Cyber Security Threats in Digital Advertising

Karl Dominguez
Introduction

- IBM Business Services, Threat Analyst
- Malware Research and Software Development, zvelo Inc.
- Mobile Malware Analyst, Asurion LLC
- Threat Research Engineer, Trend Micro
Topics

- Digital Advertising Economy
- Ad Tech Ecosystem
- The Ad Fraud:
  - Publisher-based Ad Fraud
  - Malicious and “Objectionable” Content
  - Non Human Traffic
- The Bieber Project
Digital Advertising Economy

US Digital Ad Spending for 2016 is at $72 billion

Source: https://www.emarketer.com/Article/US-Digital-Ad-Spending-Surpass-TV-this-Year/1014469
Ad Tech Ecosystem
Ad Tech Ecosystem

Advertiser
Ad Agency
Demand Side Platform
Ad Exchange
Supply Side Platform
Publisher
Setting up a Campaign

Website Campaign

General

Budget

Max CPM Bid: $3.00
Budget: $100.00

Spend evenly throughout the day

Note: A budget may take up to 60 seconds to take effect. High volume sites sometimes cause overspend.

Flight Dates: All Days

Location

Geographic: Browse & Add Locations

DMA Code: Enter codes separated by commas
Zip/Postal Code: United States

Next Step
Setting up a Campaign - Criteria
Setting up a Campaign

### Website Campaign

<table>
<thead>
<tr>
<th>General</th>
<th>inventory</th>
<th>Your Ads</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>tvropes.org</td>
<td>186</td>
<td>Uncategorized</td>
<td>33Across</td>
</tr>
<tr>
<td>sharetv.com</td>
<td>27</td>
<td>Uncategorized</td>
<td>33Across</td>
</tr>
<tr>
<td>realclear.com</td>
<td>8</td>
<td>Uncategorized</td>
<td>33Across</td>
</tr>
</tbody>
</table>

#### Chosen Inventory

<table>
<thead>
<tr>
<th>Site ID</th>
<th>Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>73-1297726</td>
<td>wizard101central.com</td>
</tr>
<tr>
<td>73-1144378</td>
<td>superheroyme.com</td>
</tr>
<tr>
<td>73-1195103</td>
<td>sharetv.com</td>
</tr>
<tr>
<td>73-1256991</td>
<td>quizon.com</td>
</tr>
</tbody>
</table>

- Viewing 126 of 40960
- 4 Sites

Back  
Next Step  
Cancel
Setting up a Campaign – Uploading Creative
The Ad Fraud Problem

- Deliberate practice of attempting to serve ads that have no potential to be viewed by a human user.
- Lots of varying statistics regarding the extent of the problem.
- Estimates range from 13% to as high as 60% of impressions served online were “suspicious”.
Show me the Money!

- Who makes money out of this?
  - **Traffic Sellers** - The people who sells traffic to publishers.
  - **Publishers** - The publishers who buys the traffic and get money off the advertisers.

What can we do about it?
Interactive Advertising Bureau

- What is the IAB?
- Released a Ad Fraud Taxonomy

IAB Ad Fraud Taxonomy

- **Illegitimate and Non-Human Traffic Sources**
  - Hijacked device
  - Crawler masquerading as a legitimate user
  - Data-center traffic

- **Non-traditional / other traffic**
  - Proxy traffic
  - Non-browser User-Agent header
  - Browser pre-rendering

- **Hijacked Tags**
  - Ad Tag Hijacking
  - Creative Hijacking

- **Site Impression Attributes**
  - Auto-Refresh
  - Ad Density
  - Hidden Ads
  - Viewability
  - Misappropriated Content
  - Falsely Represented
  - Non Brand Safe
  - Contains Malware

- **Ad creative / other**
  - Cookie Stuffing
101: What it Really Means

*There are basically 3 main types of Ad Fraud:*

1. Publisher tricks to Increase Impression Count
2. Illegal or Malicious Content
3. Use of Non Human Traffic to Increase Impressions
Publisher Tricks to Increase Impression Count

- Various techniques that publishers use to make an Ad impression look like more.

- Some prominent examples are:
  - Hidden Ads
  - Ad Stacking
Publisher Tricks to Increase Impression Count

What the advertiser wants:

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.
Publisher Tricks to Increase Impression Count

But some publishers will do this (Hidden Ads):

1x1, nx1, 1xn, 0xn, nx0 iFrames
Publisher Tricks to Increase Impression Count

Or this (Ad Stacking):

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.
Objectionable or Malicious Content

- Malvertisiting
- Greyware
- Scams
- Objectionable Content
Illegal or Malicious Content
Illegal or Malicious Content

Ad network was serving malware!
Illegal or Malicious Content

Adware
Ads that will serve you more Ads
Illegal or Malicious Content

Scamvertising!
Illegal or Malicious Content

Libreng gift certificate worth P20,000

Choose your gift certificate

- Sodexo
  - P20,000
- Robinsons
  - P20,000
- Puregold
  - P20,000
Use of Non Human Traffic to Increase Impressions

- Bots. This is probably the most common thing that comes to mind.

What is the best way to investigate this?
Buying Internet Traffic

What is Purchased Internet Traffic made of?

Can I buy internet traffic and get away with it?
The Bieber Project

Justin Bieber Ultimate Fan Blog
Honeypot

Bieber with a “Wire”

Collected Information

Fraudulent Impressions?
Bieber with A Wire
Traffic Vendors

**Buy Website Traffic**

Are you looking for the easiest way to get a huge traffic boost on your website? Maxvisits.com is here to meet your needs! We can deliver traffic from 45 different countries, targeted for your site category, from as low as $1 per 1,000 visitors.

That’s right, our cheap traffic will bring you targeted visitors, customers, rankings improvement and most importantly real web traffic. Your site will be the proud recipient of a steady flow of website visitors, and this will finally lead to your success as a site owner.

There are plenty of businesses online that offer to buy website traffic, but not all of them are going to be beneficial to your website. We offer top level visitors to your site for the best prices and we will not fail you.

*We have provided 1,486,225,000 visitors to our loyal customers!*
Traffic Vendors

Traffic specialist
www.bringvisitor.com

The No.1 choice for buying web traffic!

Log in    Free sign up

Home    Visit traffic    Click traffic    Targeted traffic    Reviews    More service    Member center

Bulk Traffic
Up to 55,000 unique visitors per day

$9.99

100% real visitors from 24-hour unique ips
Refund guaranteed
Excellent customer service
0% risk to skyrocket your web traffic

25,000 unique visitors (3,000-4,000 unique visitors per day for 7 days!)

Clicks
For votes, ads, links...
Traffic Vendors

You can customize and set up your own traffic campaign below. We offer dozens to choose from, 1,000 visitors to 250,000 visitors, VisitorZoom will give your site the boost it needs. Just setup a campaign, sit back, and watch new targeted visitors arrive to your site!

Choose amount of visitors

- 1,000 visitors
- 2,500 visitors
- 5,000 visitors
- 10,000 visitors

ORDER TOTAL: $0.00

Checkout
Traffic Market Places

I will 15000 Safe visitors 400 to 500 Daily Website Traffic

I will send 600 daily quality USA social network traffic for

I will deliver Guaranteed Search Traffic

I will send real social 3500 keyword target Website Traffic

I will send UNLIMITED Google Search Traffic

I will help get TRAFFIC to your Website

$5

$5

$5

$5

$5

$5
Traffic Market Places

SEO Marketplace

Search Results: traffic

UNLIMITED HUMAN TRAFFIC BY Google Facebook Twitter Yo... for $29
unlimited verified unique human traffic by google facebook twitter youtube pinterest l...

Sort by:

TrafficDemon - Generate UNLIMITED TRAFFIC For Life for $24
looking to give your stats a nice boost or skyrocket them! or even start your own webs...

Deliver 11000 Real Human Adult Targeted Traffic from ... for $25
if you are looking for quality and real human adult visitors to your website, this is...
What is Purchased Internet Traffic Made Of?
Well... obviously BOTS!
How do we know?

Clues are in the Impression...
There are Lots of Clues…

A browser can provide a lot of clues…

Look for suspicious information…

- Plugins
- Mime Types
- Screen Attributes
- Window Attributes
- Product identifiers
- Navigator Attributes
- Location Attributes
- Frame Rates
- Browser Rendering Attributes
- User Agents
- JavaScript Enabled
- Cookies Enables
- And many more…
Clues

Analyzing Impression 2 ...

- BrowserVersion: 5.0 (Macintosh; Intel Mac OS X 10_10_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.90 Safari/537.36
- SERVER_NAME: justinfan.zerodeays.org
- LocationPort: 
- BrowserLanguage: en-US
- SCRIPT_FILENAME: /home/content/r/y/a/ryantalabis/html/justinfan/record.php
- MimeTypeLength: 0
- PATH_TRANSLATED: 
- ScreenAvailableHeight: 1057
- HistoryLength: 2
- LocationRef: http://justinfan.zerodeays.org/
- BrowserOnline: TRUE
- LocationHost: justinfan.zerodeays.org
- SCRIPT_NAME: /record.php
- PluginName: Widevine Content Decryption Module+Chrome PDF Viewer+Shockwave Flash+Chrome Remote Desktop Viewer+Native Client+Chrome PDF Viewer+
- DocumentReferrer: 
- HTTPS: 
- HTTP_ACCEPT_CHARSET: 
- REQUEST_METHOD: GET
- HTTP_CONNECTION: keep-alive
- REMOTE_ADDR: 122.53.187.210
- REMOTE_PORT: 53501
- WindowScreenY: -161
- WindowScreenWidth: -1917
- SERVER_ADMIN: support@supportwebsite.com
- HTTP_ACCEPT_LANGUAGE: en-US;en;q=0.8
- HTTP_ACCEPT_ENCODING: gzip, deflate, sdch
- SERVER_ADDR: 173.201.211.56
- HTTP_USER_AGENT: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.90 Safari/537.36
- HTTP_REFERER: http://justinfan.zerodeays.org/
- WindowPageXOffset: 0
- REMOTE_HOST: 
- WindowOuterHeight: 1049
- REQUEST_TIME_FLOAT: 
- ScreenWidth: 1020
- WindowTop: TRUE
- BrowserGoo: 
- LocationHostName: justinfan.zerodeays.org
- JavaEnabled: TRUE
- CookiesEnabled: TRUE

zvelo proprietary and confidential
Some clues are obvious…
Traffic Generators

Miracle Traffic Bot™
One Click Submission & SEO Automation Software

I Got Massive Traffic!
I Got Quality Backlinks!
I Made More Money!

Perpetual Traffic Generator

Creates A Self-Feeding, Never-Ending Stream of Prospects

Push Button Traffic Getting Robot Pulls 101,488 Visitors Per Month
...And Gets Top Search Engine Rankings, More Backlinks and Massive Boost in Sales - Guaranteed!

Brand *NEW* Traffic Software Generates 867,981 Targeted Visitors On Autopilot And Banks $540,430.00...

Without Software
17,726 Visitors

With Software
867,981 Visitors

$540,430.00

Download Here
Traffic Demon

TrafficDemon - Generate UNLIMITED TRAFFIC For Life for $24

Created 1 year ago in Bots

TrafficDemon
Generate Unlimited Website Traffic 24/7

Looking to give your stats a nice boost (or skyrocket them!) or even start your own website traffic business? In either case you have found the last software package you will ever need!
Traffic Spirit (also known as Traffic Ghost)
Fake Traffic Generator

Website Information
URL(s) To Visit (1 Per Line):
http://referringsite.com/

Referring URL's To Use (Optional):
https://facebook.com/
https://youtube.com/

Browser Data
Useragents To Use:
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43
Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2383.0
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/...
Visitor Maker
Tunkas Hits Generator

Referrers show where visitors come from!

Referring URL: http://

Referring URLs: 6181

- http://www.yahoo.com/
- http://www.google.com/
- http://www.microsoft.com/
- http://www.usatoday.com/
- http://www.zdnet.com/
- http://www.sun.com/
- http://www.sun.com/
- http://www.lycos.com/
- http://www.real.com/
- http://www.macromedia.com

zvelo proprietary and confidential
Dominator

![Shorte.st Dominator v1.1.0 window](image)

- **File** menu
- **Edit** menu
- **Help** menu

**URLs (One Per Line):**
- http://sh.st/tsf2
- http://sh.st/tsl1
- http://sh.st/tsidS

**Hits (Per URL):**
- 1000
- 88.159.140.239:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80

**Wait Before Skip:**
- 5 to 18
- 88.159.99.32:80
- 91.209.67.1:8080
- 91.209.67.0:8080
- 91.209.67.0:8080
- 91.209.67.0:8080
- 91.209.67.0:8080
- 91.209.67.0:8080
- 91.209.67.0:8080
- 91.209.67.0:8080

**Wait After Skip:**
- 7 to 48
- 88.159.99.32:80
- 91.209.67.1:8080
- 91.209.67.0:8080
- 91.209.67.0:8080
- 91.209.67.0:8080
- 91.209.67.0:8080
- 91.209.67.0:8080
- 91.209.67.0:8080
- 91.209.67.0:8080

**Delay Between Hits:**
- 34 to
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80

**Threads:**
- 1

**Referrers (Optional):**
- Hits: 0
- Proxy: 0.0.0.0
- Status: Idle

**Proxies (Optional):**
- 88.159.140.239:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80
- 88.159.99.32:80

**Buttons:**
- Import URLs List
- Import Referrers List
- Import Proxies List
- Start
- Stop

- Use Proxies Once Only
- Disable Proxies
Auto Web Bot
Traffic Exploder

Traffic Exploder v1.04 - Enter your Website URL(s) and views then click Go to begin.

URL(s)
http://www.reddit.com

Views | View for | Threads | Timeout
--- | --- | --- | ---
100 | 10 to 30 Seconds | 16 | 12 | Stop

Use HMA VPN (Requires software + Subscription)

Working.

<table>
<thead>
<tr>
<th>Proxies</th>
<th>565</th>
<th>The number of proxies scraped from sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing</td>
<td>15</td>
<td>The number of currently being watched</td>
</tr>
<tr>
<td>Completed</td>
<td>15</td>
<td>The number of completed Views</td>
</tr>
<tr>
<td>Progress</td>
<td>14 of 100</td>
<td>Progress Completed</td>
</tr>
</tbody>
</table>

1 action | 2+ actions | Hide map | Enable popups | Zoom

zvelo proprietary and confidential
Traffic Predator

[Image of Traffic Predator software interface]

[43x461] zvelo proprietary and confidential
Magic Traffic Bot

College Degree in 5 Days
30% Commission

Target URL
http://

What would you like to do?
START
PAUSE
STOP
Help?
Free Web Traffic Generator

**Target URL:** [Enter URL here]

**Max Wait Time To Load Page (sec):** [Enter time here]

**Millisecond Pause After Each Page Loaded:** [Enter value here]

**Proxy Server List:**
- 201.39.233.217.0080
- 187.168.105.122.0000
- 203.93.104.20.80
- 186.251.144.58.3129
- 200.103.97.218.80
- 117.178.15.61.8123
- 123.6.244.72.0832
- 117.178.132.238.8123
- 117.178.109.140.8123
- 201.58.174.194.40
- 117.178.126.59.8123
- 91.26.200.162.0000
- 117.178.114.51.8123
- 121.14.5.76.80
- 117.121.234.241.0000
- 109.22.171.44.8000
- 117.178.115.226.0123
- 187.111.97.90.80
- 202.165.105.100.8000
- 21.7.178.171.0808
- 117.178.104.23.0123
- 187.44.165.158.8008
- 117.178.170.0123
- 116.236.216.116.8008
- 201.123.233.0000
- 186.67.116.142.8008
- 117.177.162

**Web Browser**

**Proxy Extract Tools**

**Current Proxy:** [Enter proxy here]

**All Visit Count:** [Enter count here]

**All Loop Count:** [Enter count here]
TRAFFIC Haul

TRAFFIC BOT ADVANCED WITH 60+ HITS IN A SECOND, GUARANTEED!

http://fourerr.com/danish1658
Automated Traffic Bot
Supreme Traffic Bot

The color scheme has been changed to Windows 7 Basic. 

The current color scheme has been automatically changed to improve performance. Click to see more information.
Traffic Generator Characteristics

- Direct URL Visits
- InnerPages URL Visits
- Random Links Visits
- AutoClick Direct Links
- AutoClick Selected Area
- Multithreads
- Custom Screen Resolution
- Delay Between Threads
- Delay in Stay URL
- Delay Between Clicks
- Random Number of Views
- Repeat Every X Hours/Min.

- Delete History & Cookies
- Desktop User Agents
- Mobile User Agents
- Custom Referrers
- VPN Support
- IP Change every "X" min.
- IP Change every "X" Views
- Proxy Support
- SSH Support
- Proxy Scraper & Validator
- FTP Upload Proxies
- Mass Email Proxies
Traffic Exchange 101

My Website

Other Peoples Jingling

Other Peoples Jingling

Other Peoples Jingling

Other Peoples Website

Other Peoples Website

Other Peoples Website

Tokens

Tokens

My Jingling

Tokens
Using Malware for Traffic

- Create hidden browsers
- Generate random mouse movements
- Page Scrolls
- Random Clicks
- Mute volume
User Events and Engagements

Total Time in Page: 108 seconds
Scroll Events: 217

Element Hovered: BODY[0]
X Mouse Location: 574
Y Mouse Location: 991
Time Hover Started: 108 sec
Text: Justin Bieber and Canadian tennis...

Per Element Statistics:

* undefined HTML(1): 1 mouseovers | 0 clicks | 0 sec | 'Total Time In Page: 108...'
* Title of the Blog(2): 6 mouseovers | 0 clicks | 6 sec | 'Justin Bieber Ultimate Fan Blog...'
* BODY[1]: 2 mouseovers | 2 clicks | 43 sec | 'Total Time In Page: 108...'
* BODY[0]: 2 mouseovers | 0 clicks | 9 sec | '
* BODY[1]: 4 mouseovers | 0 clicks | 4 sec | 'Welcome to the fastest, largest...
* BODY[2]: 6 mouseovers | 1 click | 5 sec | 'Justin Bieber closed the 11th...'
* BODY[3]: 6 mouseovers | 2 clicks | 10 sec | 'Justin Bieber and Canadian tennis...'
* BODY[4]: 1 mouseovers | 2 clicks | 4 sec | 'Jugene Bouchard...'
* BODY[5]: 1 mouseovers | 1 click | 2 sec | 'Justin Bieber...

Selected Text: "La Quinta, California" self-professed crush "Will Ferrell"

...est, largest and longest running Justin Bieber fansite. Ever wonder what Justin is up to? Our goal is to provide you with the latest info, pictures and videos of the two times grammy nominated star. Do to get our blog updates on your Tumblr dashboard.

The 11th Annual Desert Smash tennis tournament (hosted by Will Ferrell) with a stunning acoustic set on Tuesday evening. He was one of four musical acts at the concert. British songstress Natasha St. Luce, and a tribute band also performed.

Canadian tennis superstar Eugenie Bouchard are the new power couple of celebrity tennis. Okay, Bouchard and her self-professed crush The Biebs aren't a couple in a dating sense, but the two talents join star power to the 11th annual Desert Smash in La Quinta, California.
Can the NHT traffic actually be coming from a human?

Who for all intents and purposes they do not know they are visiting your site
Traffic is delivered to you through:

- Pop-ups
- Pop-unders
- iFrames
What are the Clues…?

70% of the viewports are 1 pixel!

Meaning the size of the browsers viewing your site looks like this:
What are the Clues...?

The window is not the active window:

Your site is here
So... can I buy internet traffic and get away with it?
If an advertiser will audit the traffic and they know what to look for, you will get caught.

If they don’t you’ll get away with it.

The “quality” of traffic is directly proportional to how much you pay for it.
  - The lower prices, you’ll get bots.
  - They higher prices, you’ll get frames, popups or pop-unders.

Depends.
Thank You!

Cyber Security Threats in Digital Advertising and Ad Fraud 101

Karl Dominguez