OTA
Online Trust Alliance

Best Practices to Detect Fraudulent Customers & Agencies

Summer Koide
VP Product Management
ZEDO

James Koons
Chief Privacy Officer
Listrak

Craig Spiezle
Executive Director
Online Trust Alliance

OTA Mission, Goal & Values

Mission - To enhance online trust, while promoting innovation and the vitality of the internet.

- Goal to help educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity.
- OTA supports collaborative public-private partnerships, benchmark reporting, meaningful self-regulation and data stewardship.

Internet Wide Issue

- Cybercriminals targeting trusted infrastructure
- Compromising the reputation and trust of known mailers, leading web sites and key online brands
  - Sending spam and spear phishing campaigns
  - Deploying botnets and DDos attacked targeting key infrastructure & consumers
  - Exploiting the ad supply chain to deploy malvertising and fraudulent advertising (search & display)

Masquerading as legitimate ….

- Marketers
- Advertisers
- Resellers
- Ad Agencies
- Publishers
- Online Brands
- Financial Institutions
- ……

Impact

- Consumer trust of ads & email
- Brand reputation (advertisers, publishers)
- Drive users to use ad blockers
- Economic impact
- Call for regulation
- Potential of sleeper cells "in waiting"

OTA Ecosystem Approach

- Multi-Stakeholder Collaborative Initiative
  - Advertising & Content Publishing
  - Anti-Botnet Working Group
  - Email Security & Infrastructure
- Goals
  - Publish prescriptive advice
  - Demonstrate collaboration, leadership & self-regulation
  - Advance promising technologies / solutions
  - Highlight early adopters and "North Stars"

A Challenge – "Water Falling"

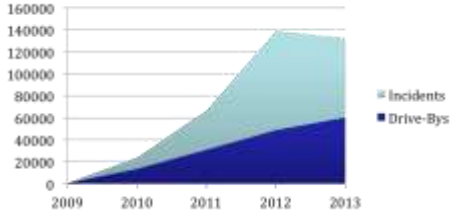
- Get on-boarded, deploy, "wear out their welcome" and jump to a new provider.
- Often start with low volumes and then deploy major "campaign".
- Had we done due diligence we would have seen the red flags.
- If we only knew others had the same issue

The Impact of Malvertising

- Evolving threat with the ability to be a pervasive and damaging threat to legitimate brands and consumers
- Victims - Non-Participatory, highly dynamic and scalable
- Ease of remaining anonymous
- 1 incident = 100,000 impressions
  - Over 10 billon malicious impressions were served in 2012.
  - 42% of malvertising is drive-by exploits, (RiskIQ)
- Upwards of 60% of malvertising can be prevented through onboarding vetting of new customers.

Headlines

Overall Trends – 2013 YTD



- 42% are Drive-bys

Source: RiskIQ

Impact of Spam

- Gaining access to ESPs and trusted IP reputation
- Impacts ESP (and Hosters) and all users on shared resources
- Can result in all mail from an ISP being blocked
- Blacklisted
  - Anti-spam community
  - Web browsers
  - ……

Slide 11

Solution - Framework

- Onboarding review of new customers, agencies partners, resellers
- Vet bad apples from legitimate
- Provide a framework to apply scoring based on their risk tolerance

Malvertising & Ad Fraud

Evaluate the advertiser or agency against risk factors balanced against organization's risk tolerance level and procedures:

1. Ad Serving Domain Reputation
2. Ad Tag Behavior
3. Timing and Urgency
4. Corporate Identity
5. Individual Identity

Advertising Checklist - #1

New Account Risk Evaluation – Check List

	Low Risk (0)	Caution (2)	High Risk (4)
1. Ad Serving Domain Risk Factors			
a. Age – How long has it been registered?	> 12 months	6-12 months	< 6 months
b. How active has the domain or IP been over the last 90 days?	Consistent high activity		Low or No activity
c. Has the domain been recently transferred to or from a 3rd party?	No	Unknown	Yes
d. Is the "Who Is" registration private or by proxy?	No	Unknown	Yes
e. Does the country TLD code match the address of the advertiser contact information?	Yes	Unknown	No
f. Does the site have a physical address that can be validated?	Yes	Unknown	No
2. Ad Tag Risk Factors			
a. Is the ad tag obfuscated or use flash code?	No	Unknown	Yes
b. Does the ad tag trigger security warnings?	No	Unknown	Yes
c. Does the ad creative offer security or PII or enhanced privacy offerings?	No	Unknown	Yes *
3. Timing and Urgency Risk Factors			
a. Is the engagement a last minute insertion order, or before a holiday?	No		Yes
b. Is the order inbound and unsolicited?	No		Yes
c. Is the order pressed?	No		Yes
d. High CPM (a premium, over value to inventory)	No		Yes
e. Does the ad targeting "make sense" for this advertiser or agency?	Yes		No

Advertising Check List - #2

	Low Risk (0)	Caution (2)	High Risk (4)
4. Corporate / Website Risk Factors			
a. Do they have a DUNS number (Data Universal Number)?	Yes	No	Yes
b. Does the website appear to be unprofessional or have multiple obvious errors?	No		Yes
c. Is the privacy policy discoverable on the home page of the site?	Yes		No
d. Does the site have an insecure SSL connection, a mismatched SSL certificate or expired SSL certificate?	No	Unknown	Yes *
e. Does the site have malware or known exploits?	No	Yes	Yes
f. Does the site list corporate officers and lines which can be validated via other sites?	Yes	No	No
g. Do they participate in any privacy self-regulatory programs?	Yes		No
h. Are they members of industry organizations which promote best practices, transparency and accountability?	Yes		No

Advertising Check List - #3

	Low Risk (0)	Caution (2)	High Risk (4)
5. Individual Risk Factors			
a. Pass or no industry contacts, references or reliable and consistent search data	No		Yes
b. Can you validate the identity of the contact?	Yes		No
c. Does the email address (domain) correspond to corporate site? (both the "from" and "reply" email addresses)?	Yes		No
d. Does the reply email address bounce?	No		Yes
6. Reputational / Other			
a. Is the company in a known vertical that has historically been exploited by bad actors? (at risk segments include nutraceuticals, payday loans, stock tips, security, anti-virus products or solutions);	No		Yes
b. Can you check their reputation with another known and trusted service provider?	Yes		No
c. Do they frequently change service providers, agencies or ad servers?	No		Yes
TOTAL			

Cloud Services & Hosters

- Key risk factors
  - Domain reputation
  - Past complaints
  - Timing and Urgency
  - Corporate Identity
  - Individual Identity
  - Data Use

Cloud & Hosters

New Account Risk Evaluation – Check List

	Low Risk (0)	Caution (2)	High Risk (4)
1. Domain Risk Factors			
a. Age – How long has the domain been registered?	> 12 months	6-12 months	< 6 months
b. Activity – How active has the domain or IP been over the last 90 days?	Consistent activity		No activity
c. Has the domain been recently transferred to or from a 3rd party?	No	Unknown	Yes
d. Is the "Who Is" registration private or by proxy?	No	Unknown	Yes
e. Does the country TLD code match the address of the customer contact information?	Yes	Unknown	No
f. Does the site have a physical address that can be validated?	Yes	Unknown	No
g. Does the corporate domain utilize SPF, DKIM & DMARC for their TLD and subdomains?	Yes		No
2. Reputation Risk Factors			
a. Has the company or contact ever been blocked by a third party anti-abuse or anti-spam organization?	No	Unknown	Yes
b. Validate the forecasted daily traffic or volumes, are they realistic?	Yes	Unknown	No
c. Can you check their reputation with previous service provider?	Yes		No
d. Do they frequently change service providers?	No		Yes
e. Is the company in a known vertical that has historically been exploited by bad actors? (at risk segments include nutraceuticals, payday loans, stock tips, security, anti-virus products or solutions);	No	Unknown	Yes *

Cloud / Hosters #2

Cloud Hosters #3

Summary Call to Action

- Review your current procedures.
- Review those of your partners / resellers (down steam threat).
- Customize framework based on your risk tolerance
- Educate account teams.
- Establish out of band process / escalation.
- Develop remediation plan.
- Review collaboration and sharing data to help curb “water falling”.

Resources

- Anti-Malvertising / Ad Integrity https://otalliance.org/resources/malvertising.html
- Anti-Botnet Multi-Stakeholder Working Group https://otalliance.org/botnets.html
- Email Security & Authentication https://otalliance.org/eauth.html
- Data Protection & Privacy https://otalliance.org/breach.html
- 2013 Honor Roll https://otalliance.org/2013HonorRoll.html
- Infrastructure https://otalliance.org/ssl.html

 Slide 22

Get Involved

Friday, October 4, 9 AM PDT / Noon EST
Anti-Botnet Remediation Best Practices
Register at https://cc.readytalk.com/r/6xwcmo5v6cev&eom

Sponsor OTA
craigs@otalliance.org
425-455-7400