



# Social Engineering with Web Analytics

Tyler Rosonke, @zorksec

# whoami

- Omaha, Nebraska based hackerman.
- Information Assurance degree from University of Nebraska at Omaha.
- Helped build and run a red team at large fortune 200 company.
- Now am a Security Consultant at TrustFoundry.
- I run a blog at [zonksec.com](http://zonksec.com).
- Photography, outdoors, vintage 2 stroke mopeds.



# Disclaimers

- This presentation is for informational and educational purposes only.
- Neither I, nor my employers, are responsible for any trouble you may get yourself into.
- Use at your own risk.

# Web Analytics?

- Web Analytics are the measurement, collection, analysis and reporting of web data.
- Used by tons of websites to figure out how their users are getting to their content and what they are doing while there.
- This data is typically interpreted to build better content and products.
- Top platform by far is Google Analytics, although others exist.

# Strange referrals...

- I run google analytics on my blog and I encountered some strange referrals from the following domains:
  - free-traffic.xyz
  - social-buttons-ii.xyz
  - make-money-online.7makemoneyonline.com
  - buttons-for-website.com
  - Etc.
- Clearly some sort of spam/scam.
- It got me wondering....

# How can this be used for evil?

- Being red team / penetration testing focused.
- Get malicious links in front of people for SE.
  - Sorta like phishing with analytics.

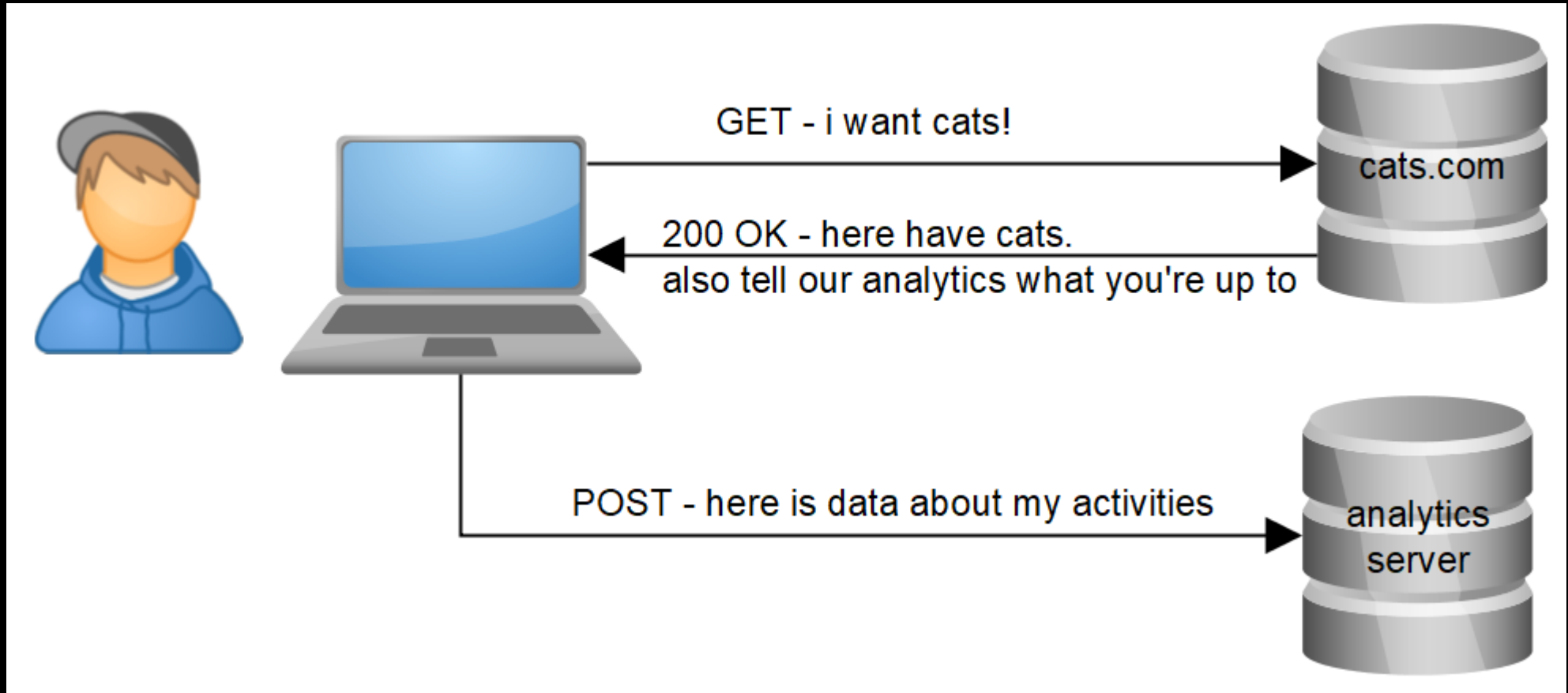


# How can this be used for evil?

1. OSINT on target
2. Buy tempting domain
  - Retail Company => Consumer Review Site
  - University => Top 10 Schools in \$State
  - Blog => Similar Topic blog
3. Add exploit to attacker controlled site
  - HTA attack
  - Credential Harvest (Google Analytics)
  - Known CSRF vuln
  - Browser Exploit
4. Generate referral traffic to target
5. Target visits attacker controlled site
6. Profit!



# How does it work?





# How are they doing that?

- Given this snippet of JS on setup and asked to add to every page:

```
<script>
  (function(i,s,o,g,r,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){
  (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),
  m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
  })(window,document,'script','//www.google-analytics.com/analytics.js','ga');
  ga('create', 'UA-xxxxxxx-x', 'auto');
  ga('send', 'pageview');
</script>
```

# How are they doing that?

- If I can figure out how the JS requests are being made to google-analytics.com, then I can probably just spam it with “referrals”.
  - I can start by reverse engineering the JS
  - I can proxy the browser and try and make sense of the request made by JS

# How are they doing that?



```
this.m[""+a]=b:this.values[""+a]=b};ee.prototype.get=function(a){return this.m.hasOwnProperty(""+a)?
this.m[""+a]:this.values[""+a]};ee.prototype.map=function(a){for(var b=0;b<this.keys.length;b++){var
c=this.keys[b],d=this.get(c);d&&a(c,d)};var O=window,M=document;var F=window,G=function(a){var
b=F._gaUserPrefs;if(b&&b.ioo&&b.ioo()||a&&!0===F["ga-disable-"+a])return!0;try{var
c=F.external;if(c&&c._gaUserPrefs&&"oo"==c._gaUserPrefs)return!0}catch(d){}return!1};var Ca=function(a){var b=
[],c=M.cookie.split(";");a=new RegExp("^\\s*" + a + "\\s*(.*)\\s*$");for(var d=0;d<c.length;d++){var
e=c[d].match(a);e&&b.push(e[1]);return b},zc=function(a,b,c,d,e,g)
{e=G(e)?!1:eb.test(M.location.hostname)||"/"==c&&vc.test(d)?!1:!0;if(!e)return!1;b&&1200<b.length&&
```

# How are they doing that?

or...

- Google will have amazing documentation:
  - <https://developers.google.com/analytics/devguides/collection/protocol/v1/reference>
  - <https://developers.google.com/analytics/devguides/collection/protocol/v1/parameters>

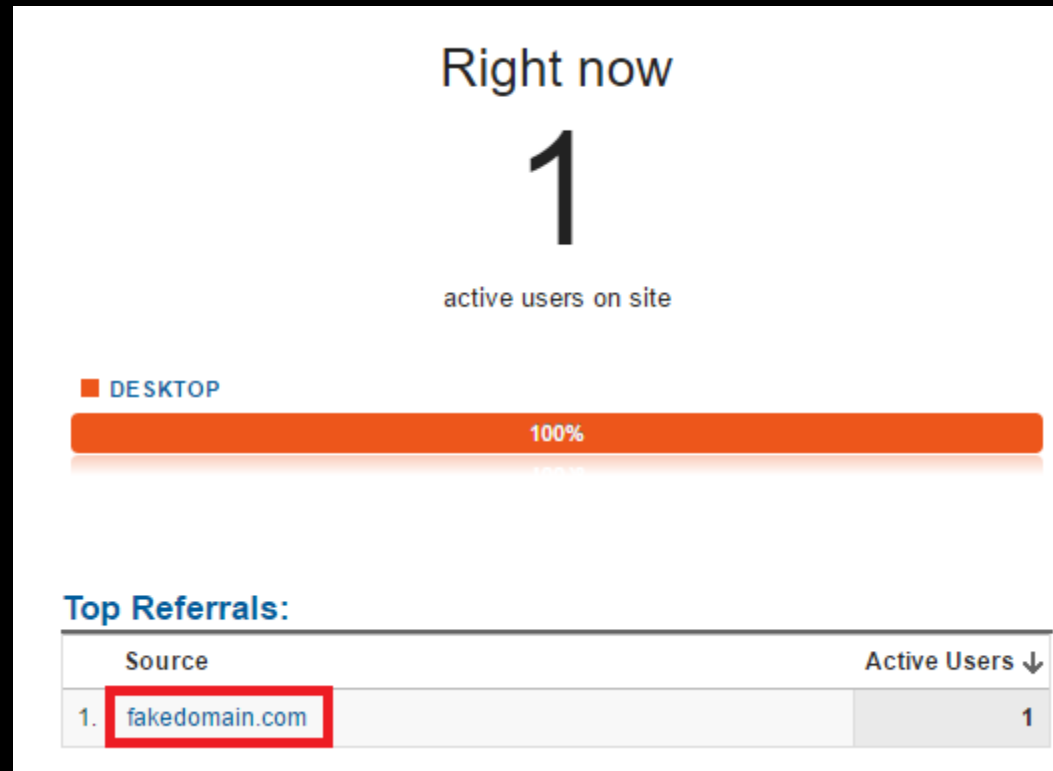
# How are they doing that?

- Required URL params

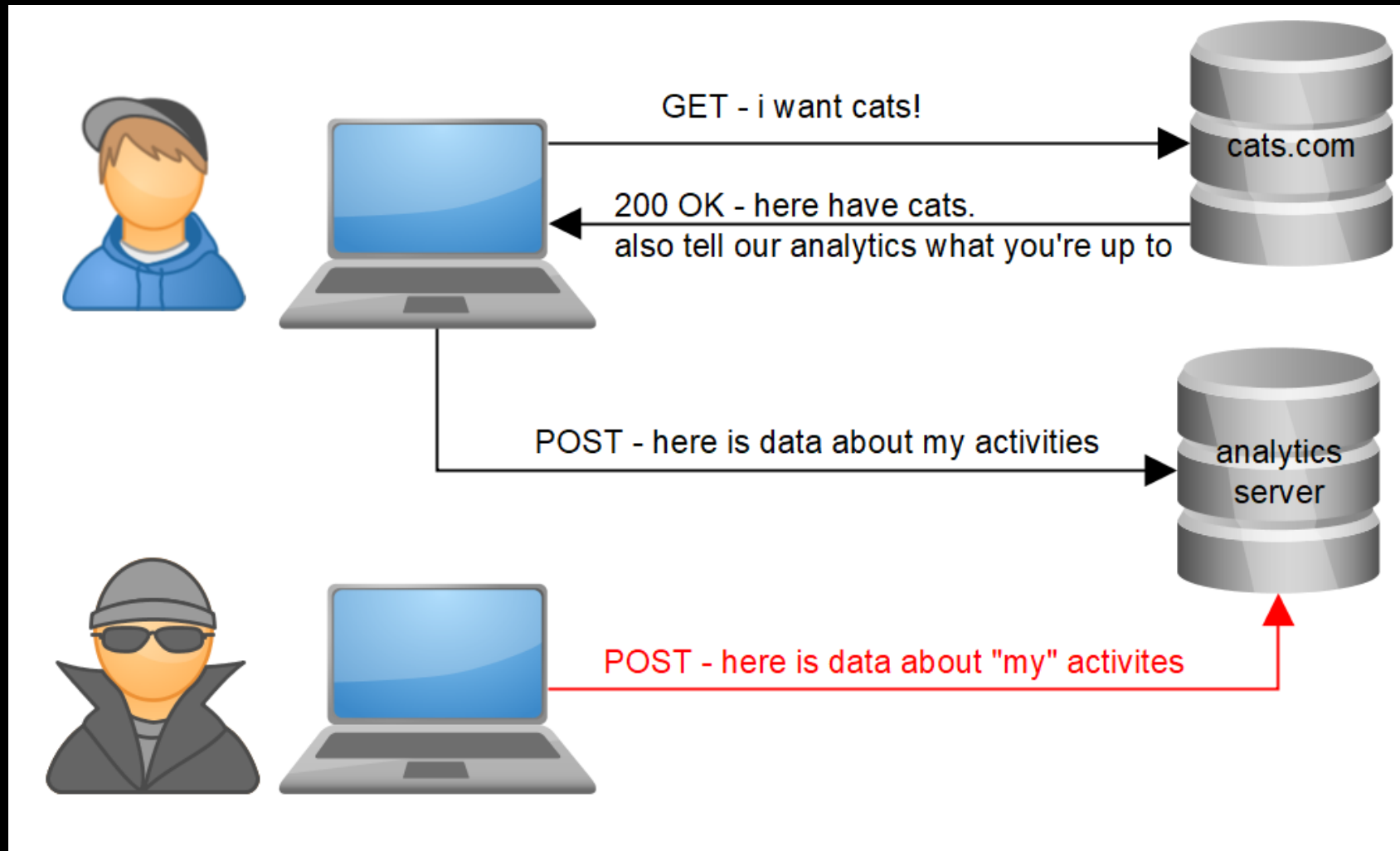
Name	Parameter	Example	Description
Protocol Version	v	v=1	The protocol version. The value should be 1.
Tracking ID	tid	tid=UA-123456-1	The ID that distinguishes to which Google Analytics property to send data.
Client ID	cid	cid=xxxxx	An ID unique to a particular user.
Hit Type	t	t=pageview	The type of interaction collected for a particular user.
Document Path	dp	dp=/aboutme	The path portion of the page URL. Should begin with '/
Document Host Name	dh	dh=http://xyz.com	Specifies the hostname from which content was hosted.
Document Title	dt	dt=About	The title of the page / document.
Document Referrer	dr	dr=http://fakedomain.com/	Specifies which referral source brought traffic to a website.
Anonymize IP	aip	aip=1	When present, the IP address of the sender will be anonymized.



# Success!



# Success!





# Automation

```
Welcome to the Social-Engineer Toolkit (SET).  
The one stop shop for all of your SE needs.
```

```
Join us on irc.freenode.net in channel #setoolkit
```

```
The Social-Engineer Toolkit is a product of TrustedSec.
```

```
Visit: https://www.trustedsec.com
```

```
It's easy to update using the PenTesters Framework! (PTF)  
Visit https://github.com/trustedsec/ptf to update all your tools!
```

```
There is a new version of SET available.
```

```
Your version: 7.4.3
```

```
Current version: 7.7
```

```
Please update SET to the latest before submitting any git issues.
```

```
Select from the menu:
```

- 1) Social-Engineering Attacks
- 2) Penetration Testing (Fast-Track)
- 3) Third Party Modules
- 4) Update the Social-Engineer Toolkit
- 5) Update SET configuration
- 6) Help, Credits, and About

```
99) Exit the Social-Engineer Toolkit
```

```
set> 3
```

```
[-] Social-Engineer Toolkit Third Party Modules menu.
```

```
[-] Please read the readme/modules.txt for information on how to create your own modules.
```

```
3. Google Analytics Attack by @ZonkSec
```

```
99. Return to the previous menu
```

```
set:modules>3
```

```
Loading module. Please wait...
```

```
-----  
Google Analytics Attack  
By Tyler Rosonke (@ZonkSec)  
-----
```

```
User-Guide: http://www.zonksec.com/blog/social-engineering-google-analytics/
```



# Automation

Google Analytics Attack  
By Tyler Rosonke (@ZonkSec)

User-Guide: <http://www.zonksec.com/blog/social-engineering-google-analytics/>

References:

-<https://developers.google.com/analytics/devguides/collection/protocol/v1/reference>  
-<https://developers.google.com/analytics/devguides/collection/protocol/v1/parameters>

[\*] Choose mode (automatic/manual): auto

[\*] Entering automatic mode.

[\*] Target website (E.g. 'http://xyz.com/'): <https://zonksec.com/>

[\*] Enter referral URL to spoof (E.g. 'http://xyz.com/'): <http://fakedomain.com/>

[+] Payload ready.

[\*] Print payload?(y/n): y

dh = <https://zonksec.com>

cid = 555

aip = 1

t = pageview

v = 1

tid = UA-72589501-1

dt = ZonkSec - security never sleeps

dr = <http://fakedomain.com/>

dp = /

Press <enter> to send payload.

[+] Payload sent.

<https://www.google-analytics.com/collect?dh=https%3A%2F%2Fzonksec.com&cid=309&aip=1&t=pageview&v=1&tid=>

[\*] Send payload on loop?(y/n) y

[\*] Seconds between payload sends: 5

Sending request every 5 seconds. Use CTRL+C to terminate. Press <enter> to begin loop.

[+] Payload sent.


<https://www.google-analytics.com/collect?dh=https%3A%2F%2Fzonksec.com&cid=723&aip=1&t=pageview&v=1&tid=>

[+] Payload sent.

<https://www.google-analytics.com/collect?dh=https%3A%2F%2Fzonksec.com&cid=122&aip=1&t=pageview&v=1&tid=>


[+] Payload sent.

<https://www.google-analytics.com/collect?dh=https%3A%2F%2Fzonksec.com&cid=593&aip=1&t=pageview&v=1&tid=>

Browser window: Tyler | ZonkSec - Social Engine | www.zonksec.com/blog/social- |  BLOG ABOUT


## Social Engineering with Google Analytics


September 25, 2016



Top Referrals:	
Source	Active Users ↓
1. lookmomfakedomainreferral.com	79

A few weeks back I logged into my [Google Analytics](#) account and noticed some strange hits from domains such as 'free-traffic xvz' 'social-buttons-ii xvz' and 'eu-

Browser window: Tyler | This Russian Is Spammin... | motherboard.vice.com/read/th |  THE VICE CHANNELS EN



## This Russian Is Spamming Google Analytics to Show His Support for Trump

Written by **JOSEPH COX**

December 2, 2016 // 10:00 AM EST

#validated



...also there is more here.

# What else could happen?

- I need to understand how analytics is used.
- I need to talk to people who use analytics in the field.

After a handful of discussions, this is what I came up with...

...but first. A common theme.

- Humans love validation and reinforcement.
- Analytics traffic == validation and reinforcement of a particular page.

# therefore...

- Assuming we can control various aspects of analytics.
- Any decisions made using those analytics could be manipulated.
- Any sort of measurements where those analytics are the measuring stick, could be manipulated.

# Scenario 1 - Content Control

- Content creators may use analytics to decide to keep making content.
- To control, simply reinforce specific content.
- Could be used to reinforce specific political or social ideals.
  
- Also the reverse...
- Nefarious or antithetical referrals could discourage content.

# Scenario 2 - Ecommerce Control

- Ecommerce sites may use analytics to decide:
  - What new products to develop
  - What items should go on sale
  
- Reinforce particular products or types of products to control



## Scenario 3 - WebDev Espionage

- WebDev companies use analytics to monitor website usage, and in some cases share data with customers.
- A competitor could destroy the integrity of the data by bombarding with traffic.
- Client is disgruntled by losing insight, maybe switch WebDev.
- WebDev company can no longer use analytics gloat to persuade new clients.

# Scenario 4 - Nation State Espionage

- Assumption:
  - Nation state can subpoena analytics data of any site
  - Nation state is using said analytics data to identify suspicious web sites and operators
- Analytics can be used to frame innocent sites and operators
- Analytics data could be manipulated to cloak the real bad guys



# Scenario 5 - SEO & Traffic Scam

- SEO is not affected by analytics... but people don't always understand.
- Analytics traffic != real traffic
- Many scams are possible with right clientele:
  - “Pay me and I will use SEO black magic to get you 15% increase in analytics or money back.”
  - “Your sales are weak on the east coast. Pay me and I can get you more east coast visitors.”
  - “Buy cheap traffic here!”

Overview Compare Packages Description Reviews

Favorite

77

## I Will Get You 25,000 Unlimited Google Traffic

★★★★★ (137)

Digital Marketing / Web Traffic

**I Will Send 25K**  
Real Web Traffic

100% MONEY BACK GUARANTEE | 100% SATISFACTION GUARANTEE

**24 Hours Express Delivery**

**25,000K ++ Exclusive on fiverr®**



### Compare Packages

	\$5	\$10	\$20
	Basic	Standard	Premium

\$5 Basic



\$10 Standard

🕒 1 Day Delivery

50000 High Quality Real Traffic

I will Drive 10000 Daily visitors for 5 days. "10000 x 5 = 50000 Visit"

✓ 40000 Visitors

Proceed to Order (\$10)

Compare Packages

\$20 Premium



Keep08traffic

Level 2 Seller

From Sri Lanka

Speaks English

Positive Rating 99%

Avg. Response Time 1 Day

## Scenario 6 - Bad guy use it too!

- Domain-ers, ad fraud networks, malware networks, and etc have been identified to use analytics.
- Helps them decide which schemes are best. Also helps defenders in attribution. 😊
- Defenders could potentially disrupt operations by manipulating analytics data or bombarding and ruining integrity.



# Failures for automation 1.0

- Failed at user emulation
  - Incredibly high bounce rate
  - “users” visited one page and disappeared
  - All users came from same geographic location
- Failed at OPSEC
  - Makes request to Google Analytics and target site from attacker IP
- Failed at other perspectives
  - Only accounted for Pentest perspective
  - Could only do referrals.



What is good user emulation?





Landing Page

→ /blog/social-en...ogle-analytics/  
11

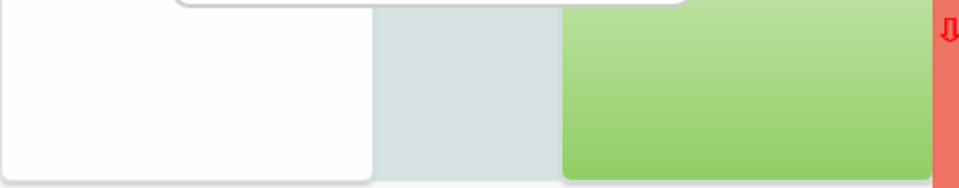
/blog/social-en...ogle-analytics/  
(1 page)

0 Through traffic (0.00%)  
11 Drop-offs (100%)

11 Sessions

es  
, 27 drop-offs

1st Interaction  
1 sessions, 1 drop-offs



→ /blog/persi...or-script/  
7

blog/persis...or-script/  
7

→ /blog/hands...erability/  
5

blog/hands-...erability/  
5

→ /blog/magic...filtering/  
4

blog/magic-...filtering/  
4

→ /  
1

1

1  
/blog/build...s-journey/



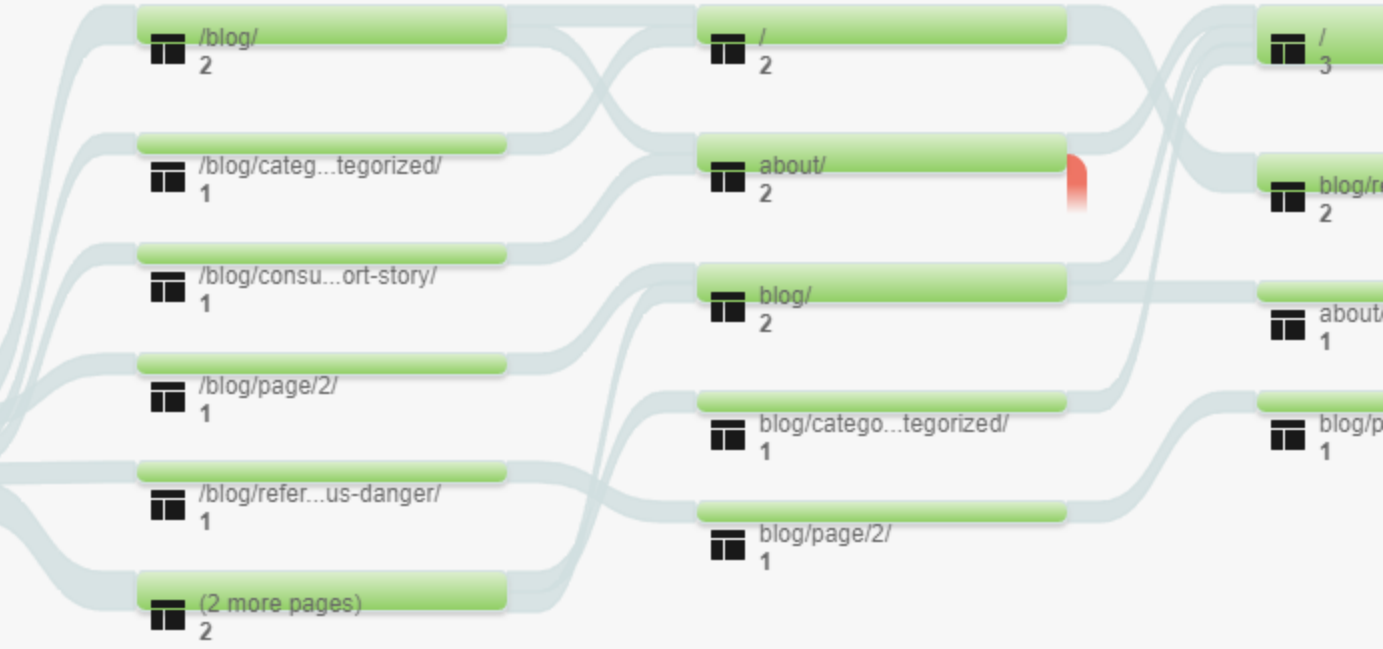
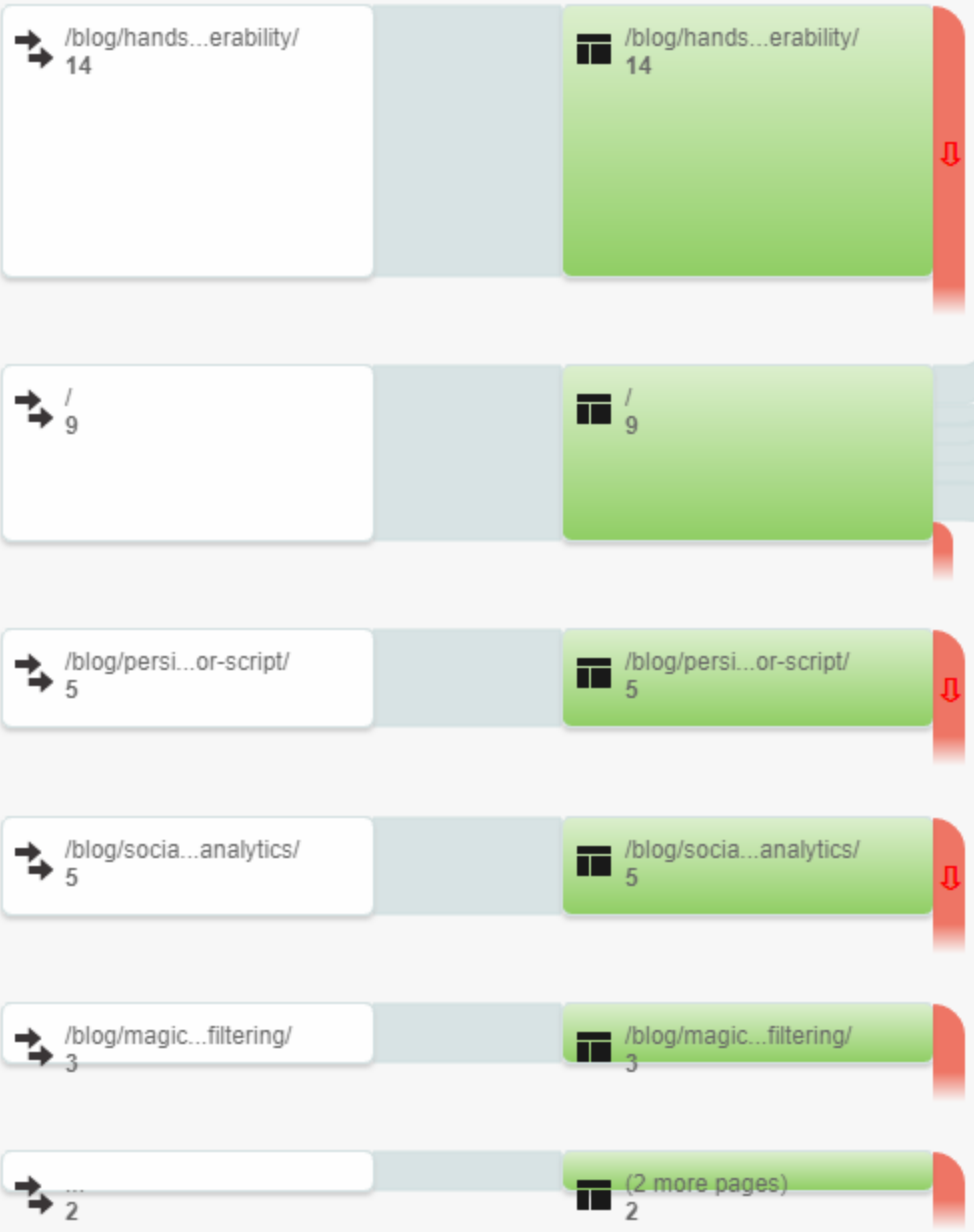
Landing Page

Starting pages  
38 sessions, 30 drop-offs

1st Interaction   
8 sessions, 0 drop-offs

2nd Interaction   
8 sessions, 1 drop-offs

3rd Interaction  
7 sessions,



Source ?	Acquisition			Behavior		
	Sessions ? ↓	% New Sessions ?	New Users ?	Bounce Rate ?	Pages / Session ?	Avg. Session Duration ?
	<b>2,780</b> % of Total: 40.37% (6,887)	<b>92.84%</b> Avg for View: 94.09% (-1.33%)	<b>2,581</b> % of Total: 39.83% (6,480)	<b>64.82%</b> Avg for View: 83.61% (-22.47%)	<b>1.90</b> Avg for View: 1.41 (34.91%)	<b>00:00:12</b> Avg for View: 00:00:12 (0.75%)
1. <a href="#">fakesite.com</a>	<b>884</b> (31.80%)	94.00%	831 (32.20%)	80.32%	1.32	<00:00:01
2. <a href="#">lol.com</a>	<b>807</b> (29.03%)	95.04%	767 (29.72%)	56.75%	1.72	<00:00:01
3. <a href="#">not.com</a>	<b>325</b> (11.69%)	96.31%	313 (12.13%)	58.46%	1.65	00:00:00
4. <a href="#">github.com</a>	<b>181</b> (6.51%)	83.98%	152 (5.89%)	86.74%	1.30	00:01:05
5. <a href="#">lolololol.com</a>	<b>77</b> (2.77%)	93.51%	72 (2.79%)	100.00%	1.00	00:00:00
6. <a href="#">badboy.com</a>	<b>75</b> (2.70%)	97.33%	73 (2.83%)	54.67%	2.24	00:00:01
7. <a href="#">test.com</a>	<b>67</b> (2.41%)	85.07%	57 (2.21%)	31.34%	3.72	00:00:12
8. <a href="#">fake.com</a>	<b>53</b> (1.91%)	98.11%	52 (2.01%)	9.43%	5.34	00:00:04
9. <a href="#">gethackedhere.com</a>	<b>53</b> (1.91%)	94.34%	50 (1.94%)	9.43%	3.79	00:00:47
10. <a href="#">hackerman.com</a>	<b>51</b> (1.83%)	98.04%	50 (1.94%)	15.69%	3.33	00:00:10

# Analytics Attack NG

- User Emulation
- Threading
- Geographical spoofing
- Auto URLs
- Proxy support (HTTP and SOCKS5 )
  - yay TOR!

# User Emulation

Session

URLs

Bounces

Referral

Target

Bounce

# of

Duration

# Auto URLs

- Automatically grabs URLs from Google if needed.
  - Referrals based on keywords.
    - “good hacker blogs” => zonksec.com
  - Additional target URLs based on “site:\$site” results
  - Additional bounce URLs based on “site:\$site” results

Demo



Demo gods have failed me..





```
INFO:root:[*] Starting 2 threads.  
INFO:root:[*] Waiting for threads.  
INFO:root:[+] T1: Session complete. CID: 54494. GEO_ID: 1018199 Behavior: https://defconiscanceled.com => [T] https://z  
nksec.com (5 sec delay) => https://www.zonksec.com/wp-content/uploads/2016/03/ContradictionC2_Final_Paper.pdf (50 sec de  
lay) => https://zonksec.com/blog/keepass-eating-dog-food/  
INFO:root:[*] T1: Sleeping for 0  
INFO:root:[+] T1: Session complete. CID: 10755. GEO_ID: 1020703 Behavior: https://defconiscanceled.com => [T] https://z  
nksec.com (2 sec delay) => https://zonksec.com/blog/dakotacon-talks-training-ctf-writeups/ (11 sec delay) => https://zon  
ksec.com/blog/page/2/  
INFO:root:[*] T1: Sleeping for 0  
INFO:root:[+] T0: Session complete. CID: 77360. GEO_ID: 1014950 Behavior: https://defconiscanceled.com => [T] https://z  
nksec.com (40 sec delay) => https://zonksec.com/blog/page/2/ (31 sec delay) => https://zonksec.com/blog/page/2/  
INFO:root:[*] T0: Sleeping for 0
```

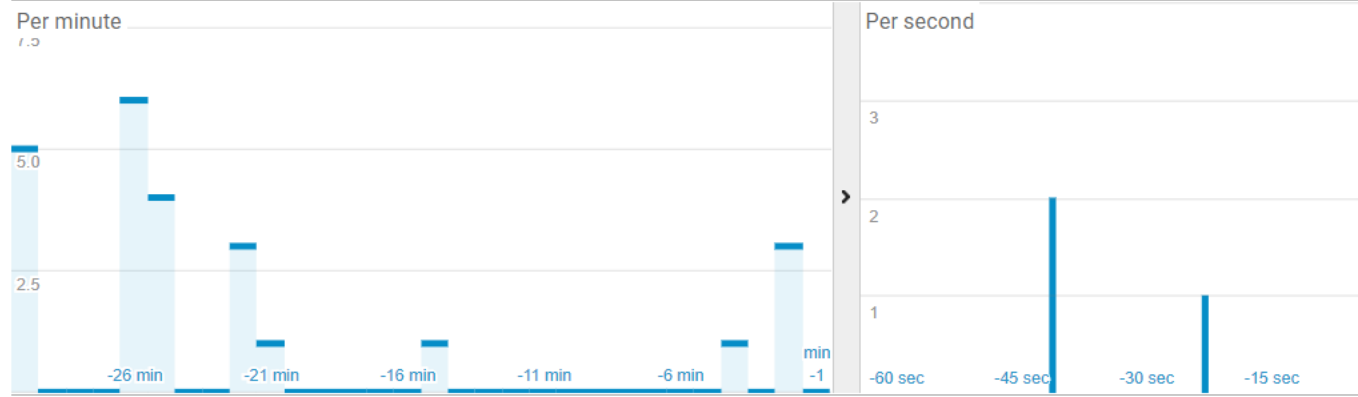
### Right now

# 3

active users on site



### Pageviews



### Top Referrals:

Source	Active Users ↓
1. defconiscanceled.com	2

### Top Social Traffic:

Source	Active Users ↓
There is no data for this view.	

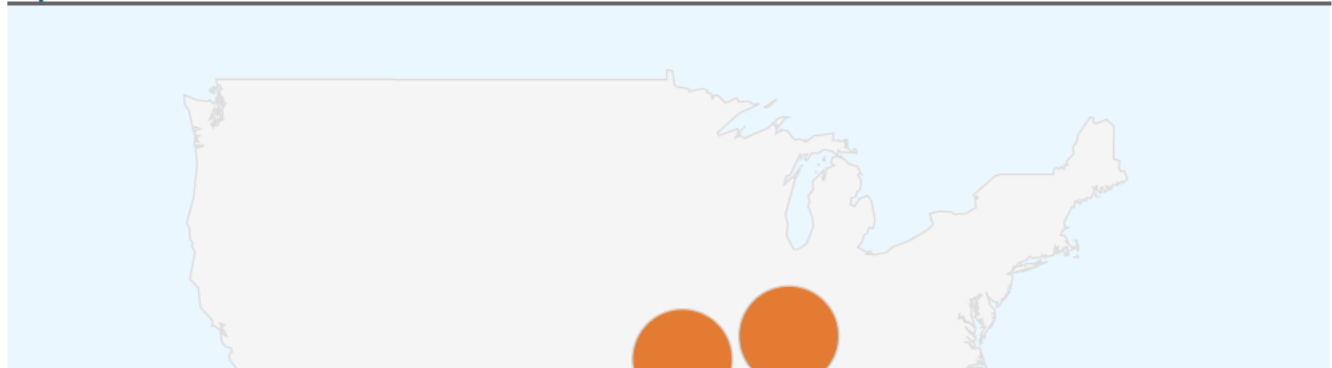
### Top Keywords:

Keyword	Active Users ↓
1. (not provided)	1

### Top Active Pages:

Active Page	Active Users ↓
1. /	1 33.33%
2. /blog/dakotacon-2017-ctf-write-ups/	1 33.33%
3. /blog/magic-mirror-dns-filtering/	1 33.33%

### Top Locations:





```
INFO:root:[*] Starting 1 threads.
INFO:root:[*] Waiting for threads.
INFO:root:[+] T0: Session complete. CID: 53980. GEO_ID: 1020829 Behavior: https://www.quora.com/Which-blogs-websites-are
-best-for-latest-hacking-tutorials-and-current-scenarios-of-hacking-world => [T] https://zonksec.com/blog/referer-redire
ction-inconspicuous-danger/
INFO:root:[*] T0: Sleeping for 0
INFO:root:[+] T0: Session complete. CID: 69803. GEO_ID: 1020829 Behavior: http://zack.onisko.com/50-growth-hacker-blogs-
to-follow/ => [T] https://zonksec.com/blog/referer-redirectation-inconspicuous-danger/
INFO:root:[*] T0: Sleeping for 0
INFO:root:[+] T0: Session complete. CID: 98092. GEO_ID: 1020829 Behavior: https://blog.hubspot.com/marketing/best-growth
-hacker-blogs-experts => [T] https://zonksec.com/blog/consumed-defcon-short-story/
INFO:root:[*] T0: Sleeping for 0
INFO:root:[+] T0: Session complete. CID: 49262. GEO_ID: 1020829 Behavior: http://zack.onisko.com/50-growth-hacker-blogs-
to-follow/ => [T] https://zonksec.com/blog/dakotacon-2017-ctf-write-ups/
INFO:root:[*] T0: Sleeping for 0
INFO:root:[+] T0: Session complete. CID: 82206. GEO_ID: 1020829 Behavior: https://www.optimonk.com/blog/22-best-growth-h
acker-sites-videos-ebooks-tools-growth-hacking/ => [T] https://zonksec.com/blog/consumed-defcon-short-story/
INFO:root:[*] T0: Sleeping for 0
INFO:root:[+] T0: Session complete. CID: 60545. GEO_ID: 1020829 Behavior: https://www.hackerone.com/blog/hacker-blogs-we
-love-reading => [T] https://zonksec.com/blog/dakotacon-2017-ctf-write-ups/
INFO:root:[*] T0: Sleeping for 0
INFO:root:[+] T0: Session complete. CID: 44388. GEO_ID: 1020829 Behavior: https://growthrocks.com/blog/ => [T] https://z
onksec.com/blog/referer-redirectation-inconspicuous-danger/
INFO:root:[*] T0: Sleeping for 0
INFO:root:[+] T0: Session complete. CID: 93732. GEO_ID: 1020829 Behavior: https://digitalguardian.com/blog/top-50-infose
c-blogs-you-should-be-reading => [T] https://zonksec.com/blog/dakotacon-talks-training-ctf-writeups/
INFO:root:[*] T0: Sleeping for 0
INFO:root:[+] T0: Session complete. CID: 64321. GEO_ID: 1020829 Behavior: http://hackaday.com/ => [T] https://zonksec.co
m/blog/building-iot-hackers-journey/
INFO:root:[*] T0: Sleeping for 0
INFO:root:[+] T0: Session complete. CID: 59760. GEO_ID: 1020829 Behavior: https://www.optimonk.com/blog/22-best-growth-h
acker-sites-videos-ebooks-tools-growth-hacking/ => [T] https://zonksec.com/blog/building-iot-hackers-journey/
INFO:root:[*] T0: Sleeping for 0
```



ZonkSec  
All Web Site Data

Search reports and help

HOME

CUSTOMIZATION

Reports

- REAL-TIME
- Overview
- Locations
- Traffic Sources
- Content
- Events
- Conversions

AUDIENCE

ACQUISITION

BEHAVIOR

DISCOVER

ADMIN

2.	<a href="#">optimonk.com</a>	2
3.	<a href="#">zack.onisko.com</a>	2
4.	<a href="#">blog.hubspot.com</a>	1
5.	<a href="#">digitalguardian.com</a>	1

### Top Social Traffic:

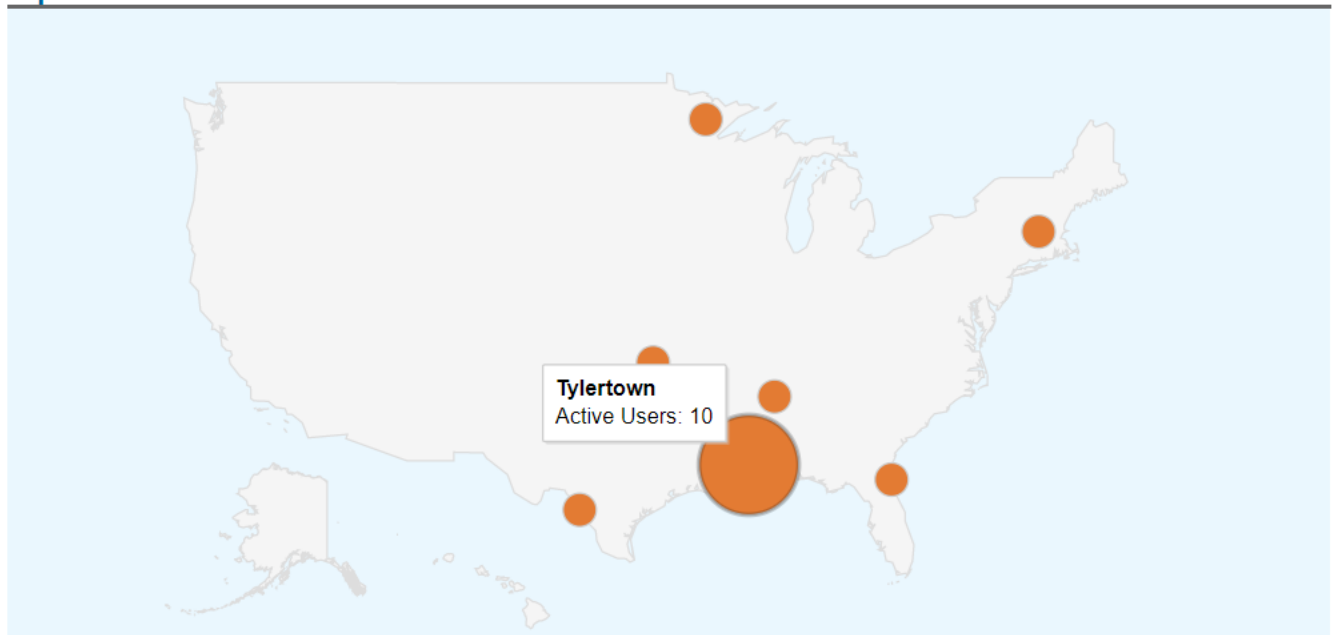
	Source	Active Users ↓
1.	<a href="#">Quora</a>	1

### Top Keywords:

	Keyword	Active Users ↓
There is no data for this view.		

2.	/	2	11.11%
3.	<a href="#">/blog/building-iot-hackers-journey/</a>	2	11.11%
4.	<a href="#">/blog/consumed-defcon-short-story/</a>	2	11.11%
5.	<a href="#">/blog/dakotacon-2017-ctf-write-ups/</a>	2	11.11%
6.	<a href="#">/blog/page/2/</a>	2	11.11%
7.	<a href="#">/blog/category/uncategorized/</a>	1	5.56%
8.	<a href="#">/blog/dakotacon-talks-training-ctf-writeups/</a>	1	5.56%
9.	<a href="#">/blog/keepass-eating-dog-food/</a>	1	5.56%
10.	<a href="#">/blog/persistence-aggressor-script/</a>	1	5.56%

### Top Locations:



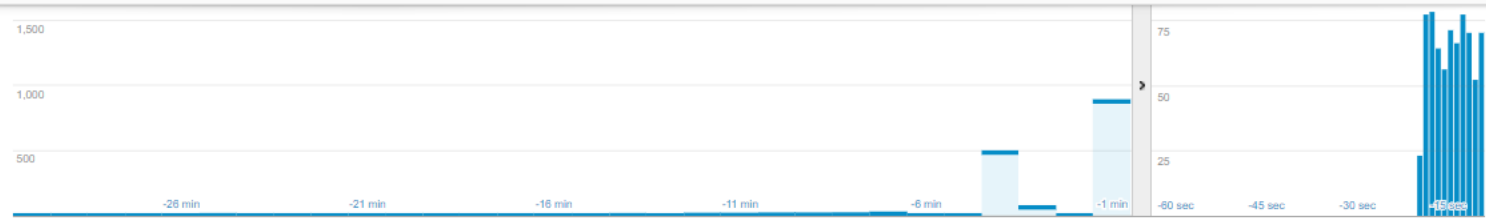


```
INFO:root:[+] T0: Session complete. CID: 18790. GEO_ID: 1012006 Behavior: => [T] https://zonksec.com/blog/dakotacon-2017-ctf-write-ups/
INFO:root:[*] T0: Sleeping for 0
INFO:root:[+] T1: Session complete. CID: 75404. GEO_ID: 1011878 Behavior: => [T] https://zonksec.com/blog/magic-mirror-dns-filtering/
INFO:root:[*] T1: Sleeping for 0
INFO:root:[+] T12: Session complete. CID: 95709. GEO_ID: 1012037 Behavior: => [T] https://zonksec.com/blog/building-iot-hackers-journey/
INFO:root:[+] T8: Session complete. CID: 89908. GEO_ID: 1012021 Behavior: => [T] https://zonksec.com/blog/building-iot-hackers-journey/
INFO:root:[+] T9: Session complete. CID: 23440. GEO_ID: 1011967 Behavior: => [T] https://zonksec.com/blog/indeed-com-recon-ng-module/
INFO:root:[+] T2: Session complete. CID: 49863. GEO_ID: 1011894 Behavior: => [T] https://zonksec.com/blog/social-engineering-google-analytics/
INFO:root:[+] T10: Session complete. CID: 18818. GEO_ID: 1012013 Behavior: => [T] https://zonksec.com/blog/persistence-aggressor-script/
INFO:root:[+] T4: Session complete. CID: 31145. GEO_ID: 1011885 Behavior: => [T] https://zonksec.com/blog/persistence-aggressor-script/
INFO:root:[+] T3: Session complete. CID: 22329. GEO_ID: 1011986 Behavior: => [T] https://zonksec.com/blog/consumed-defcon-short-story/
INFO:root:[+] T11: Session complete. CID: 54904. GEO_ID: 1011855 Behavior: => [T] https://zonksec.com/blog/referer-redirection-inconspicuous-danger/
INFO:root:[+] T6: Session complete. CID: 43542. GEO_ID: 1012033 Behavior: => [T] https://www.zonksec.com/wp-content/uploads/2016/03/ContradictionC2\_Final\_Paper.pdf
```



# 825

active users on site



### Top Referrals:

Source	Active Users
There is no data for this view.	

### Top Social Traffic:

Source	Active Users
There is no data for this view.	

### Top Keywords:

Keyword	Active Users
There is no data for this view.	

### Top Active Pages:

Active Page	Active Users	
1. /blog/building-iot-hackers-journey/	60	7.27%
2. /blog/dakotacon-2017-ctf-write-ups/	56	6.79%
3. /	50	6.06%
4. /blog/keepass-eating-dog-food/	49	5.94%
5. /blog/social-engineering-google-analytics/	49	5.94%
6. /about/	48	5.82%
7. /blog/contradiction2-a-t...tnet-based-on-dead-drops/	48	5.82%
8. /blog/indeed-com-recon-ng-module/	47	5.70%
9. /blog/page/2/	47	5.70%
10. /blog/category/uncategorized/	45	5.45%

### Top Locations:



# Possible Improvements

- CSV configs
- Social media referrals
- Random User Agent

# Bonus Content

- Denial of Service
  - Sometimes analytics portals can not handle all the data incoming = DOS.
- Covert channel
  - Using analytics for C2 (command&control) for botnets could be interest.

# Mitigation Ideas

- User Awareness
- Protect trackingID
  - Script parses server logs in real time and POSTs to analytics
- Export analytics data and corroborate with server logs

# Conclusion

- Analytics != Real Traffic
- Be careful when clicking links in google analytics
- Any decisions made using analytics could be potentially manipulated.
- Any sort of measurements where analytics are the measuring stick, could be potentially manipulated.

# Questions?

Thanks!

- Twitter: @zonksec
- Blog: zonksec.com
  
- Script will be on GitHub momentarily.
- Slides and user-guide will be in future blog post.