168	113

Most Recent Incidents

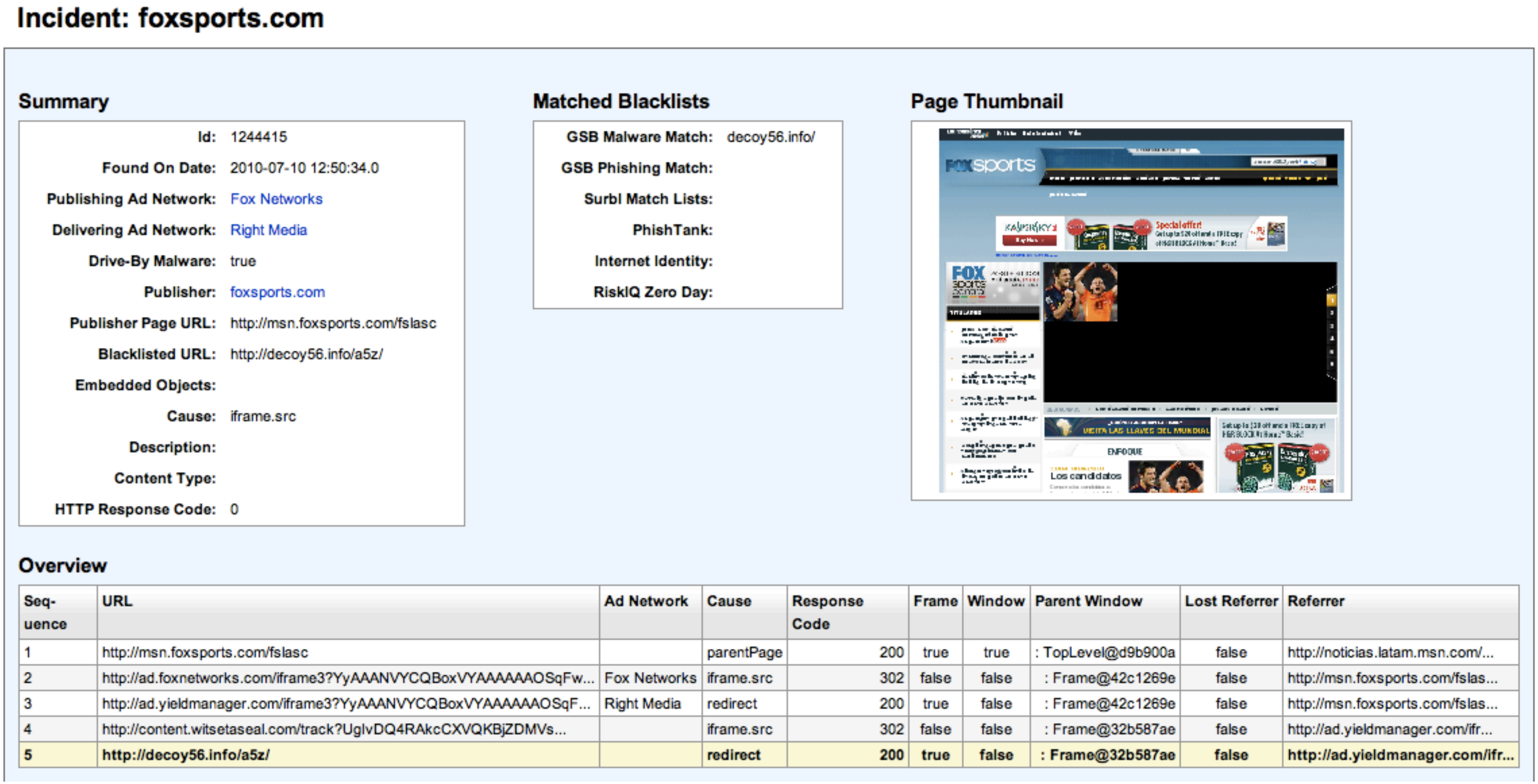
	Date ▼	Host	Publisher	Drive By
ⓘ	2010-09-16	doubleclick.net	mixtapekings.com	true
ⓘ	2010-09-16	doubleclick.net	closecombattraining.com	-
ⓘ	2010-09-16	doubleclick.net	perfectconnectiongolfswing.com	-
ⓘ	2010-09-15	doubleclick.net	projectcoreconnect.com	-
ⓘ	2010-09-11	doubleclick.net	shopping.yahoo.com	-
ⓘ	2010-09-09	doubleclick.net	protection-av63.co.cc	-
ⓘ	2010-09-06	doubleclick.net	allseasonspools.com	-

Weekly Incident Volume

Publishers Affected - More than 15 Found

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

Incident Example



Incident: foxsports.com

Summary

Id:	1244415
Found On Date:	2010-07-10 12:50:34.0
Publishing Ad Network:	Fox Networks
Delivering Ad Network:	Right Media
Drive-By Malware:	true
Publisher:	foxsports.com
Publisher Page URL:	http://msn.foxsports.com/fslasc
Blacklisted URL:	http://decoy56.info/a5z/
Embedded Objects:	
Cause:	iframe.src
Description:	
Content Type:	
HTTP Response Code:	0

Matched Blacklists

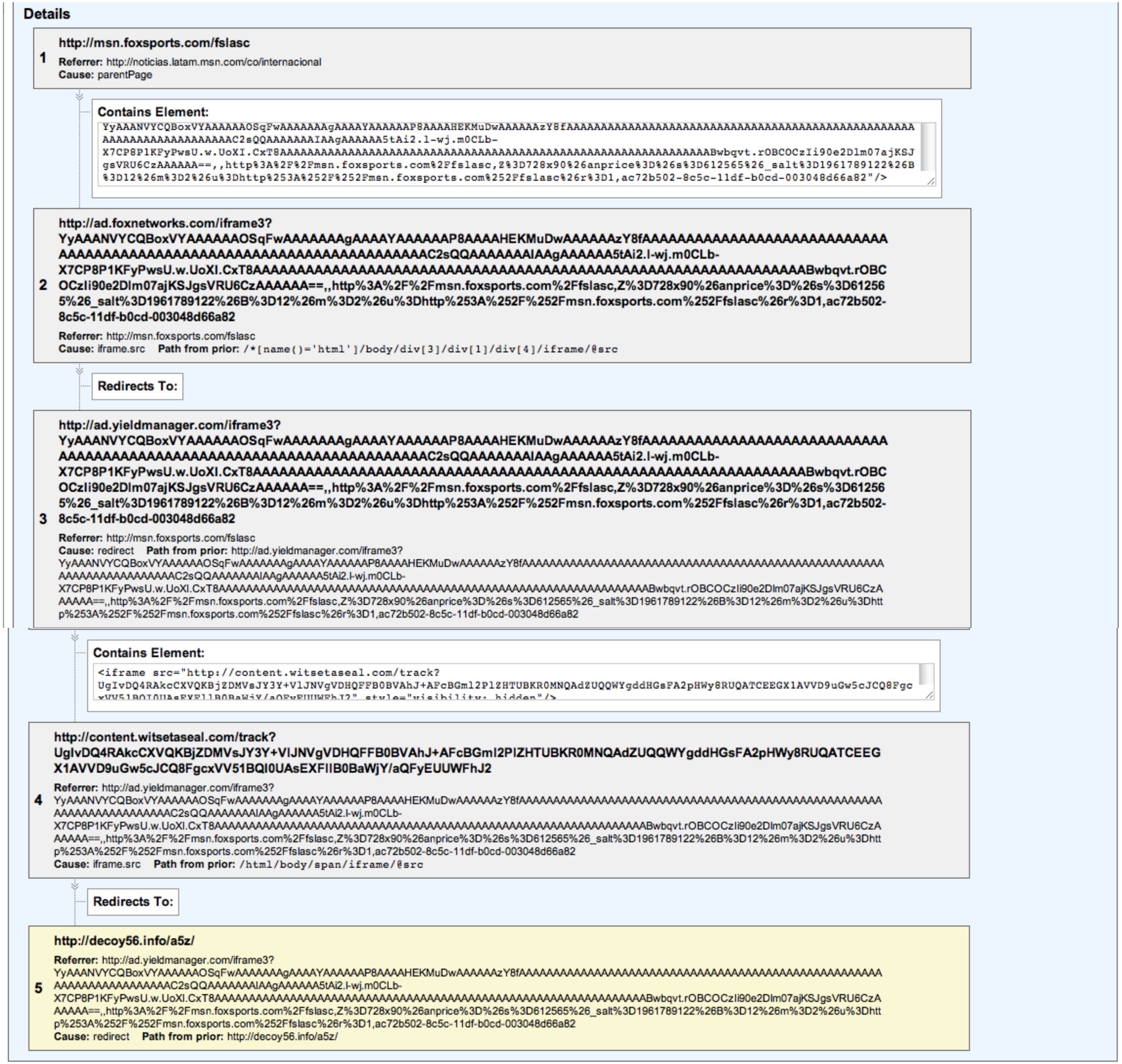
GSB Malware Match:	decoy56.info/
GSB Phishing Match:	
Surbl Match Lists:	
PhishTank:	
Internet Identity:	
RiskIQ Zero Day:	

Page Thumbnail

Overview

Seq-uence	URL	Ad Network	Cause	Response Code	Frame	Window	Parent Window	Lost Referrer	Referrer
1	http://msn.foxsports.com/fslasc		parentPage	200	true	true	: TopLevel@d9b900a	false	http://noticias.latam.msn.com/...
2	http://ad.foxnetworks.com/iframe3?YyAAANVYCQBoxVYAAAAAAOSqFw...	Fox Networks	iframe.src	302	false	false	: Frame@42c1269e	false	http://msn.foxsports.com/fslas...
3	http://ad.yieldmanager.com/iframe3?YyAAANVYCQBoxVYAAAAAAOSqF...	Right Media	redirect	200	true	false	: Frame@42c1269e	false	http://msn.foxsports.com/fslas...
4	http://content.witsetaseal.com/track?UglvDQ4RAkcCXVQKBjZDMVs...		iframe.src	302	false	false	: Frame@32b587ae	false	http://ad.yieldmanager.com/ifr...
5	**http://decoy56.info/a5z/**		**redirect**	**200**	**true**	**false**	**: Frame@32b587ae**	**false**	**http://ad.yieldmanager.com/ifr...**

riskIQ



Details

1 **http://msn.foxsports.com/fslasc**

Referrer: http://noticias.latam.msn.com/co/internacional
Cause: parentPage

Contains Element:

```
YyAAANVYCQBoxVYAAAAAAOSqFwAAAAAAAgAAAAYAAAAAAP8AAAAHEKMuDwAAAAAAzY8fAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAC2sQQAAAAAAAIAAgAAAAAA5tAi2.l-wj.m0CLb-
X7CP8P1KFyPwsU.w.UoXI.CxT8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABwbqvt.rOBCOCzIi90e2Dlm07ajKSJ
gsVRU6CzAAAAAA==,,http%3A%2F%2Fmsn.foxsports.com%2Ffslasc,Z%3D728x90%26anprice%3D%26s%3D612565%26_salt%3D1961789122%26B
%3D12%26m%3D2%26u%3Dhttp%253A%252F%252Fmsn.foxsports.com%252Ffslasc%26r%3D1,ac72b502-8c5c-11df-b0cd-003048d66a82"/>
```

2 **http://ad.foxnetworks.com/iframe3?YyAAANVYCQBoxVYAAAAAAOSqFwAAAAAAAgAAAAYAAAAAAP8AAAAHEKMuDwAAAAAAzY8fAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAC2sQQAAAAAAAIAAgAAAAAA5tAi2.l-wj.m0CLb-X7CP8P1KFyPwsU.w.UoXI.CxT8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABwbqvt.rOBCOCzIi90e2Dlm07ajKSJgsVRU6CzAAAAAA==,,http%3A%2F%2Fmsn.foxsports.com%2Ffslasc,Z%3D728x90%26anprice%3D%26s%3D612565%26_salt%3D1961789122%26B%3D12%26m%3D2%26u%3Dhttp%253A%252F%252Fmsn.foxsports.com%252Ffslasc%26r%3D1,ac72b502-8c5c-11df-b0cd-003048d66a82**

Referrer: http://msn.foxsports.com/fslasc
Cause: iframe.src **Path from prior:** `/*[name()='html']/body/div[3]/div[1]/div[4]/iframe/@src`

Redirects To:

3 **http://ad.yieldmanager.com/iframe3?YyAAANVYCQBoxVYAAAAAAOSqFwAAAAAAAgAAAAYAAAAAAP8AAAAHEKMuDwAAAAAAzY8fAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAC2sQQAAAAAAAIAAgAAAAAA5tAi2.l-wj.m0CLb-X7CP8P1KFyPwsU.w.UoXI.CxT8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABwbqvt.rOBCOCzIi90e2Dlm07ajKSJgsVRU6CzAAAAAA==,,http%3A%2F%2Fmsn.foxsports.com%2Ffslasc,Z%3D728x90%26anprice%3D%26s%3D612565%26_salt%3D1961789122%26B%3D12%26m%3D2%26u%3Dhttp%253A%252F%252Fmsn.foxsports.com%252Ffslasc%26r%3D1,ac72b502-8c5c-11df-b0cd-003048d66a82**

Referrer: http://msn.foxsports.com/fslasc
Cause: redirect **Path from prior:** http://ad.yieldmanager.com/iframe3?YyAAANVYCQBoxVYAAAAAAOSqFwAAAAAAAgAAAAYAAAAAAP8AAAAHEKMuDwAAAAAAzY8fAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAC2sQQAAAAAAAIAAgAAAAAA5tAi2.l-wj.m0CLb-X7CP8P1KFyPwsU.w.UoXI.CxT8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABwbqvt.rOBCOCzIi90e2Dlm07ajKSJgsVRU6CzAAAAAA==,,http%3A%2F%2Fmsn.foxsports.com%2Ffslasc,Z%3D728x90%26anprice%3D%26s%3D612565%26_salt%3D1961789122%26B%3D12%26m%3D2%26u%3Dhttp%253A%252F%252Fmsn.foxsports.com%252Ffslasc%26r%3D1,ac72b502-8c5c-11df-b0cd-003048d66a82

Contains Element:

```
<iframe src="http://content.witsetaseal.com/track?
UgIvDQ4RAkcCXVQKBjZDMVsJY3Y+VlJNVgVDHQFFB0BVAhJ+AFcBGml2PlZHTUBKR0MNQAdZUQQWYgddHGsFA2pHWy8RUQATCEEGX1AVVD9uGw5cJCQ8Fgc
xVV51BQI0UAsEXFlIB0BaWjY/aQFyEUUWFhJ2" style="visibility: hidden"/>
```

4 **http://content.witsetaseal.com/track?UglvDQ4RAkcCXVQKBjZDMVsJY3Y+VlJNVgVDHQFFB0BVAhJ+AFcBGml2PlZHTUBKR0MNQAdZUQQWYgddHGsFA2pHWy8RUQATCEEGX1AVVD9uGw5cJCQ8FgcxVV51BQI0UAsEXFlIB0BaWjY/aQFyEUUWFhJ2**

Referrer: http://ad.yieldmanager.com/iframe3?YyAAANVYCQBoxVYAAAAAAOSqFwAAAAAAAgAAAAYAAAAAAP8AAAAHEKMuDwAAAAAAzY8fAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAC2sQQAAAAAAAIAAgAAAAAA5tAi2.l-wj.m0CLb-X7CP8P1KFyPwsU.w.UoXI.CxT8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABwbqvt.rOBCOCzIi90e2Dlm07ajKSJgsVRU6CzAAAAAA==,,http%3A%2F%2Fmsn.foxsports.com%2Ffslasc,Z%3D728x90%26anprice%3D%26s%3D612565%26_salt%3D1961789122%26B%3D12%26m%3D2%26u%3Dhttp%253A%252F%252Fmsn.foxsports.com%252Ffslasc%26r%3D1,ac72b502-8c5c-11df-b0cd-003048d66a82
Cause: iframe.src **Path from prior:** `/html/body/span/iframe/@src`

Redirects To:

5 **http://decoy56.info/a5z/**

Referrer: http://ad.yieldmanager.com/iframe3?YyAAANVYCQBoxVYAAAAAAOSqFwAAAAAAAgAAAAYAAAAAAP8AAAAHEKMuDwAAAAAAzY8fAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAC2sQQAAAAAAAIAAgAAAAAA5tAi2.l-wj.m0CLb-X7CP8P1KFyPwsU.w.UoXI.CxT8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABwbqvt.rOBCOCzIi90e2Dlm07ajKSJgsVRU6CzAAAAAA==,,http%3A%2F%2Fmsn.foxsports.com%2Ffslasc,Z%3D728x90%26anprice%3D%26s%3D612565%26_salt%3D1961789122%26B%3D12%26m%3D2%26u%3Dhttp%253A%252F%252Fmsn.foxsports.com%252Ffslasc%26r%3D1,ac72b502-8c5c-11df-b0cd-003048d66a82
Cause: redirect **Path from prior:** http://decoy56.info/a5z/

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