

Social Media Mining for Threat Intelligence

Vladimir Kropotov, Dr. Fyodor Yarochkin,
Natasha(Sasha) Hellberg

FTR Team

About us



Agenda

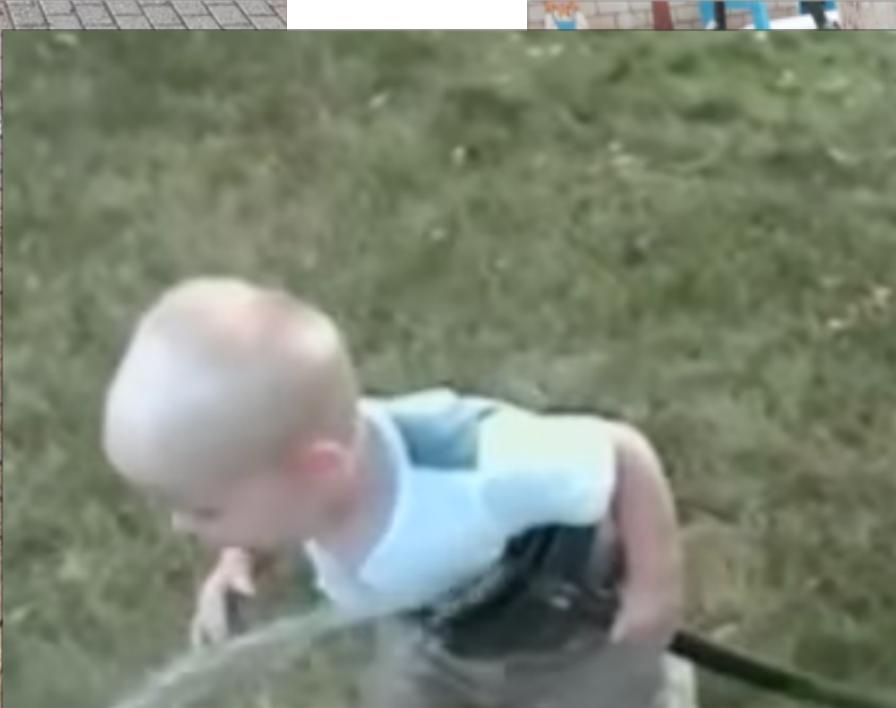
- The project background
- Methodology
- Social Media and Blue Teams
- Social Media and Red Teams
- Findings and Case Studies
- Conclusion

Project Background

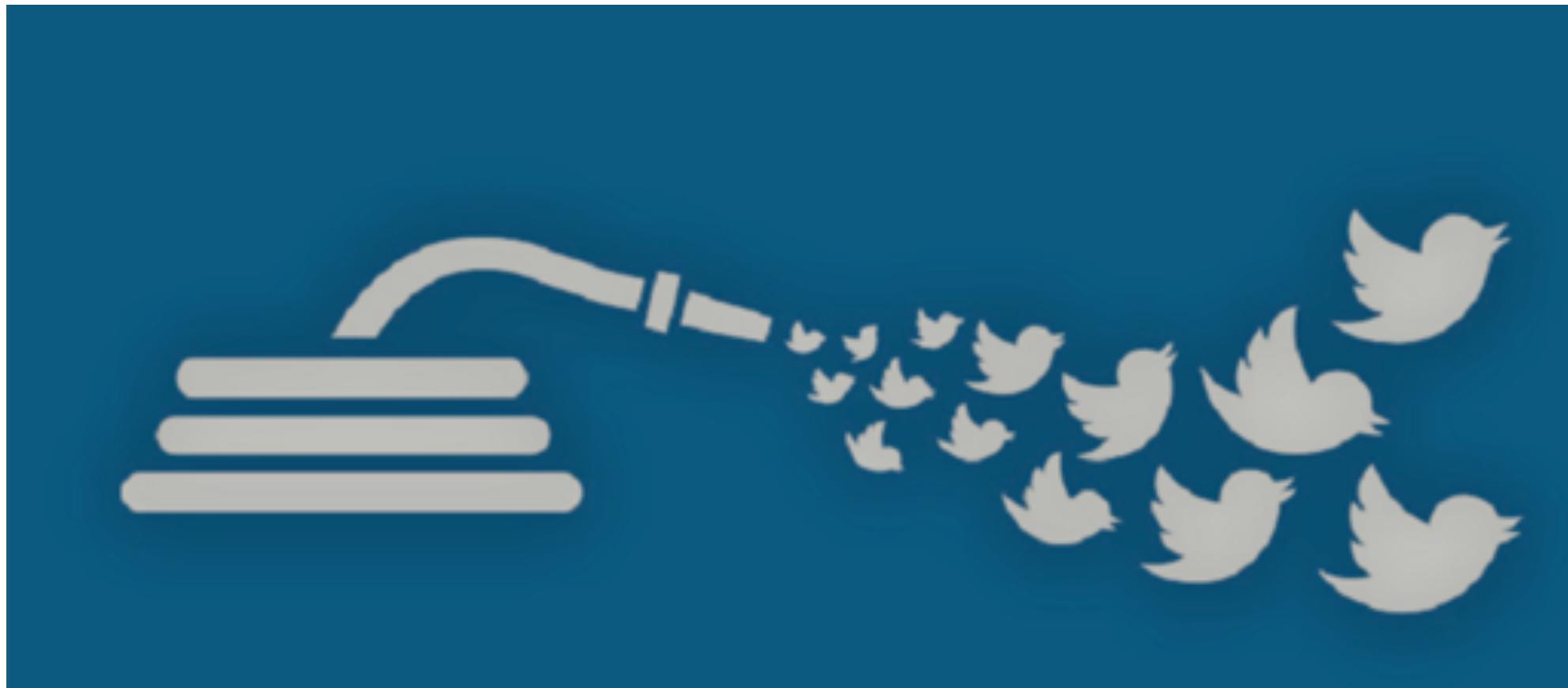
- *The objective - find “interesting” stuff on “social media” that can be used by blue and red teams*
- Not novel
- Objectives:
 - identify mal-actor and mal-group activities (hacking and digital extortion)
 - Identify indicators of interest
 - Identify other possible anomalous use of social media

Twitter Inc.
Social network company





Twitter Firehose: Public. Everyone can play with it



Usability of Social Media Hunting for Blue Teams

Threat Intelligence and Social Media

- Predictability of Future events
- Situational Awareness and real time monitoring
- Restrospection and looking into past

Why hunting Twintel?



Nicolas Krassas
@Dinosn

PoC for persisting .NET payloads to Windows Notification Facility names using low-level Windows API calls.



ustayready/CasperStager
PoC for persisting .NET payloads (WNF) state names using low-level Windows API calls.
[github.com](https://github.com/ustayready/CasperStager)

1:15 PM - 28 Oct 2018



Joël Perras
@jperras

A firewall exploited to install a docker container that spawns a BTC miner to steal CPU. What a time to be alive.



Platzii

[dockmylife/memorytest] Report malicious image · Issue #1...
Hi all I would like to report this malicious image:
<https://hub.docker.com/r/dockmylife/memorytest/> It contains a miner for Monero. This got deployed on one of our servers which...
github.com

10:11 PM - 7 Aug 2017

12 Retweets 15 Likes



Right keywords is gold mine

1 Security Doggo and 2 others Retweeted

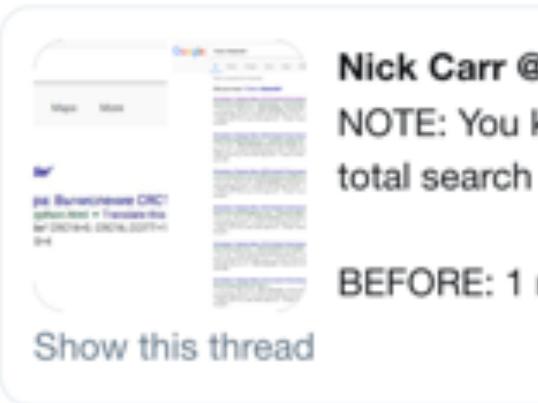
Nick Carr @ ATT&CKcon @ItsReallyNick · 18h

Replying to @ItsReallyNick @Drur

So the lesson is something like – significant ICS attack frameworks

DON'T:

- re-use your old code
- misspell your own name in that yara rule)
- put your picture on the team we #TRITON



Nick Carr @ ATT&CKcon
@ItsReallyNick

Following

Looks like someone uploaded the actual crc.pyc from the #TRITON attack

Uploaded: 58 minutes ago

MD5:

4e5797312ed52d9eb80ec19848cad95

@yararules from this blog fired on it: fireeye.com/blog/threat-re ... #DFIR

Musings on the CRC function and who



Hacker



Hacker



Hacker

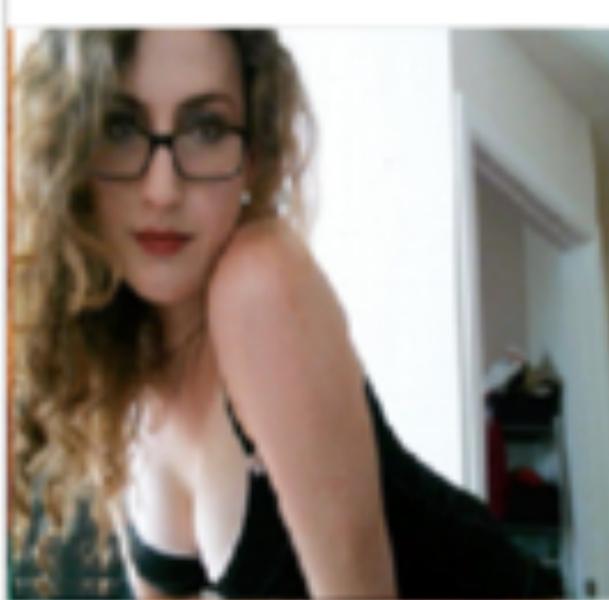


Hacker

Usability of Social Media Hunting for Red teams

Linked in fake profiles

15 ways to detect a fake LinkedIn profile



Elizabeth Obrien

Marketing at Best Builder Websites

Scottsdale, Arizona | Internet

Current Best Builder Websites

Education San Jose State University

2nd

Accept invitation

Send InMail

50
connections

www.linkedin.com/in/elizabethcobrien/

BACKGROUND

Known use by “red teams”

פרופילים מזויפים בפוייסבוק, בעיקר של נשים נאות, פיתו חיילים להוריד תוכנה שאפשרה לארנון הטרור לאסוף מידע • הערכות בצה"ל: פוטנציאלי הנזק הוא אדיר • הצבא י חמיר את ההנחיות לשימוש של חיילים ברשות החברתיות • כך עבדה השיטה

לייר שובל //

poraom ב: 03:22 01.01.2018 | עדכן ב: 15:57 11.01.2017



Karen Cohen



Daniela Kovaliu



Jeme Aidan



Amit Cohen



Aitai Yosef



Naama Sheva



Loren Alian



Nir Leitner



Verena Sonner



Dan Natal



אלビינה נתן



אליאחנן אפר



חחח למה את מתכוונת? מה זה
מעניין

שנייה אני אשלח לך תמונה נשמה

ଓק"חח



??

סבבי

שלחי תמונה בנתים חח להתקrror

[http://www.apkpkg.com/
android/?product=yeecallpro](http://www.apkpkg.com/android/?product=yeecallpro)



YC Pro |

apkpkg.com



מ // צילום: דובר צה"ל

So what you can do on social media putting a blue hat

- Hunting for IoCs
 - Hashes
 - IP addresses
 - CVEs
- Tracing Information Leaks through Social Media
- Investigating malware using Social Media
- Investigate Script-kiddie actors using Social Media



Malware on Social Media



What is this ..? Retrohunt!

The file being studied is Android related! DEX Android file m

Tl Interesting strings

```
http://  
http://en.utrace.de  
http://ktosdelaetskrintotpidor.com  
http://sositehuypidarasi.com  
https://  
https://support.google.com/calendar/answer/6261  
https://twitter.com/96vqZcsxmL7sv73  
https://yb84h8hu8i8uj8u4554.com
```

Microsoft	-
MicroWorld-eScan	-
NANO-Antivirus	Trojan.Android.BankBot.fjpsxy
Panda	-
Qihoo-360	-
Rising	-
Sophos	Andr/Banker-GTN
SUPERAntiSpyware	-
Symantec	Trojan.Gen.2
SymantecMobileInsight	AppRisk:Generisk
TACHYON	-
Tencent	-

Identification

Details

Content

Attachments

Submissions

MTU

Comments

The file being studied is Android related! DEX

T1 Interesting strings

<http://>
<http://en.utrace.de>
<http://ktosdelaetskrintotpidor.com>
<http://sositehuypidarasi.com>
<https://>
<https://ejiuehsfuihrizh97ihkefush8fih>
<https://support.google.com/calendar/a>
<https://twitter.com/salupko>



Peter Salupko

@salupko

Joined October 2018

[Tweet to Peter Salupko](#)

Tweets

1

[Tweets](#)

[Tweets & replies](#)



Peter Salupko @salupko · Oct 5

< zero
>MzZhYzA4MmM1MWUzZmUzZ
ZTA5YWVhMTU0ZDViNzUyNDNj<



Generical hunting ... in Twitter FIREHOSE

TEXT =>

Regular Expression

```
/^[-A-Za-z0-9+=]{10,200}|=[^=]|={3,}$/
```

Twitter Web Client	KeremTu81270252	Wed Ai
Twitter Web Client	KeremTu81270252	Wed Ai
Twitter for Android	UmutDalkran4	Sat Se
Twitter Web Client	LuptonnSigfried	Tue Se
. Twitter Web Client	ztormhouse	Thu Ma

More hashes...

3ed56b46d63a579c41b6155549cbf34d4658f897

887d70b487f02bf4b371463762b5d08aeccdf95f

e61ad5266bde54d52d82c44456f0a0a57f751c35

304c2700fe23cc2fdb9db32793c18fe38cb68c8d

d279011af309b02c71913650d078bb89e66ef66c

869924789293a5d4fd0b2d4d562e19b0340d5b0d

1f3c34040362fcc65e5f28ed146a83319ef40330

1b2359b3bd089431c53beba111ae4d68f854402b

a770bea65a9d6881a9592f6eb33f87df99df926d

5e3fc74cb9fc4052cb42de0af64b26785b972d01

a9f56a6def1413dc5f072add4ba6310207b1493d

49367acd5d2952e77b131d98c5f107f72f7bdd28

c0680c6c394920dbd13664d835de4811782fc1be

10f38918460fa89fa986320e124dd15fc58a33ac

1888739385f8052b7bb8e39f91724174a9feb5cb

57dd3fce429bca2b78f9de424422a323400782d

2f3a699502e1a5d26f7874a7ebdcba550c2dc701

a8293f802437f2027d1fe4c9fc72e4c0ef56a9d8

fc29a335a846edab3a843f7005262aeff1881c1b

1fd8c3320af1e39fa66bf92690f3f9d73cf9f8

647ae0dc7df2019beecc6adf796497b0b9e276bf

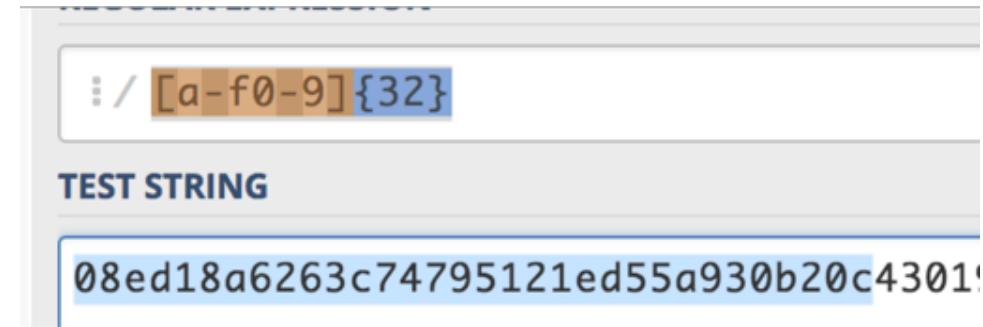
830cac9b5992edefd946335aa1fdb235bd9ca110



Indicator Hunting on Social Media

Security Operations Manager

More hashes... the Ultimate hunting skill 😊



What is this ..?

https://twitter.com/GrantEfendyan/status/1052200123034406912

Notifications Messages  Search Twitter

 GE
@GrantEfendyan 

Does anyone know what it could be
08ed18a6263c74795121ed55a930b20c4301
9c8b? [@Antelox](#) [@forensico](#) [@demonslay335](#)
[@securitydoggo](#) [@avman1995](#)
[@malwrhunerteam](#) [@JAMESWT_MHT](#)
[@Antelox](#) [@forensico](#) [@securitydoggo](#)
[@James_inthe_box](#) [@avman1995](#) [@xme](#)
[@Ring0x0](#) [@PolarToffee](#) [@siri_urz](#) [@x0rz](#)
[@dvk01uk](#)

10:10 PM - 16 Oct 2018

2 Likes 

 4   2  



 **Martin Stopka** @stopka_martin · Oct 17
Replying to @GrantEfendyan @Antelox and 13 others
Win64/Exploit.CVE-2018-8453.A

2 2 2 1

NVD - CVE-2018-8453
<https://nvd.nist.gov/vuln/detail/CVE-2018-8453> ▾
Oct 10, 2018 - Description. An elevation of privilege vulnerability exists in Windows v... component fails to properly handle objects in memory, ...

Investigating Mal-Actors on Social Media



Disclaimer and clarification

We refer to these individuals as hackers for simplicity

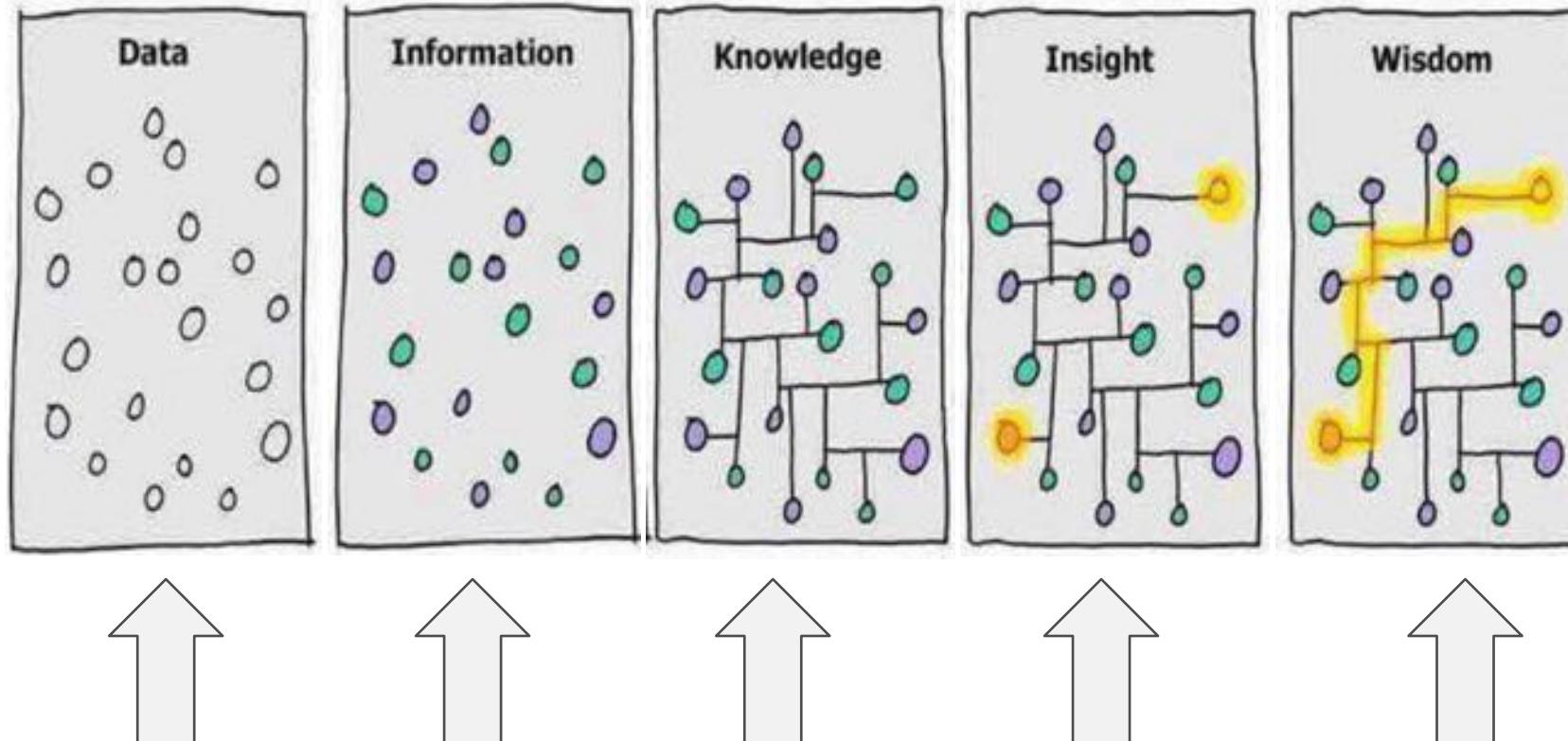
“Hacker” groups in context of this presentation are :

- Mostly Anonymous and other “Hacktivism” communities that cause some mischief and trouble.
- have low technical skill level
- highly socially active
- can be damaging due to low cost of online “Hacker” services
- can produce or provoke a social response. At times, in real-life

Methodology - Overview

- Utilized Tweets scrapped from known handles for suspected hackers and hacking groups: sources - Hacktivism and Digital Extortion actors
- Used a variety of methods to map inter-relationship between entities:
 - Shout Outs
 - Quotes/Retweets/Reposts
 - Followings
 - Followers
- Used a variety of metrics to weight the social mapping
- Goal: **Situational Awareness**

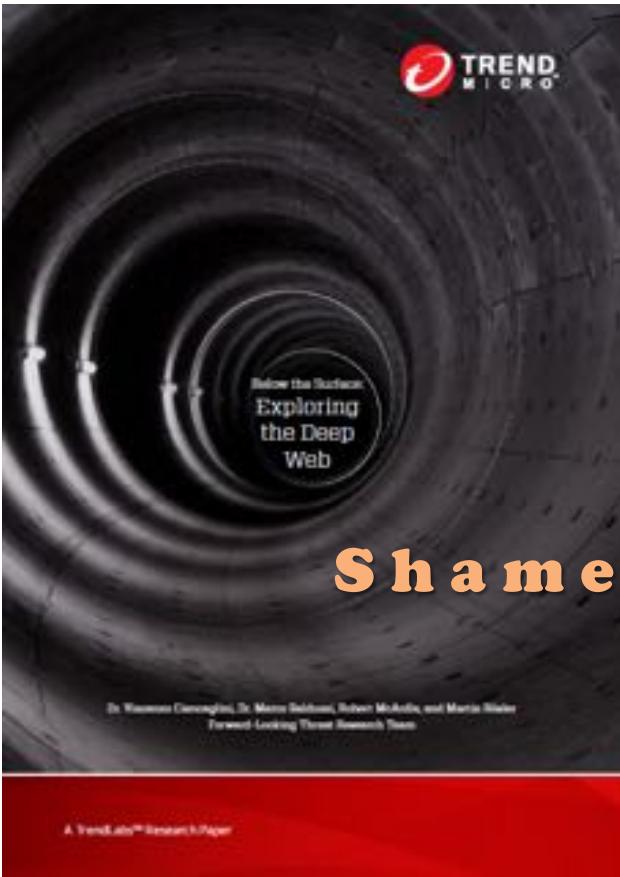
Methodology - Overview



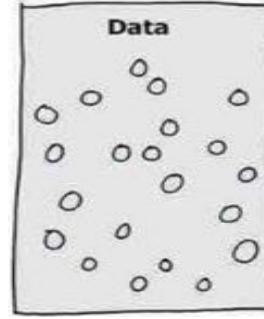
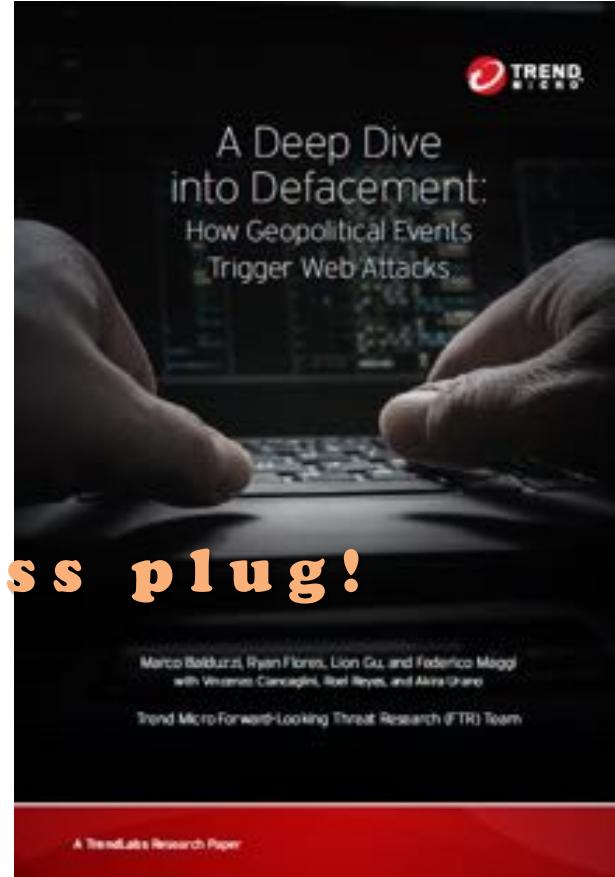
Twitter Specific Shoutout Identify Assess
/ Tweets Accounts Mapping Connections Relationship

The Data: Identify Groups

Deepweb



Hacktivism

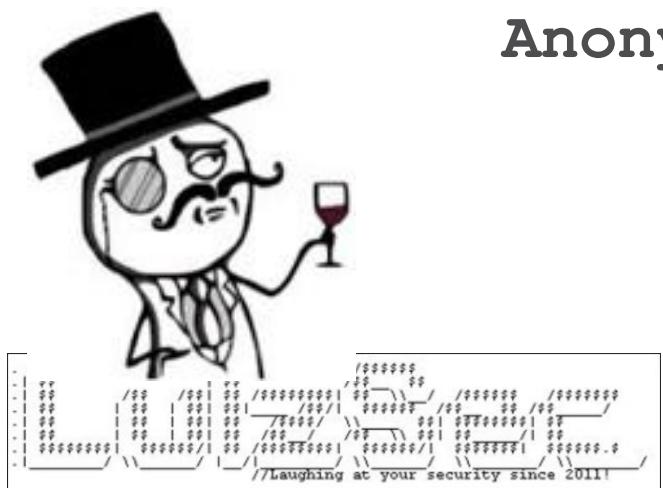


Where did we start?

ARMADA COLLECTIVE
@accREthink



Anonymous

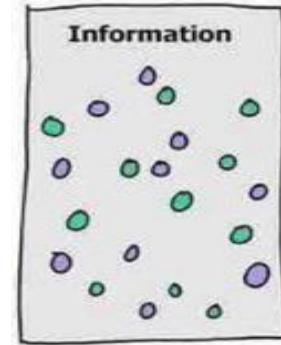


Found More Info

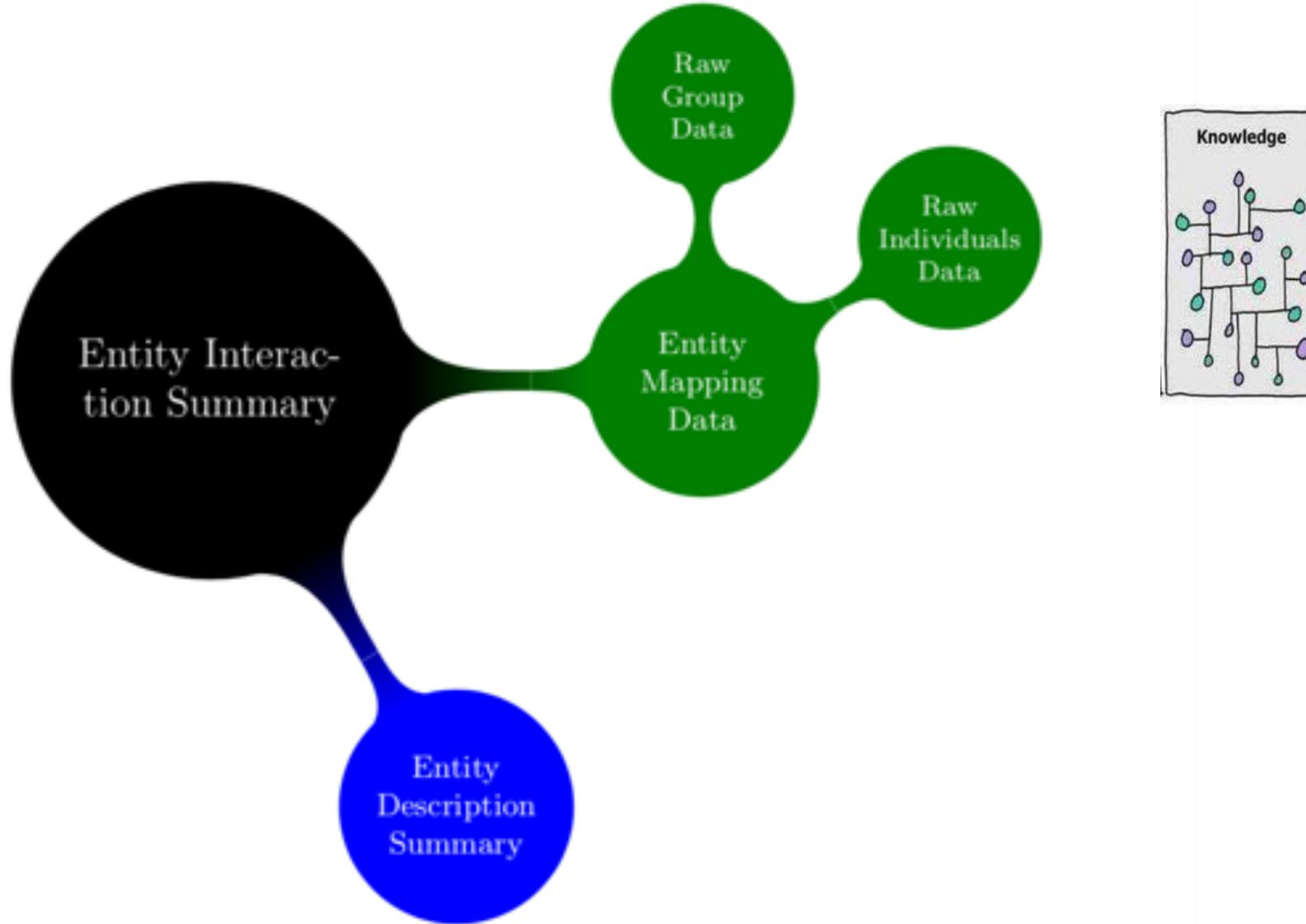
n.ScreenName	n.UserName	n.ScreenName	n.UserName
LizardL4nds	R.I.U. Lizard Sq	UGLegion	Lizard Squad
DeepWebOutlaws	Deep Web Out	Official_SEA7	SyrianElectronicArmy
DeadSecurity	Anonymous	TheLizzardSquad	Lizard Squad
		FancyBears	Fancy Bears' HT
		cyberberkut2	?????????????
		Offsecurity	OffSecurity
		Liz4rdL4nds	Alg0d (LizardSquad)
		accREthink	ARMADA COLLECTIVE
X0mbra32	Xombr @_Team	darkunity1174	DARKUNITY
uwteam	UW-TEAM.org	GhostSecGroup	Ghost Security Group
LizardLands	Lizard Squad	GhostSec_	GhostSec
Team_Missing_No	Team MissingN	LulzGhost2017	LulzGhost
Oxarch	NullCr3w	mcaddosteam	MCA DDOS Team
GhostSquadHack	~#GhostSquad	nwhownz	New World Hackers
FinestSquad	The Finest	reswitchedteam	ReSwitchedTeam
ShadowBroker	Shadow Vine	Shad0wS3C	Shad0w Security
AnonySecTeam	Anonymous	TheSshadowSquad	Shadow Squad
		Teamgreyhat	Team Greyhat
SlimeHax	Team Slime	TeaMp0sioN	TeaMp0sioN
plagueethehacker	plague	null	
HY9R0	./HYDRO\\.	null	

The Information: Twitter Harvesting

- Use your favorite hunting tool, such as Maltego
 - **PRO:** Easy to use, click of a button
 - **CON:** LOTS of noise, Extracting data a pain; tweet data is only good about 10 days, may not include data if user deleted tweet
- Invest in a social media tool (shout out to MentionMapp – paid, but not expensive)
 - **PRO:** SUPER easy to use, click of a button
 - **CON:** Generally only 1 user or hashtag at a time so have to do rest manually; only have as back as the tool allows, most only go back 2 weeks even at premium accounts
- Get an easy to use command line tool for twitter write a cron to do ongoing scrapping, like Twint
 - **PRO:** Very good coverage, easy to manipulate once collection has soaked
 - **CON:** Takes a bit to set up and test; lots of data to scrape through



The Knowledge: Putting it together



The Knowledge: Putting it together

```
sasha@vm-sasha:~/reports/twitter/GroupsAndIndividuals/analysis
SHOUTOUTTIMESTAMP=$(SHOUTOUTTIME2)" "$SHOUTOUTOFFSET

#make list of URLs posted
echo $LINE | csvcut -c 3 | sed 's/hashtags/!hashtags/' | sed 's/user_mentions/!user_mentions/' | grep urls | tr -d_url=//>> URLList.tmp

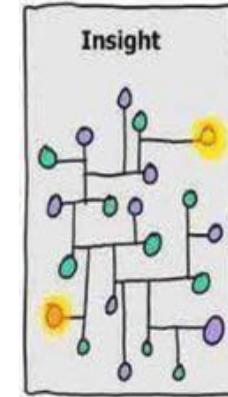
sasha@vm-sasha:~/reports/twitter/GroupsAndIndividuals/analysis
sasha@ftrCluster 2018-05-16 14:32:12$ cat parser.sh
#!/bin/bash

#script to parse shoutouts out of twitter
#sashahellberg May2018

#vars
INPUTFILE=$1
TYPE=$((2^2))
TIMESTAMP='date +%Y%m%d-%H%M%S'
PARSEDFILE="Parsed_$INPUTFILE.tmp"
OUTPUTFILE="MappingList_$TYPE_entities_$TIMESTAMP.out"

#setup
echo "ENTITIES"
csvcut -c 1
echo parse
cat $INPUTFILE
ls -la $PARSEDFILE

AmberHo08469812,groups,KEEMSTAR,Individual,Shoutout,TwitterLogs_InText,M2,20180429,16:05:59 +0000
AmberHo08469812,groups,KimDotcom,Individual,Shoutout,TwitterLogs_InText,M2,20180429,16:05:59 +0000
AmberHo08469812,groups,LizardMafia,Individual,Shoutout,TwitterLogs_InText,M2,20180429,16:05:59 +0000
AmberHo08469812,groups,AnonymousWiki,Individual,Shoutout,TwitterLogs_InText,M2,20180429,16:05:59 +0000
DataBreachToday,groups,ThaiCERT,Individual,Shoutout,TwitterLogs_InText,M2,20180426,14:48:00 +0000
DataBreachToday,groups,McAfee,Individual,Shoutout,TwitterLogs_InText,M2,20180426,14:48:00 +0000
ipfconline1,groups,Shirastweet,Individual,Shoutout,TwitterLogs_InText,M2,20180426,17:16:51 +0000
pierrepinna,groups,Shirastweet,Individual,Shoutout,TwitterLogs_InText,M2,20180426,11:57:36 +0000
inquit,groups,threatpost,Individual,Shoutout,TwitterLogs_InText,M2,20180427,17:33:02 +0000
NicaTuitero,groups,LorianSynaro,Individual,Shoutout,TwitterLogs_InText,M2,20180426,14:06:33 +0000
NicaTuitero,groups,NamaTikure,Individual,Shoutout,TwitterLogs_InText,M2,20180426,14:06:33 +0000
NicaTuitero,groups,Manwe_Ainur_Sec,Individual,Shoutout,TwitterLogs_InText,M2,20180426,14:06:33 +0000
NicaTuitero,groups,Scode404,Individual,Shoutout,TwitterLogs_InText,M2,20180426,14:06:33 +0000
IdeaGov,groups,threatpost,Individual,Shoutout,TwitterLogs_InText,M2,20180427,16:06:16 +0000
```

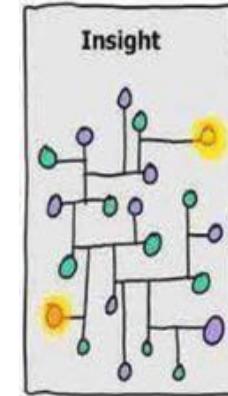


The Insight: Mapping Connections

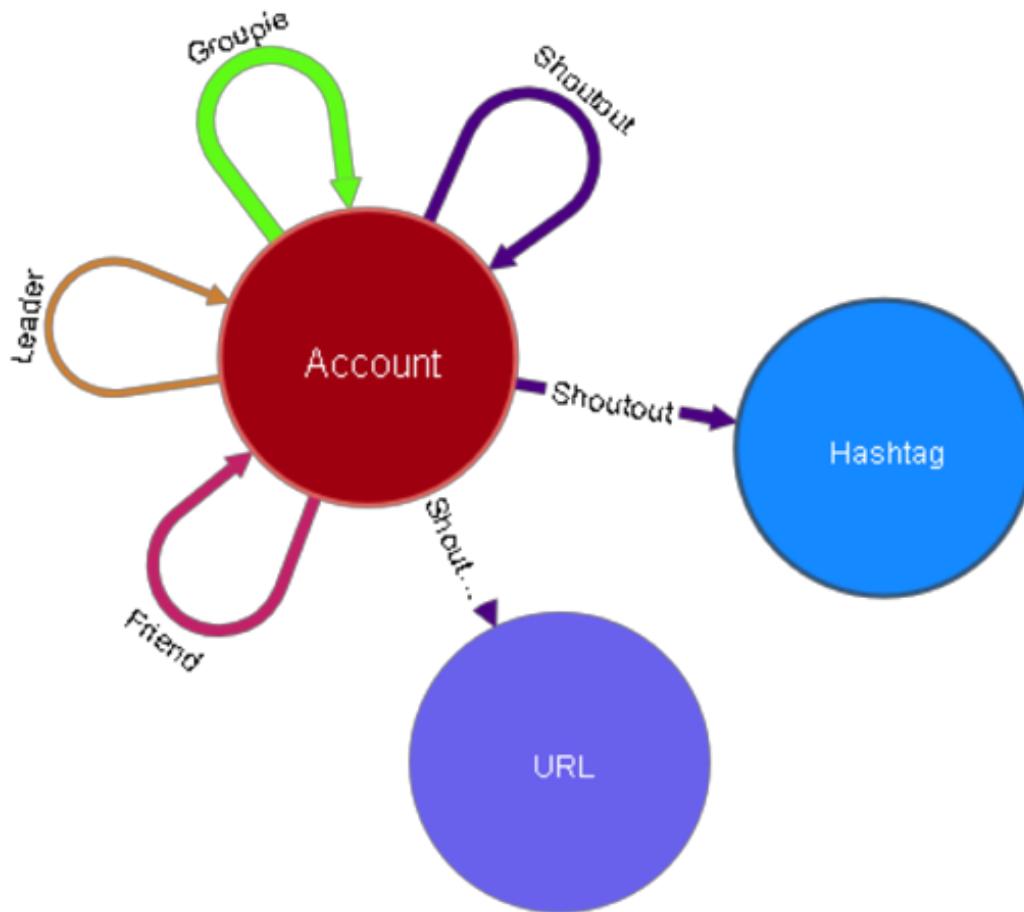
Where entity == matching in either the name or display name to a known nick for a hacker or group

- Type 1: Shout outs by Entity: If an entity does a shoutout in the body of their tweet to another user (@), hashtag (#), or URL (http)
- Type 2: Shout outs to the Entity: If the entity is in the text of a tweet, either as a user (@) or hashtag (#)
- Type 3: If the entity is quoting someone
- Type 4: If the entity is retweeting (RT) someone
- Type 5: If the entity is being quoted by someone
- Type 6: If the entity is being RT'ed by someone

Each of these were mapped as a 1 way connection, but in some cases the findings would show a mutual connection

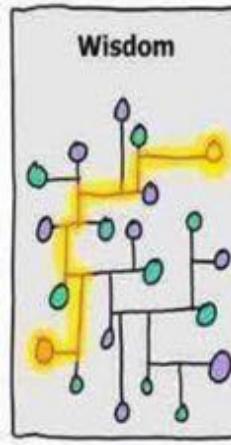


The Insight: Mapping Connections



The Insight: Mapping Connections

ENTITY	LINK	LASTUPDATE
probouwteam_nl GROUP https://		
probouwteam_nl GROUP https://		
AB3bouwteam GROUP https://www.		
AB3bouwteam GROUP #female		
AB3bouwteam GROUP https://www.		
AB3bouwteam GROUP #animalwri		
AB3bouwteam GROUP #maximumvi		
AB3bouwteam GROUP #eho500		
AB3bouwteam GROUP #ebueco		
AB3bouwteam GROUP #glasir N		
probouwteam_nl GROUP https://		
probouwteam_nl GROUP https://		
AB3bouwteam GROUP https://www.		
AB3bouwteam GROUP #report I		
AB3bouwteam GROUP #workingpro		
AB3bouwteam GROUP #absbouwte		
probouwteam_nl GROUP https://		
probouwteam_nl GROUP Renovat		
probouwteam_nl GROUP https://		
probouwteam_nl GROUP https://		
official_SEA7 GROUP https://		
uvteam GROUP https://twitter		
uvteam GROUP maniarcowicz I		
uvteam GROUP #2Bmocelidt B		
Official_SEA7 GROUP http://d		
bouwteamdoest GROUP https://w		
bouwteamdoest GROUP #tvcoast		
official_SEA7 GROUP http://d		
Official_SEA7 GROUP https://		
Team_Missing_No GROUP https:		
	A	
1 ENTITY	B	
2 Syriasonline	Official_SEA7	20180412 20:31:14 +0000
3 EllenBoontje1	Top_Job_Afbouw	
4 EllenBoontje1	Nynemien	
5 EllenBoontje1	EenVandaag	
6 EllenBoontje1	BerkelNicolette	
7 dkeerl	Famed	
8 dkeerl	FinestSquad	
9 LITTLEONEHATE	Snowytheg	20180503 21:06:21 +0000
10 LITTLEONEHATE	FinestSquad	
11 CyB3RGh0s7	http://www.mylefkada.gr	
12 CyB3RGh0s7	#Offline	
13 CyB3RGh0s7	#TangoDown	
14 CyB3RGh0s7	SecNews_GR	
15 CyB3RGh0s7	DeepWebOutlaws	
16 CyB3RGh0s7	T0x1c_Phantom	
17 CyB3RGh0s7	h0t_p0ppy	
18 WalterEugeneCr2	realDonaldTrump	
19 WalterEugeneCr2	BarackObama	



The Wisdom: Weighing Connections

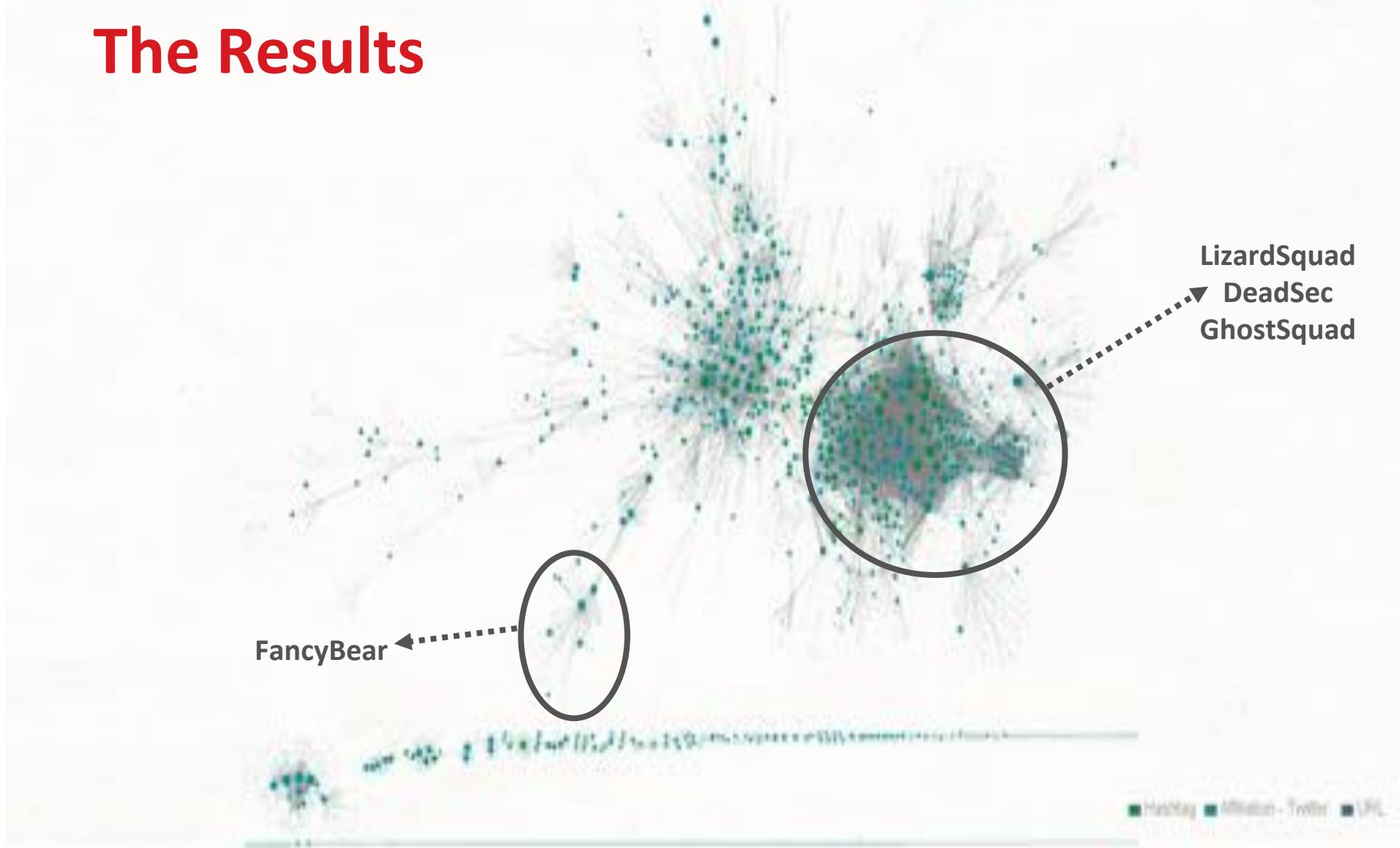
	Entity to Them	Them to Entity
Followers	<i>Needs Qualifying, see below</i>	<i>Needs Qualifying, see below</i>
Following	<i>Needs Qualifying, see below</i>	<i>Needs Qualifying, see below</i>
Friends(1)		High
Leaders(2)	Moderate	Group
Groupies(3)	Poor	Leader
Shoutout	High	Moderate
RT	Low	Poor
Quote	Moderate	Poor

(1) Friends is where both follow each other

(2) Where the first party follows the second but the second party does not follow back

(3) Where the second party follows the first, but the first does not follow back

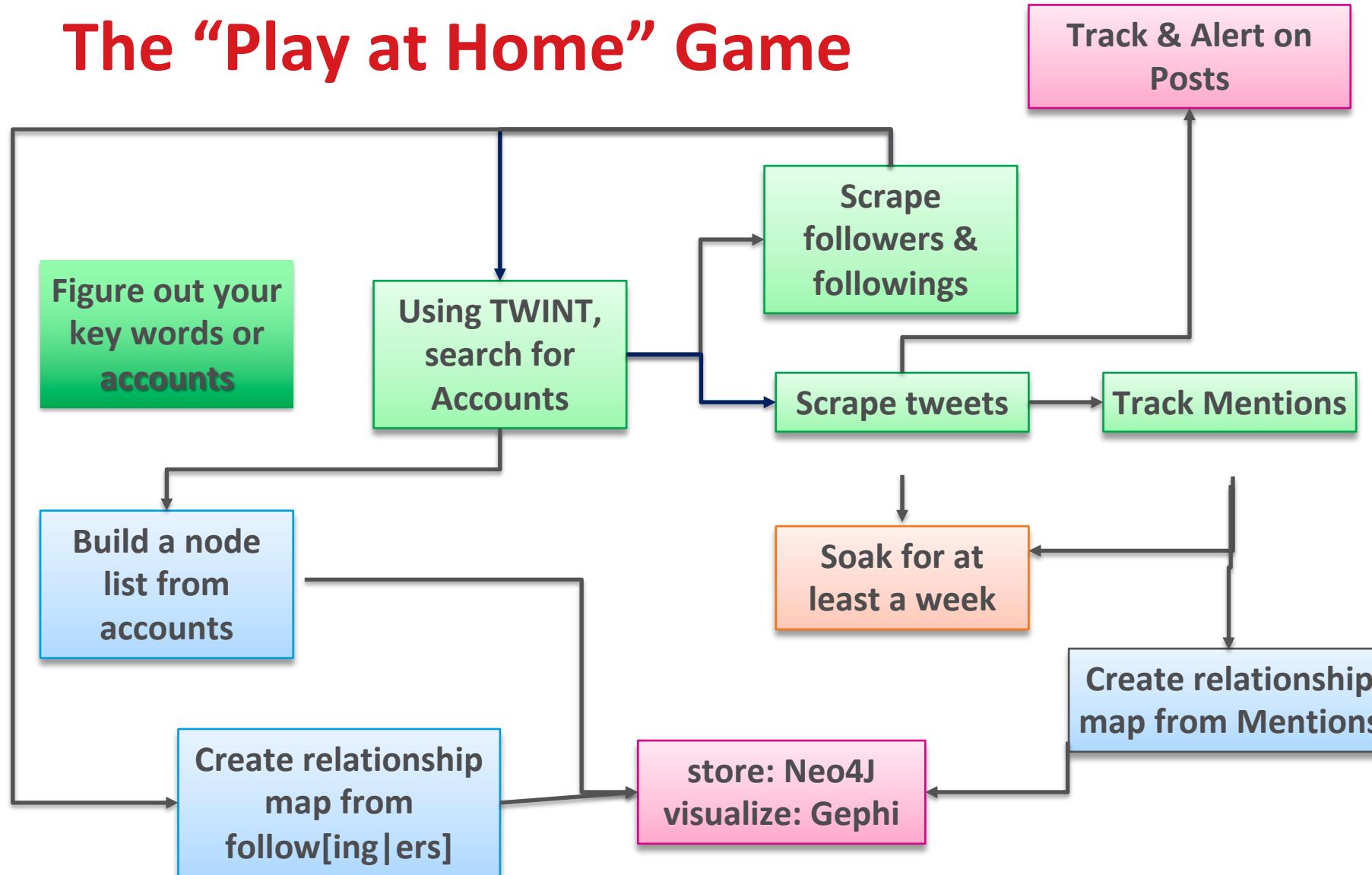
The Results



Iterative Process

- Layer 1A: Look at pre-identified Group Handles, and their connection and weightings to other entities
- Layer 1B: **Filter out the noise** each time our the map becomes unusable!!
• Layer 1C: Map them into the above to find deeper pockets
- Layer 2B: Find all the connections and weightings to those identified in Layer 1A

The “Play at Home” Game



Detecting Twitter Bot Presence

Because bots are everywhere :)

Secure | https://1000twitters.ru/zakaz-tvitter-akkaunty-s-3000-chitatelyami

HOME STORE + SERVICES + BLOG + CONTACTS Email: admin@1000twitters.ru Telegramm: @a_korrrch

Downloaded fake accounts of Twitter with 3000+ readers with EMAIL activation
TwitterAudit 96% + (twitter auditing what it is)

Ordering

Accounts with 3000+ TwitterAudit 96% + = 2570.00 руб. per account



E-mail for delivery *

Choose the possible payment method:

Payment on the site using Webmoney ▾

Secure | https://www.twitteraudit.com/realDonaldTrump

TWITTER

Upgrade to Pro to find ar

TwitterAudit Report



Donald J. Trump @realDonaldTrump

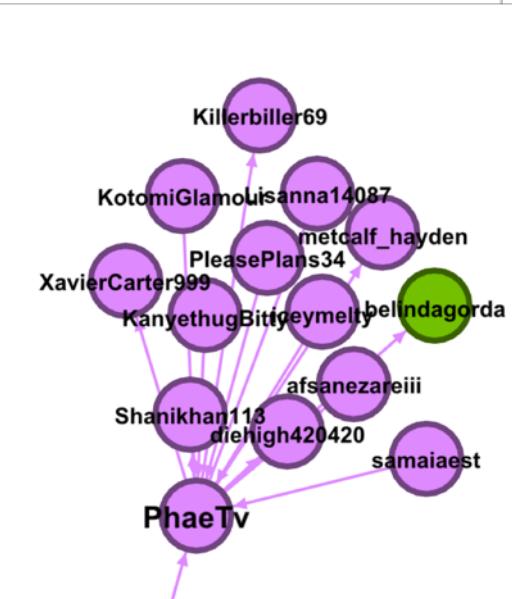
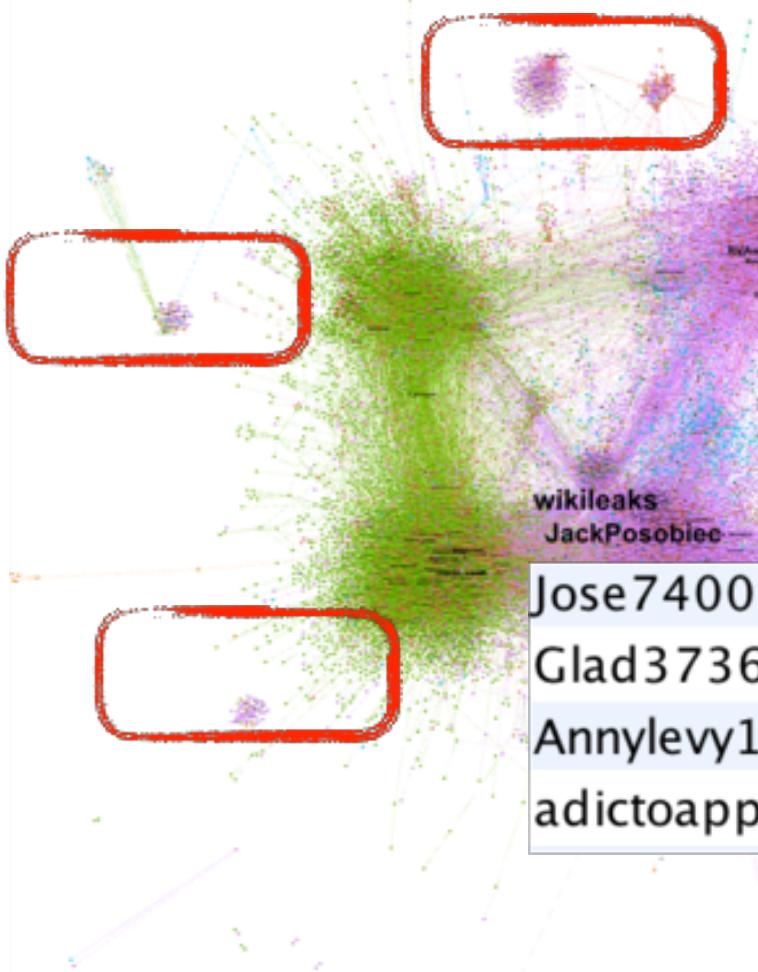


44,714,372 F

8,264,742 F

Followers

Bots, Bots Everywhere :)



2-03 13:52:22
2-03 13:51:35
2-03 13:27:42
2-03 13:27:37
2-03 11:39:02
2-03 10:59:51
2-03 10:17:13
2-03 10:15:12
2-03 10:12:46

017-12-01 22:10:02

Glad37367052	es	2017-12-01 22:09:33
--------------	----	---------------------

Annylevy1	pt	2017-12-01 21:55:01
-----------	----	---------------------

adictoapple3	es	2017-12-01 21:25:28
--------------	----	---------------------

JH1650	en	2017-12-03 03:16:17
ChandlerAlanPa1	en	2017-12-03 01:50:00
Academicolatino	es	2017-12-03 01:15:46
Rita_OraFanPage	en	2017-12-02 23:17:17
Ianadelsly	en	2017-12-02 23:17:03
CherylM27017471	en	2017-12-02 23:03:15
MissyCanadian	en	2017-12-02 22:51:23
Emmanue52216761	en	2017-12-02 22:47:28
thomassee7020	en	2017-12-02 21:17:20

Examples of Bots

The image displays five separate Twitter user profiles, each showing a different type of bot or automated account:

- Profile 1 (Top Left):** A profile featuring a circular profile picture of a hawk's head. The user is named "Дарья ДарЁва" (@PkJY2g8QyTGcH56) and is located in "РОССИЯ АЛТАЙ". It was joined in December 2015. The bio is entirely blank.
- Profile 2 (Top Middle):** A profile with a large, solid gray circular placeholder icon. The user is named "Михаил" (@x2MRrYpXCvHbyjz) and was joined in March 2017. It has 1,496 tweets, 281 followers, and 36 following.
- Profile 3 (Bottom Left):** A profile with a large, solid gray circular placeholder icon. The user is named "Вадим" (@2N9EmRyBUBQ30ch) and was joined in March 2017. It has 8,807 tweets, 18 photos and videos, and 18 photos and videos.
- Profile 4 (Bottom Middle):** A profile featuring a circular profile picture of a woman's face. The user is named "Лена" (@bKfuc47oqOCTwCb). The bio is partially visible, ending with "...тоящего и будущего". It has 1,496 tweets, 281 following, 36 followers, 1,334 likes, and 1 list.
- Profile 5 (Bottom Right):** A profile featuring a circular profile picture of a cartoon character. The user is named "Телеканал Дождь" (@tvtrain). The bio reads: "О том как к власти пришел человек, устроивший крупнейший геноцид в истории человечества, за 5 минут". It has 1,496 tweets, 281 following, 36 followers, 1,334 likes, and 1 list. A large image of Adolf Hitler giving a speech is displayed prominently.

Final Words

Should you take your threat seriously?



NullCrew @NullCrew_FTS · Feb 1

Whelp, let's start things off properly - nullcrew.org/bell.txt - Bell, hacked by
#NullCrew

[Collapse](#)

[Reply](#) [Retweet](#) [Favorite](#) [More](#)

RETWEETS

3

FAVORITE

1



12:42 AM - 1 Feb 2014 · Details



NullCrew @NullCrew_FTS · Jan 15

Just had a talk with [@Bell_Support](#), this is going to be fun.

[Expand](#)

[Reply](#) [Retweet](#) [Favorite](#) [More](#)



NullCrew @NullCrew_FTS · Jan 14

Successful day hacking internet service providers is successful. #NullCrew

[Expand](#)

[Reply](#) [Retweet](#) [Favorite](#) [More](#)



siph0n - #NullCrew @siph0n_NC · Feb 4

@fairyocarina @NullCrew_FTS hope the Mounties bring me some syrup when
they come!

[Hide conversation](#)

[Reply](#) [Retweet](#) [Favorite](#) [More](#)

4:32 PM - 4 Feb 2014 · Details



Thanks for having us!

ANY QUESTIONS?

Email us at:

fyodor_yarochkin@trendmicro.com

sasha_hellberg@trendmicro.com

Vladimir_kropotov@trendmicro.com

