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 Ted 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 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 payload by Windows Notification Facility names using low-level Win calls.

ustayready/CasperStager

Joël Perras
@jperrass

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

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

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

Uploaded: 58 minutes ago
MD5:
4e5797312ed52d9eb80ec19848cadc95

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

Musings on the CRC function and who
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 Education
Best Builder Websites San Jose State University

Accept invitation Send InMail

www.linkedin.com/in/elizabethcrobrien/

50 connections
Known use by “red teams”
http://www.apkpkg.com/android/?product=yeecallpro

שלום, تمונית בупить זה להתקין.

אוקי, זהה.

שאני אני אישה לך תaviours טעמה

??

חזרה למה אתה מתק JSONExceptionים

版权所有: דובר chức"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

- 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

Interesting strings

http://
- http://en.utrace.de
- http://ktos delaetskrintotpidor.com
- http://sositehuypidarasi.com
- https://
- https://support.google.com/calendar/answer/6261
- https://twitter.com/96vqZcsxmL7sv73
- https://ys84h8hu8i8uj8u4554.com
Generical hunting … in Twitter FIREHOSE

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

Twitter Web Client
KeremTu81270252 Wed Apr
Twitter Web Client
KeremTu81270252 Wed Apr
Twitter for Android
UmutDalkran4 Sat Sep
Twitter Web Client
LuptonnSigfried Tue Sep
Twitter Web Client
ztormhouse Thu May
More hashes…

3ed56b46d63a579c41b6155549cbf34d4658f897
887d70b487f02bf4b371463762b5d08aeccdf95f
e61ad5266bde54d52d82c44456f0a0a57f751c35
304c2700fe23cc2fddb9db32793c18fe38cb68c8d
d279011af309b02c71913650d078bb89e66ef66c
869924789293a5d4fd0b2d4d562e19b0340d5b0d
1f3c34040362fcc65e5f28ed146a83319ef40330
1b2359b3bd089431c53beba111ae4d6f854402b
a770bea65a9d6881a9592f6eb33f87df99df926d
5e3fc74cb9fc4052cb42de0af64b26785b972d01
a9f56a6def1413dc5f072add4ba6310207b1493d
49367ac5d2952e77b131d98c5f107f72f7bddd28
c0680c6c394920dbc13664d835de4811782fc1be
10f38918460fa89fa986320e124dd15fc58a33ac
1888739385f8052b7bb8e39f91724174a9feb5cb
57dd3fceb429bca2b78f9de424422a323400782d
2f3a699502e1a5d26f7874a7ebdcbba550c2dc701
a8293f802437f2027d1fe4c9fc72e4c0ef56a9d8
fc29a335a846edab3a843f7005262aeff1881c1b
1fd8c3320af1e39fa66bf92690f3f9d73ccfc9f8
647ae0dc7df2019beec6adf796497b0b9e276bf
830c9b5992e0ef946335aa1fdcb235bd9ca110
Indicator Hunting on Social Media

Security Operations Manager
More hashes… the Ultimate hunting skill 😊
What is this ..?

Does anyone know what it could be 08ed18a6263c74795121ed55a930b20c43019c8b? @Antelox @forensico @demonslay335 @securitydoggo @avman1995 @malwrhunterteam @JAMESWT_MHT @Antelox @forensico @securitydoggo @James_inthe_box @avman1995 @xme @Ring0x0 @PolarToffee @siri_urz @x0rz @dvk01uk

10:10 PM - 16 Oct 2018
Martin Stopka @stopka_martin · Oct 17
Replying to @GrantEfendyan @Antelox and 13 others
Win64/Exploit.CVE-2018-8453.A

NVD - CVE-2018-8453
Oct 10, 2018 - Description. An elevation of privilege vulnerability exists in Windows where a 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 / Tweets
Specific Accounts
Shoutout Mapping
Identify Connections
Assess Relationship
The Data: Identify Groups

Deepweb

Hacktivism

Shameless plug!
Where did we start?

Anonymous

ARMADA COLLECTIVE
@accREthink
### Found More Info

<table>
<thead>
<tr>
<th>n.ScreenName</th>
<th>n.UserName</th>
</tr>
</thead>
<tbody>
<tr>
<td>LizardL4nds</td>
<td>R.I.U. Lizard Squad</td>
</tr>
<tr>
<td>DeepWebOutlaws</td>
<td>Deep Web Out</td>
</tr>
<tr>
<td>DeadSecurity</td>
<td>Anonymous</td>
</tr>
<tr>
<td>X0mbra32</td>
<td>Xombr@_Team</td>
</tr>
<tr>
<td>uwteam</td>
<td>UW-TEAM.org</td>
</tr>
<tr>
<td>LizardLands</td>
<td>Lizard Squad</td>
</tr>
<tr>
<td>Team_Missing_No</td>
<td>Team Missing</td>
</tr>
<tr>
<td>0xarch</td>
<td>NullCr3w</td>
</tr>
<tr>
<td>GhostSquadHack</td>
<td>~#GhostSquad</td>
</tr>
<tr>
<td>FinestSquad</td>
<td>The Finest</td>
</tr>
<tr>
<td>ShadowBroker</td>
<td>Shadow Vine</td>
</tr>
<tr>
<td>AnonySecTeam</td>
<td>Anonymous</td>
</tr>
<tr>
<td>SlimeHax</td>
<td>Team Slime</td>
</tr>
<tr>
<td>plaguethethehacker</td>
<td>null</td>
</tr>
<tr>
<td>HY9R0</td>
<td>.//HYDRO\.</td>
</tr>
</tbody>
</table>
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

- Entity Interaction Summary
- Entity Mapping Data
- Raw Group Data
- Raw Individuals Data

Knowledge
The Knowledge: Putting it together
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

<table>
<thead>
<tr>
<th>ENTITY</th>
<th>LINK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syriasonline</td>
<td>Official_SEA7</td>
</tr>
<tr>
<td>EllenBoontje1</td>
<td>Top_Job_Afbouw</td>
</tr>
<tr>
<td>EllenBoontje1</td>
<td>Nynemien</td>
</tr>
<tr>
<td>EllenBoontje1</td>
<td>EenVandaag</td>
</tr>
<tr>
<td>EllenBoontje1</td>
<td>BerkelNicolette</td>
</tr>
<tr>
<td>dkeerl</td>
<td>Famed</td>
</tr>
<tr>
<td>dkeerl</td>
<td>FinestSquad</td>
</tr>
<tr>
<td>LITTLEONEHATE</td>
<td>Snowythege</td>
</tr>
<tr>
<td>LITTLEONEHATE</td>
<td>FinestSquad</td>
</tr>
<tr>
<td>CyB3R Gh0s7</td>
<td><a href="http://www.mylefkada.gr">http://www.mylefkada.gr</a></td>
</tr>
<tr>
<td>CyB3R Gh0s7</td>
<td>#Offline</td>
</tr>
<tr>
<td>CyB3R Gh0s7</td>
<td>#TangoDown</td>
</tr>
<tr>
<td>CyB3R Gh0s7</td>
<td>SecNews_GR</td>
</tr>
<tr>
<td>CyB3R Gh0s7</td>
<td>DeepWebOutlaws</td>
</tr>
<tr>
<td>CyB3R Gh0s7</td>
<td>T0x1c_Phonat</td>
</tr>
<tr>
<td>CyB3R Gh0s7</td>
<td>h0t_p0ppy</td>
</tr>
<tr>
<td>Walter Eugene Cr2</td>
<td>realDonaldTrump</td>
</tr>
<tr>
<td>Walter Eugene Cr2</td>
<td>BarackObama</td>
</tr>
</tbody>
</table>
The Wisdom: Weighing Connections

<table>
<thead>
<tr>
<th>Entity to Them</th>
<th>Them to Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Followers</td>
<td>Needs Qualifying, see below</td>
</tr>
<tr>
<td>Following</td>
<td>Needs Qualifying, see below</td>
</tr>
<tr>
<td>Friends (1)</td>
<td>High</td>
</tr>
<tr>
<td>Leaders (2)</td>
<td>Moderate</td>
</tr>
<tr>
<td>Groupies (3)</td>
<td>Poor</td>
</tr>
<tr>
<td>Shoutout</td>
<td>High</td>
</tr>
<tr>
<td>RT</td>
<td>Low</td>
</tr>
<tr>
<td>Quote</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

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**: Find all the connections and weightings to those identified in Layer 1A

- **Filter out the noise** each time our the map becomes unusable!!

- **Layer 2A**: Look at other pre-identified individuals Handles, and 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

Figure out your key words or accounts

Using TWINT, search for Accounts

Scrape followers & followings

Scrape tweets

Track & Alert on Posts

Track Mentions

Soak for at least a week

Create relationship map from Mentions

Build a node list from accounts

Create relationship map from follow[ing]ers

store: Neo4J
visualize: Gephi
Detecting Twitter Bot Presence
Because bots are everywhere :)

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

Ordering

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

Choose the possible payment method:
Payment on the site using Webmoney

Your discount: 3% Your price: 2492.90 pyb.
Bots, Bots Everywhere :)
Examples of Bots
Final Words
Should you take your threat seriously?
Thanks for having us!

Any Questions?

Email us at:
fyodor_yarochkin@trendmicro.com
sasha_hellberg@trendmicro.com
Vladimir_kropotov@trendmicro.com