CyberProof™

WHY VIRTUAL HUMINT IS VITAL TO EFFECTIVE THREAT INTELLIGENCE

BY EVA PROKOFIEV,
SENIOR INTELLIGENCE ANALYST,
CYBERPROOF

JULY, 2019

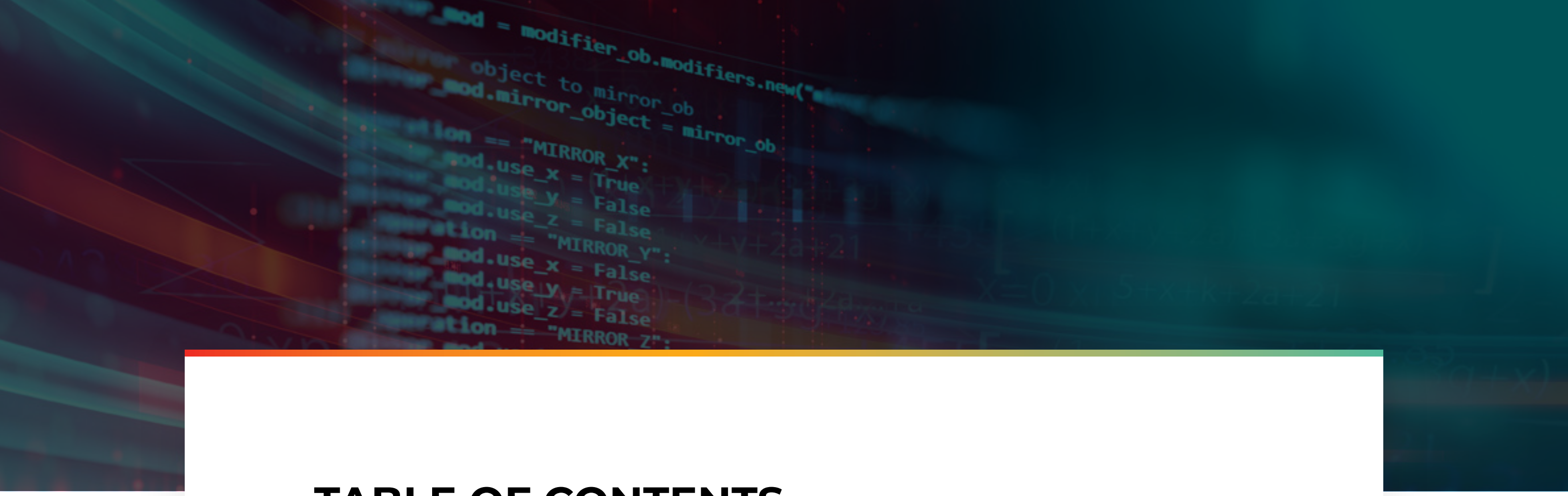


TABLE OF CONTENTS

IS HUMAN INTELLIGENCE (HUMINT) STILL RELEVANT, IN A TIME WHEN CYBERSPACE IS THE MAIN ARENA FOR ESPIONAGE?

This paper presents some of the new ways in which human intelligence (HUMINT) tactics in combination with OSINT (Open Source Intelligence) can be used to contribute to cybersecurity.

HOW HUMINT IS RELEVANT TODAY

In the era of cyber, intelligence gathering has shifted to the realm of the virtual. As a result, a variety of new methods, techniques, and tactics have been adopted that replaced the ones traditionally used in espionage.

To a large extent, many of the old approaches to intelligence gathering have been replaced. But has this had an impact on the success of intelligence? Is human intelligence (HUMINT) still relevant, in a time when cyberspace is the main arena for espionage?

This paper presents some of the ways in which human intelligence (HUMINT) tactics in combination with OSINT (Open Source Intelligence) can be used to contribute to cybersecurity. It provides investigation flows that illustrate how HUMINT, OSINT, and SOCMINT methodologies are used by analysts to explore, uncover, and understand the context and identity of threat actors. This type of investigation into a hacker's identity and motives is a crucial aspect of protecting organizations, allowing cybersecurity professionals to more effectively prevent and combat potential cyberattacks and threats.

Note that this paper does not discuss commercial threat intelligence platforms; rather, it focuses on showing OSINT methods used on top of the platforms and tools that are adopted by analysts as part of their investigations.

OVERVIEW OF THE ANALYTICAL PROCESS

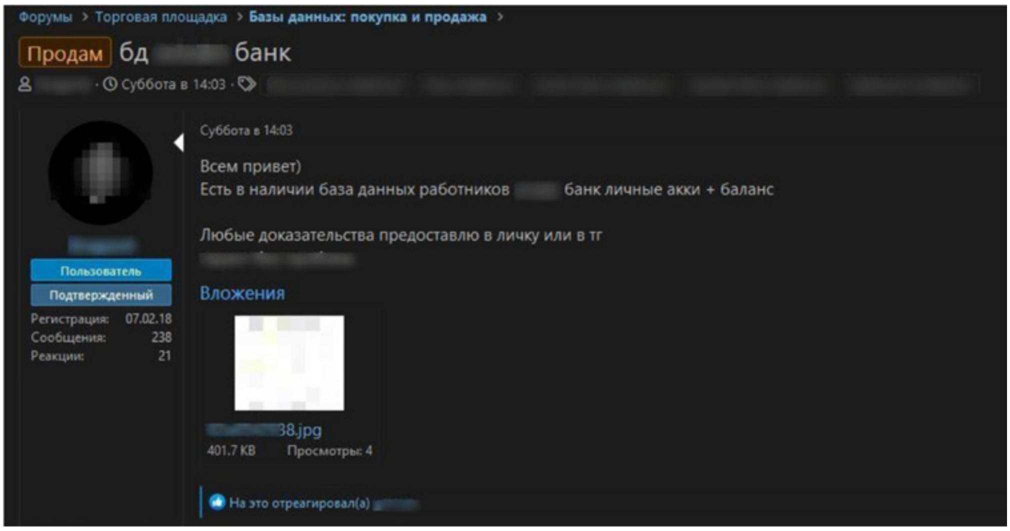
At the very highest level, conducting an analysis includes the following basic steps:

1. Define the initial information that you have access to – such as username and email address.
2. Define the goals of your analysis/investigation.
3. Gather the data.
4. Analyze the collected data.
5. Pivot, i.e., shift the investigation's focus, based on newly obtained indicators and information.
6. Validate the data gathered.
7. Generate a report.

CASE IN POINT:
A HACKER'S POST ABOUT A BANK DATABASE FOR SALE

The following sections provide an example of how cyber analysts use Virtual-HUMINT and OSINT resources, tools, techniques, and methodologies to identify and understand threat actors.

In this example, a hacker put up a post on a Russian-speaking forum that deals with hacking services and the trade of information including compromised data, databases, leaked credentials, and credit cards. The hacker made an announcement about a bank database for sale that lists the personal accounts and balances of the bank's employees.



Форумы > Торговая площадка > Базы данных: покупка и продажа >

Продам бд [redacted] банк

[redacted] · Суббота в 14:03 · [redacted]

Суббота в 14:03

Всем привет)
Есть в наличии база данных работников [redacted] банк личные акки + баланс

Любые доказательства предоставлю в личку или в тг
[redacted]

Вложения

[redacted]38.jpg
401.7 KB Просмотры: 4

На это отреагировал(а) [redacted]

[redacted]
Пользователь
Подтвержденный
Регистрация: 07.02.18
Сообщения: 238
Реакции: 21

Figure 1: Example of Bank Database for Sale

Gleaning Information from Telegram

The hacker wrote in the post on the Russian speaking forum that, in order to obtain proof of the quality of the database in question, users can either connect through the forum by sending a private message or they can connect via "тг" – which, in Russian, is short for "Telegram."

Telegram is an instant messaging, voice, and video messaging service. But as pointed out by Graham Penrose on CommsLock, for legitimate users, Telegram provides an abundance of publicly available metadata on user activities – information that can often be even more useful to threat actors than actual message content.

Telegram also exposes users to the possible theft of their phone numbers during the account verification process – which is used by criminals as an attack vector – and it potentially allows the theft of a user's contact database.

From the perspective of ethical hackers – anyone using OSINT for public safety and organizational security – Telegram is an important data provider and OSINT source.

Initial Analysis of the Post

From looking at the hacker's profile on the Russian-speaking forum, the following information could be obtained:

- Username
- Registration date, posts, and messages – indicating the hacker's level of activity in the forum
- Other means of communication and platforms where the hacker could be contacted
- Origin; based on a linguistic analysis of the posts, it seemed likely that the hacker is male and Russian
- Contact information or any other information might be revealed in other posts made by this user

Using Telegram to Learn More

By searching Telegram, we found the same username as the one displayed in the forum and identified a match. A review of the hacker's telegram profile revealed the following information:

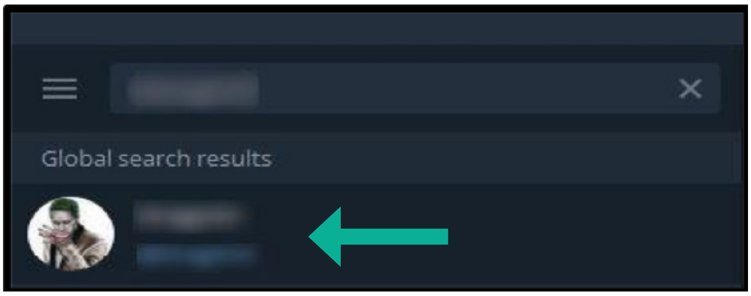
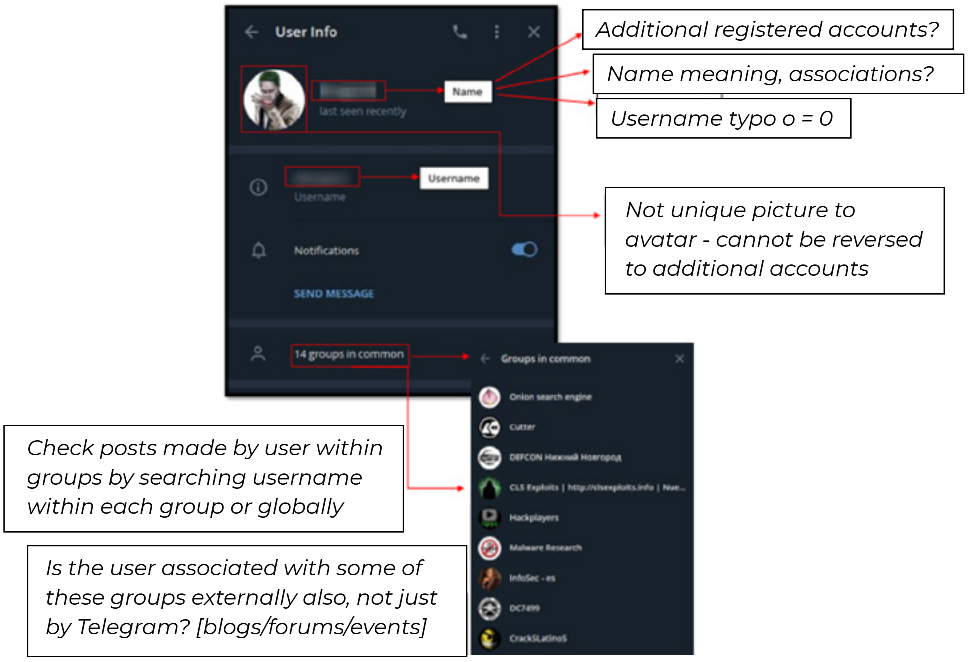


Figure 2: Extended Hacker Profile Information



Additional registered accounts?

Name meaning, associations?

Username typo o = 0

Not unique picture to avatar - cannot be reversed to additional accounts

Check posts made by user within groups by searching username within each group or globally

Is the user associated with some of these groups externally also, not just by Telegram? [blogs/forums/events]

Figure 3: Hacker's Telegram Profile

USERNAME SEARCH

When searching for a target's username, a good methodology to follow involves starting with the Google search engine.

In most cases, it is best to use multiple search engines – such as Yandex and Bing, for example, which are likely to be beneficial as they potentially provide additional results for our target.

A good username investigation methodology is IntelTechniques's username flow:

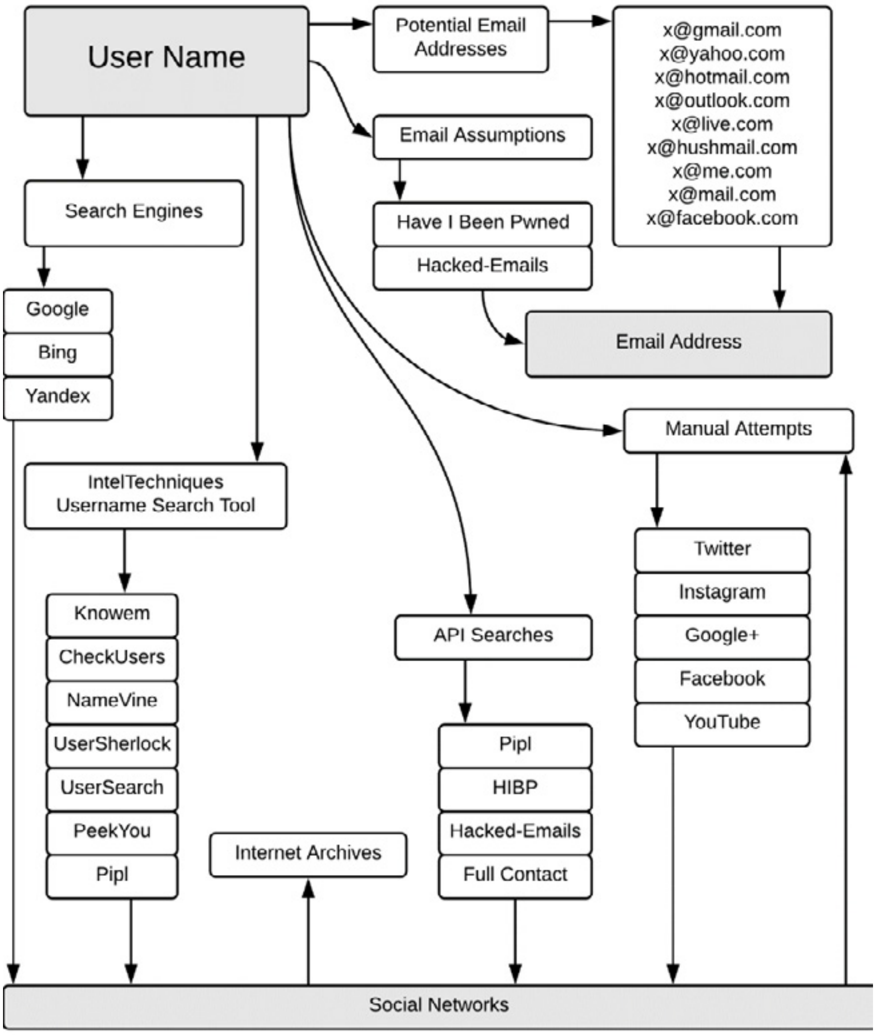


Figure 4: IntelTechniques.com OSINT Workflow Chart: User Name

Alternative search engines that are dedicated to username investigation, and that identify what social platforms usernames are registered on, include:

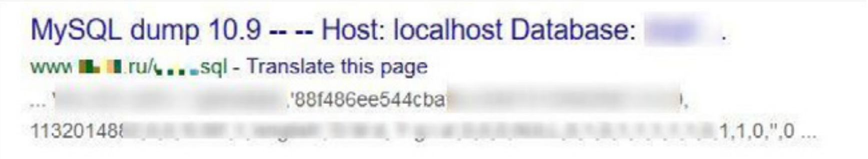
- http://www.usersherlock.com/usersearch/johndoe
- https://www.namecheckr.com/
- https://namechk.com/
- https://knowem.com/checkusernames.php?u=johndoe
- https://checkusernames.com/
- https://peekyou.com/username
- https://usersearch.org/
- https://searchpof.com/

It is best to use multiple sources in researching a single piece of information, since each search engine covers different social networks, blogs, platforms, and datasets.

Note: In some cases, it is valuable to check sql dumps, specific files, logs, or archives. These can be additional data sources where you can look for potential mentions of the username – e.g., saved archived IRC chats, non-compromised email dumps, etc.

The following is an example of what can be found using Google dork queries. A Google dork query is a search string using advanced search operators to find information not readily found on a website.

ext:txt | ext:log | ext:sql intext:johndoe

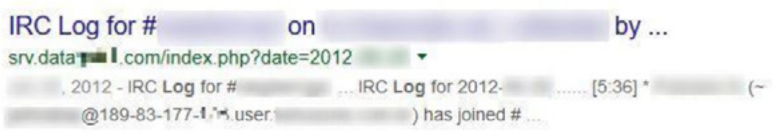


MySQL dump 10.9 -- -- Host: localhost Database: [redacted] .

www[redacted].ru/[redacted]sql - Translate this page

... [redacted] '88f486ee544cba[redacted],
11320148[redacted]1,1,0,'',0 ...

Figure 5: SQL Dumps, Logs and Archives



IRC Log for #[redacted] on [redacted] by ...

srv.data[redacted].com/index.php?date=2012[redacted] ▾

[redacted], 2012 - IRC Log for #[redacted] ... IRC Log for 2012-[redacted] ...... [5:36] * [redacted] (~
[redacted]@189-83-177-[redacted].user.[redacted]) has joined # ...

Figure 6: IRC Archived Chat Log

In this case, using Google dorks, we were able to learn additional types of information. We could also narrow our search to specific social networks including VK, Instagram, or platforms such as WordPress, blogs, forums, etc.

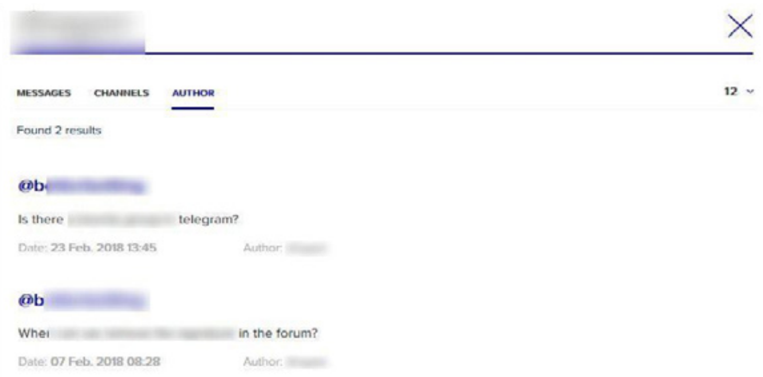
inurl:tid |thread | topic | blog intext:johndoe

Use the following syntax to search: site:vk.com johndoe – or narrow down the search to include specific keywords within the target's profile, which reduces false positives, for example: site:vk.com johndoe intext: keyword or using the + operator.

Another alternative for searching within dedicated platforms and communities (for example, Telegram) is buzz.im, which allows searching not only within groups, channels, and bots, but also searches users and user messages within public groups. Additional options are:

- Telegram's CSE
- TGSTAT

In this example, searching for the target's username allowed us to identify another group that this user posted in (or was mentioned in) – i.e., a group that we are not active members of.



MESSAGES CHANNELS AUTHOR 12

Found 2 results

@b[redacted]

Is there [redacted] telegram?

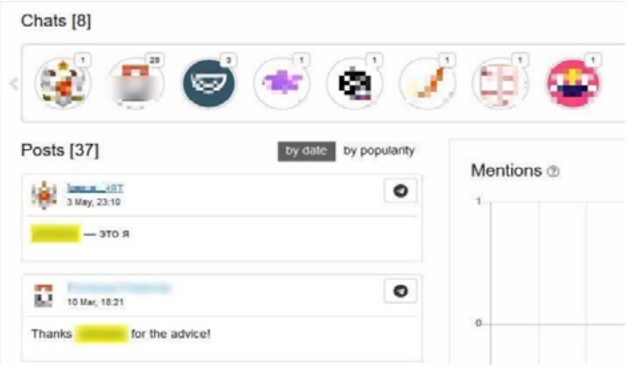
Date: 23 Feb. 2018 13:45 Author: [redacted]

@b[redacted]

Whe[redacted] in the forum?

Date: 07 Feb. 2018 08:28 Author: [redacted]

Figure 7: Alternative Search Options – buzz.im



Chats [8]

Posts [37] by date by popularity

[redacted] 3 May, 23:10

[redacted] — это я

[redacted] 10 Mar, 18:21

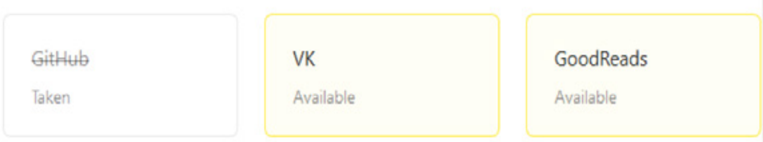
Thanks [redacted] for the advice!

Mentions

Figure 8: Alternative Search Options – tgstat

By opening the group via Telegram, we could see which user posted or mentioned the username. What is particularly useful about tgstat is that we can see data that has been deleted from the channels/groups by group administrators, or by the users themselves.

Additional methodologies and resources when using search engines for OSINT investigations can be found here, and dedicated search engines can be found here.



GitHub
Taken

VK
Available

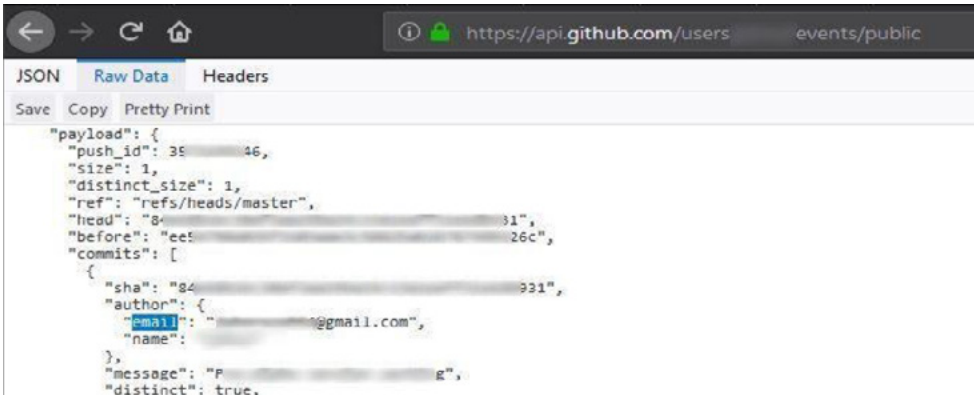
GoodReads
Available

Figure 9: Username Search Results – Github match

SCRAPING DATA FROM A GITHUB ACCOUNT

In the previous step (see Username Search) we identified a match with a registered GitHub account with the same username. This allowed us to use a method which could potentially extract interesting data from the GitHub account, such as an email address.

Use this method according to the following format, where “targetname” is the name of the user: https://api.github.com/users/targetname/events/public

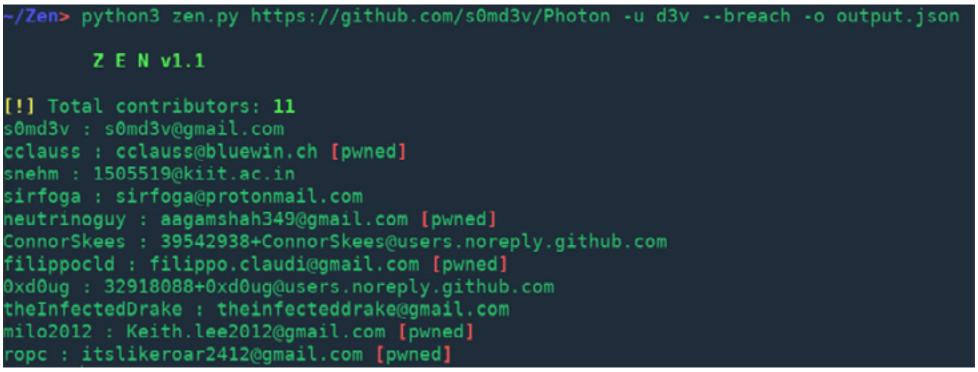


```
    "payload": {
      "push_id": [redacted],
      "size": 1,
      "distinct_size": 1,
      "ref": "refs/heads/master",
      "head": "[redacted]",
      "before": "[redacted]",
      "commits": [
        {
          "sha": "[redacted]",
          "author": {
            "email": "[redacted]@gmail.com",
            "name": [redacted]
          },
          "message": "[redacted]",
          "distinct": true,
```

Figure 10: GitHub Email

Extracted in the Following Format: johndoe.1199@gmail.com

Alternative methods and tools for scraping data from a GitHub account include Zen.



```
~/Zen> python3 zen.py https://github.com/s0md3v/Photon -u d3v --breach -o output.json

        Z E N v1.1

[!] Total contributors: 11
s0md3v : s0md3v@gmail.com
cclauss : cclauss@bluewin.ch [pwned]
snehm : 1505519@kiit.ac.in
sirfoga : sirfoga@protonmail.com
neutrinoguy : aagamshah349@gmail.com [pwned]
ConnorSkees : 39542938+ConnorSkees@users.noreply.github.com
filippocld : filippo.claudi@gmail.com [pwned]
0xd0ug : 32918088+0xd0ug@users.noreply.github.com
theInfectedDrake : theinfecteddrake@gmail.com
milo2012 : Keith.lee2012@gmail.com [pwned]
ropc : itslikeroar2412@gmail.com [pwned]
```

Figure 11: GitHub Email Extractor - Zen

GitHub Email Extractor is a resource that allows the exposure of email addresses from github accounts and checks if they were compromised.

EMAIL SEARCH

To further investigate the obtained email address (johndoe.1199@gmail.com), e.g., through Facebook or other social media, we used IntelTechnique's email address investigation methodology:

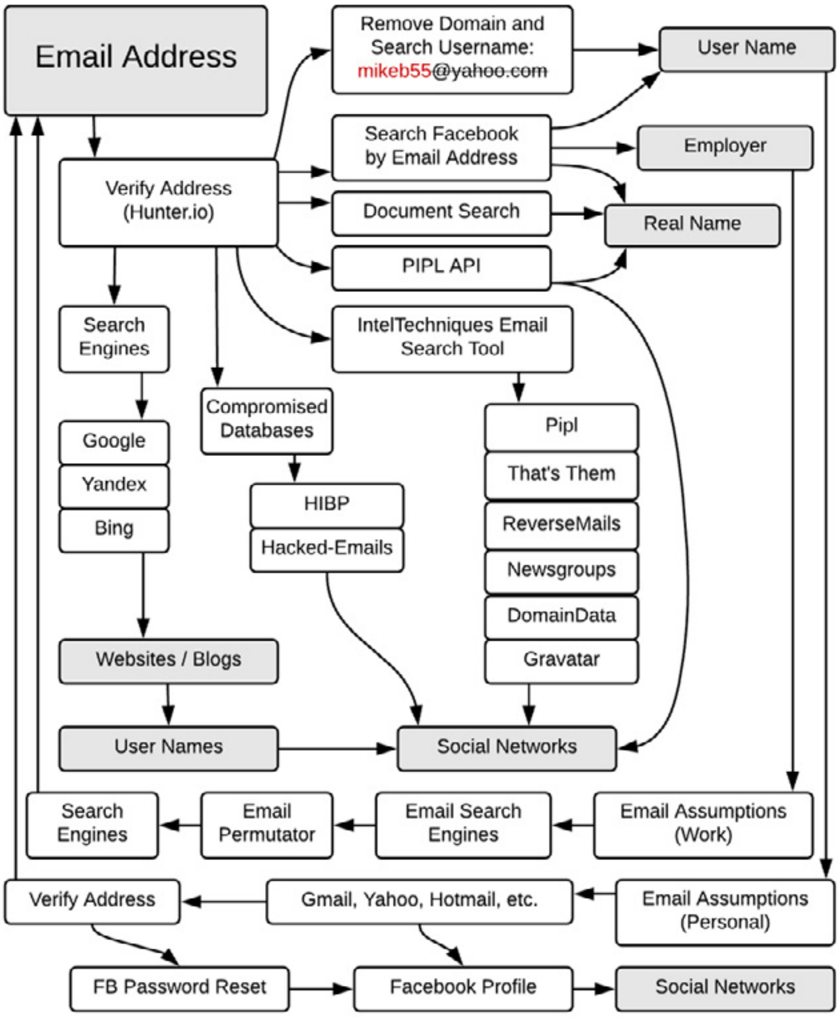
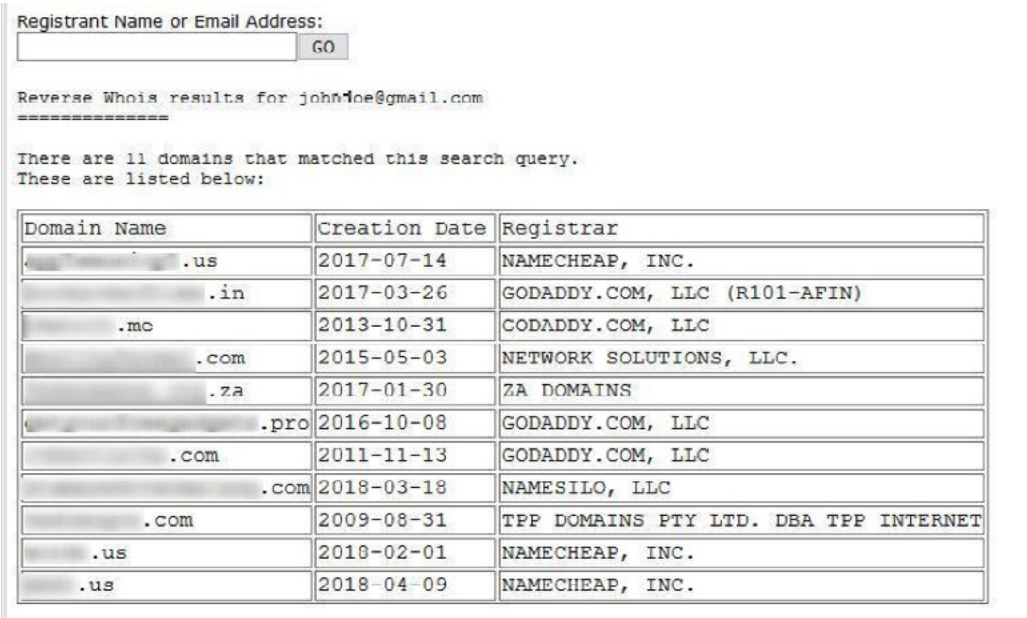


Figure 12: IntelTechniques.com OSINT Workflow Chart: Email Address

Next, identify whether any domains are registered on this same email address.
Use reverse WHOIS, for example: https://viewdns.info/



Registrant Name or Email Address:

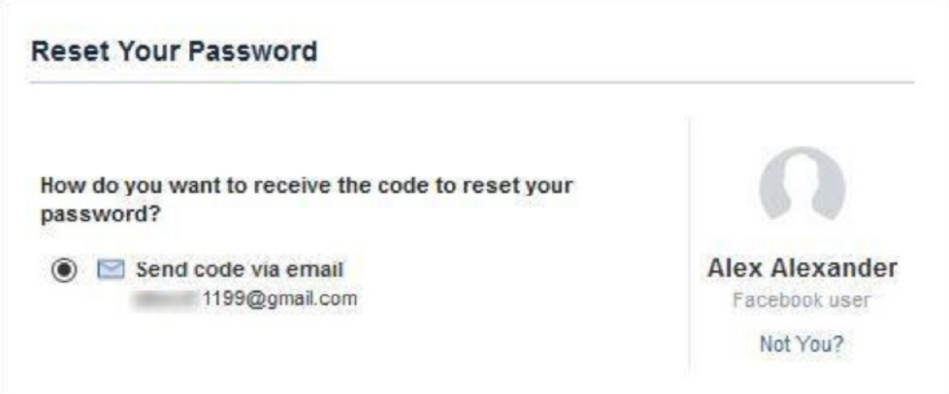
```
Reverse Whois results for johndoe@gmail.com
==============

There are 11 domains that matched this search query.
These are listed below:
```

Domain Name	Creation Date	Registrar
[redacted].us	2017-07-14	NAMECHEAP, INC.
[redacted].in	2017-03-26	GODADDY.COM, LLC (R101-AFIN)
[redacted].mc	2013-10-31	GODADDY.COM, LLC
[redacted].com	2015-05-03	NETWORK SOLUTIONS, LLC.
[redacted].za	2017-01-30	ZA DOMAINS
[redacted].pro	2016-10-08	GODADDY.COM, LLC
[redacted].com	2011-11-13	GODADDY.COM, LLC
[redacted].com	2018-03-18	NAMESILO, LLC
[redacted].com	2009-08-31	TPP DOMAINS PTY LTD. DBA TPP INTERNET
[redacted].us	2018-02-01	NAMECHEAP, INC.
[redacted].us	2018-04-09	NAMECHEAP, INC.

Figure 13: viewdns.info – Reverse WHOIS on an Email Address

Using reverse WHOIS, we were able to look up associated domains of our target based on email address, first.last name, and last.first name combinations.

While searching on Facebook, we identified an account called “Alex Alexander” associated with the email address found using GitHub:



Reset Your Password

How do you want to receive the code to reset your password?

● Send code via email
[redacted]1199@gmail.com

Alex Alexander
Facebook user

Figure 14: Identifying Target Social Media

Figure 15: Target Tagged Photo – Deleted from Posts on Social Media

Using dedicated search engines and tools for SOCMINT (social media investigations), we discovered that our target deleted all posts from his social media account, including locations and images, with one exception: We were able extract one image (since 2012) that our target was tagged in by another Facebook user.

We used this image and attempted to conduct a reverse search. Our goal was to see where else this image may have appeared in other social media platforms.

Additional resources for SOCMINT (Social Media Investigations) can be found here.

Different sites can be used to conduct a reverse image lookup – for example:

- TinEye
- Google Images
- Yandex Images
- Mobile Reverse Image Search
- Bing Images
- Collection of IMINT sources for imagery investigations
- Firefox add-on that makes it easy to check for stolen or identical pictures on the internet
- Chrome add-on that allows to conduct reverse image searches using various resources

Dedicated search engines for reverse images are focused on specific platforms, such as VK, and utilize advanced face recognition algorithms. For an example of how these are used, see the bellingcat blog here. Alternatives include FindClone.

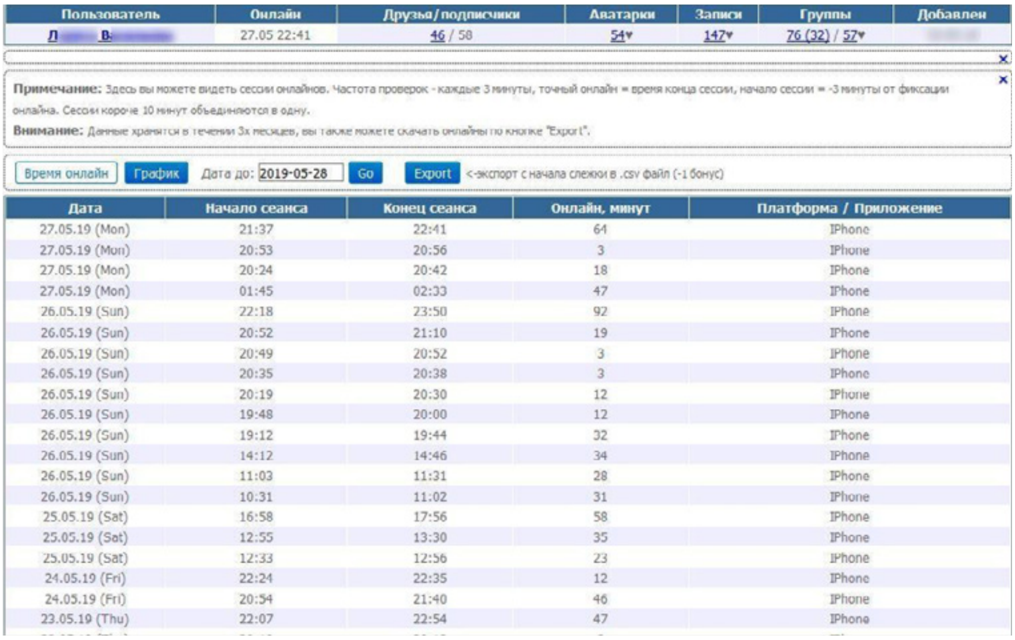
Using one of these resources, we identified a match: It turned out that this image also appeared in a different social platform called vk.com, a Russian social media and social networking service.

Additional tools that could be utilized in an image investigation like this include tools that extract interesting data metadata from pictures, such as location (GPS), camera type, and more. Some of these tools are:

- https://sno.phy.queensu.ca/~phil/exiftool/
- http://www.imageforensic.org/
- http://exif.regex.info/exif.cgi
- http://fotoforensics.com/
- https://github.com/redaelli/imago-forensics

Further information from the existing VK account can be obtained using dedicated tools and crawlers such as:

- Various OSINT resources for VK
- VK scraper – scrapes account data
- Resources that allow viewing activity analysis of a VK account ID – which is useful for investigation of a targeted ID



Пользователь	Онлайн	Друзья/подписчики	Аватарки	Записи	Группы	Добавлен
[redacted]	27.05 22:41	46 / 58	54▾	147▾	76 (32) / 57▾	[redacted]

Примечание: Здесь вы можете видеть сессии онлайнов. Частота проверок - каждые 3 минуты, точный онлайн = время конца сессии, начало сессии = -3 минуты от фиксации онлайна. Сессии короче 10 минут объединяются в одну.

Внимание: Данные хранятся в течении 3х месяцев, вы также можете скачать онлайны по кнопке "Export".

Дата до: 2019-05-28

<-экспорт с начала слежки в .csv файл (-1 бонус)

Дата	Начало сеанса	Конец сеанса	Онлайн, минут	Платформа / Приложение
27.05.19 (Mon)	21:37	22:41	64	IPhone
27.05.19 (Mon)	20:53	20:56	3	IPhone
27.05.19 (Mon)	20:24	20:42	18	IPhone
27.05.19 (Mon)	01:45	02:33	47	IPhone
26.05.19 (Sun)	22:18	23:50	92	IPhone
26.05.19 (Sun)	20:52	21:10	19	IPhone
26.05.19 (Sun)	20:49	20:52	3	IPhone
26.05.19 (Sun)	20:35	20:38	3	IPhone
26.05.19 (Sun)	20:19	20:30	12	IPhone
26.05.19 (Sun)	19:48	20:00	12	IPhone
26.05.19 (Sun)	19:12	19:44	32	IPhone
26.05.19 (Sun)	14:12	14:46	34	IPhone
26.05.19 (Sun)	11:03	11:31	28	IPhone
26.05.19 (Sun)	10:31	11:02	31	IPhone
25.05.19 (Sat)	16:58	17:56	58	IPhone
25.05.19 (Sat)	12:55	13:30	35	IPhone
25.05.19 (Sat)	12:33	12:56	23	IPhone
24.05.19 (Fri)	22:24	22:35	12	IPhone
24.05.19 (Fri)	20:54	21:40	46	IPhone
23.05.19 (Thu)	22:07	22:54	47	IPhone

Figure 16: Example of Activity Analysis Logs – VK.com User

Using the scrapers listed above, we were able to obtain the following information from our target account ID:

- Phone number
- Name
- Online activity analysis; searching for indicators of the target's full name, additional profiles, and more.

PHONE NUMBER SEARCH

Steps are described in the IntelTechniques phone investigation methodology:

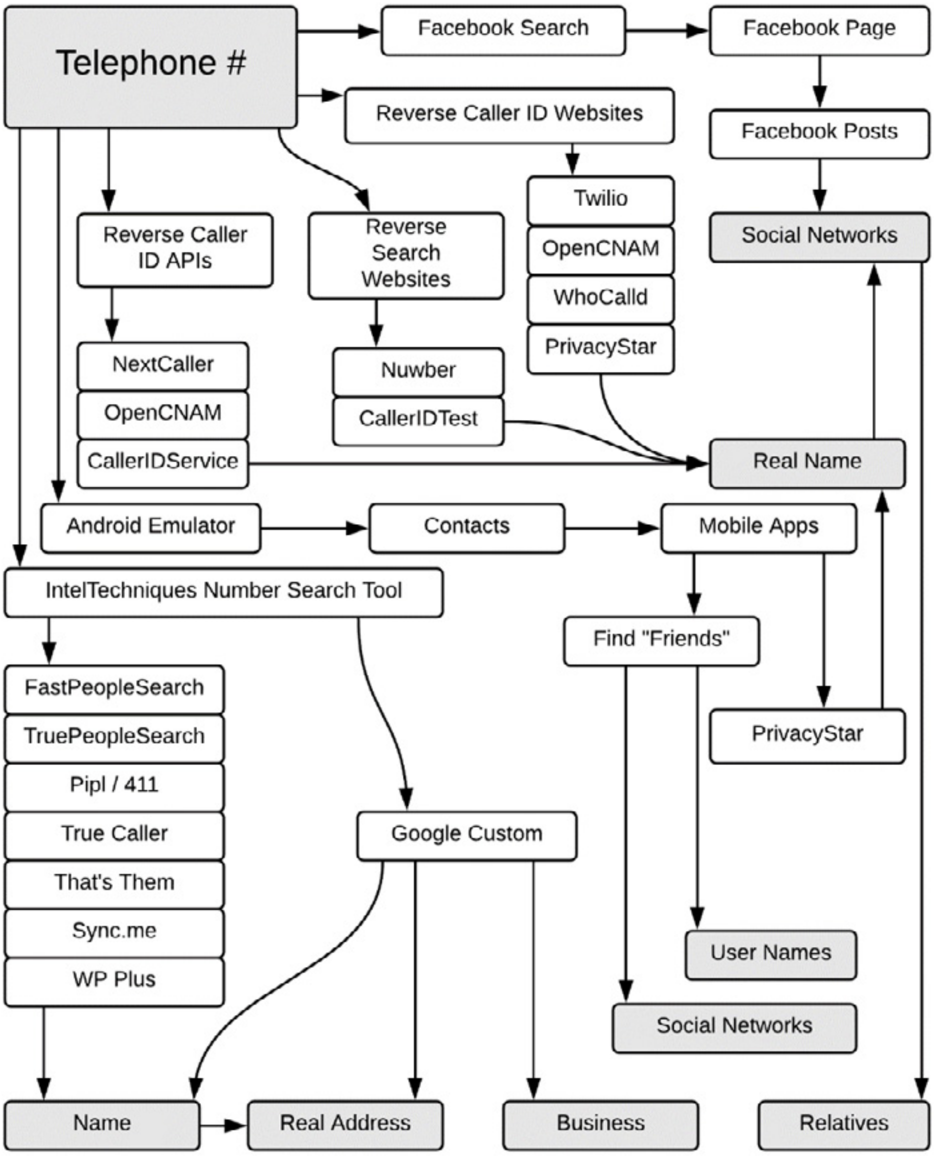
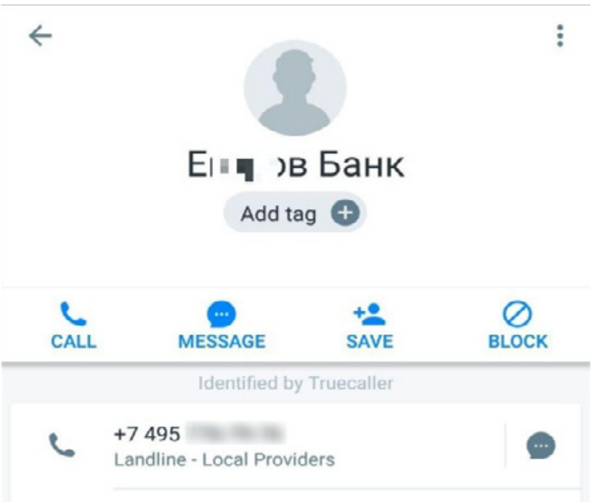


Figure 17: IntelTechniques.com OSINT Workflow Chart: Telephone #

Note:

- When viewing someone's profile on TrueCaller or other platforms, it is recommended to use a separate phone for these kinds of investigations, because the apps can often reveal the identity of whoever viewed the target's public profile.
- Using Facebook Messenger, determine if there is a Facebook account associated with a synced phone number in our contact list. For example, if we obtain the phone number of our target and he does not have his phone number directly connected to his Facebook account, we are still able to determine whether he does, just by adding him to our contacts.
- It is recommended to use social media scrapers for Instagram and Snapchat to find potential leaks, hidden posts, and other data that might be exposed by the target and which was not fully deleted.
- Cross-match information to see if the "hacker" Telegram account is registered on the same number or not.



Е[redacted]ов Банк

Identified by Truecaller

+7 495 [redacted]

Landline - Local Providers

Figure 18: Identifying How the Phone Number Registered

Note:

It is recommended to use different databases like Truecaller, Drupe, TrueCell, CallApp, GetContact, and other alternative resources. These resources allowed us to see how other people had registered this same phone number.

An example of an investigation can be seen on Bellingcat's post: Using phone contact book apps for digital research

NAME ANALYSIS

After identifying a first name and last name based on different sources, these can be combined and it's possible to start investigating different name options - in order to find legitimate accounts of the target.

First Name

The first name, Alex, is likely to be short for Alexander, Sasha, or Alexey. There are other possibilities as well.

This meant that we were looking for someone who potentially had several different first names but the same last name. This expanded our search results but, at the same time, provided more false positives.

Last Name

If it were known that the target was a woman – based on email, first name, or any avatar indicators – the last name would have shifted to: "Ivanov (Ivanova)".

Note: For more information about Russian names, see How Russian Names Work – which provides insights into how names can be changed and used.

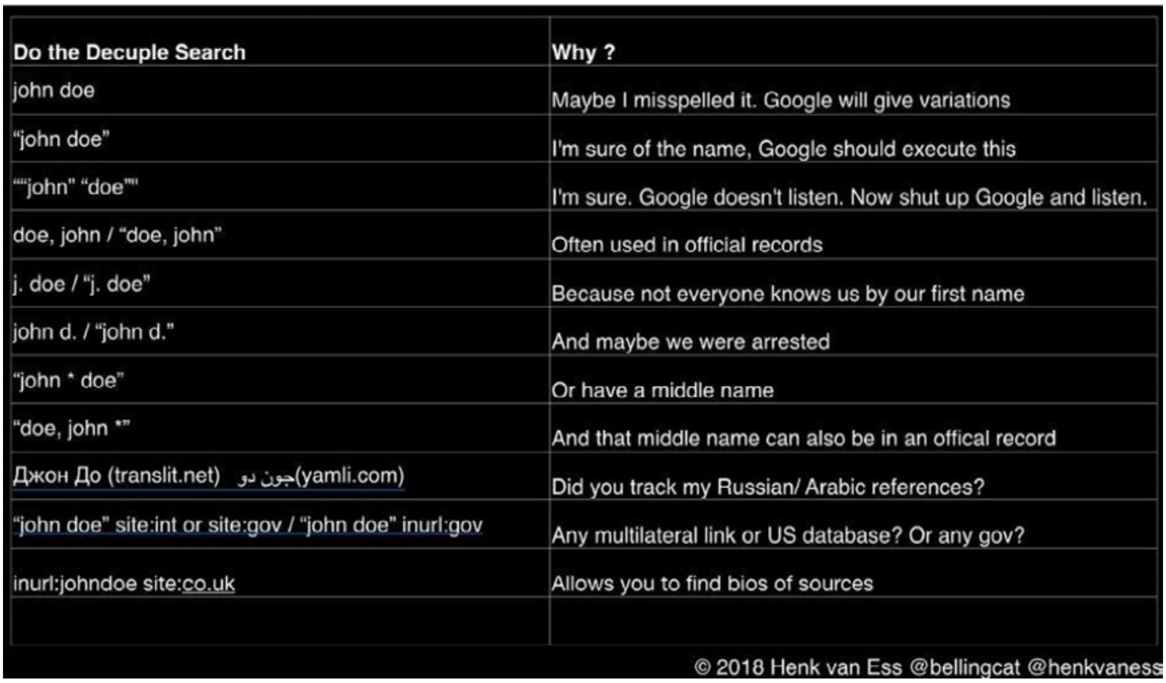
Language

In this scenario – where there is a Russian-speaking target – searches had to include potential name variations in the target's local language. This helped in obtaining additional leads for the investigation.

Language-based searches were mostly useful for finding mentions or associations on forums or "local" social media.

For example: Александр E***ов

See additional references in the Bellingcat blog below:



Do the Decuple Search	Why ?
john doe	Maybe I misspelled it. Google will give variations
"john doe"	I'm sure of the name, Google should execute this
""john" "doe""	I'm sure. Google doesn't listen. Now shut up Google and listen.
doe, john / "doe, john"	Often used in official records
j. doe / "j. doe"	Because not everyone knows us by our first name
john d. / "john d."	And maybe we were arrested
"john * doe"	Or have a middle name
"doe, john *"	And that middle name can also be in an offical record
Джон До (translit.net) جون دو(yamli.com)	Did you track my Russian/ Arabic references?
"john doe" site:int or site:gov / "john doe" inurl:gov	Any multilateral link or US database? Or any gov?
inurl:johndoe site:co.uk	Allows you to find bios of sources

© 2018 Henk van Ess @bellingcat @henkvaness

Figure 19: Potential Name Variations

EMAIL ASSUMPTIONS AND ANALYSIS

After identifying potential first and last names, it's possible to move ahead and generate potential email addresses.
Using the IntelTechniques email investigation methodology, the next step involved generating potential email addresses of our target – based on the first name of the social media account, and the last name of the Truecaller logs.

Once we knew our target's potential first name – gathered from different social media platforms – and what seems like a last name from different phone databases, we could assume that the first and last name were the real identity of our target.

At this point, we generated the target's potential email addresses – with potential variations of the first name and last name – in the format alex.e***ov@gmail.com, and proceeded by investigating the information that could be obtained through the email addresses.

There are several tools that generate email address variations for a given first name, last name, and a domain, such as:

- http://metricsparrow.com/toolkit/email-permutator/
- http://emailpermutator.com/permutator/

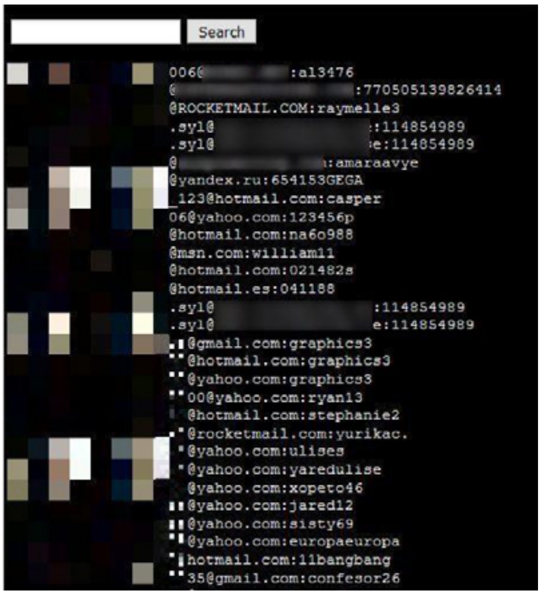
Using the following format for email guessing

Alex.e***ov

The results were as follows:

Results: Email:Pwd

Email	Password
alex.e***ov.4@gmail.com	graphics3
alex.e***ov.6@hotmail.com	graphics3
alex.e***ov.2@yahoo.com	graphics3



```
006@[redacted]:a13476
@[redacted]:770505139826414
@ROCKETMAIL.COM:raymelle3
.syl@[redacted]:114854989
.syl@[redacted]e:114854989
@[redacted]:amaraavye
@yandex.ru:654153GEGA
_123@hotmail.com:casper
06@yahoo.com:123456p
@hotmail.com:na6o988
@msn.com:william11
@hotmail.com:021482s
@hotmail.es:041188
.syl@[redacted]:114854989
.syl@[redacted]e:114854989
@gmail.com:graphics3
@hotmail.com:graphics3
@yahoo.com:graphics3
00@yahoo.com:ryan13
@hotmail.com:stephanie2
@rocketmail.com:yurikac.
@yahoo.com:ulises
@yahoo.com:yaredulise
@yahoo.com:xopeto46
@yahoo.com:jared12
@yahoo.com:sisty69
@yahoo.com:europaeuropa
hotmail.com:11bangbang
35@gmail.com:confesor26
```

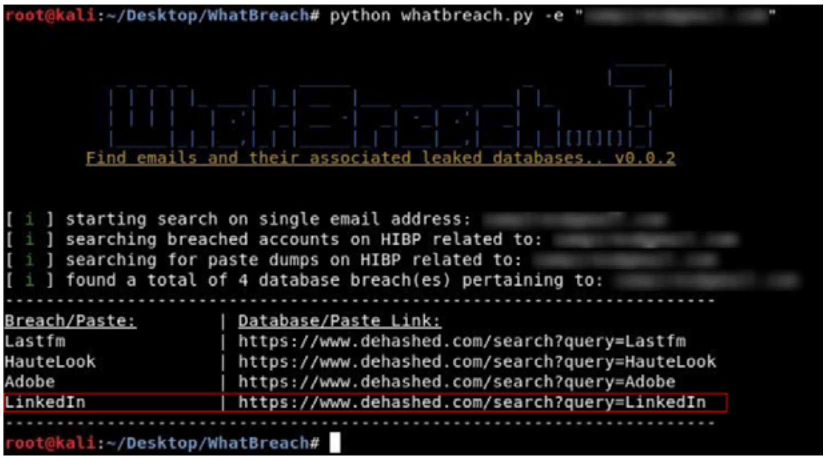
Figure 20: Potential Email Addresses Cross Matching

Because the passwords for these accounts are identical, we were able to conclude that it is highly likely these three email addresses belong to the same person. Based on these assumptions, we needed to verify that these email addresses belonged to our target.

Note:

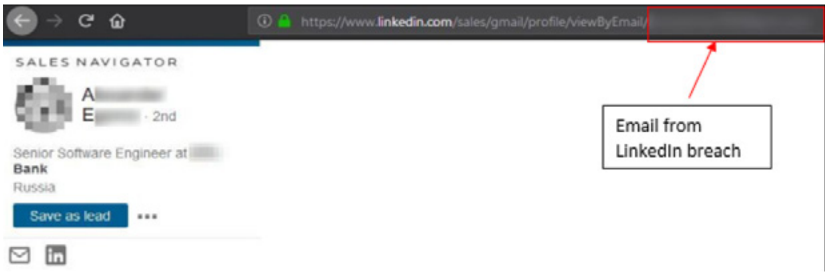
- Consider the possible meanings behind a password: Could it be a phone number? Could it be another username association, or a useful indicator?
- Could the same password be used for accounts that are not compromised?

When conducting our email investigation, we took all obtained email addresses that were found and cross-matched within specific databases where all of the addresses appear. We could see by using "WhatBreach" that one of the email addresses appeared in the famous LinkedIn breach. Therefore, it was reasonable to assume that the same email address is associated with a potential LinkedIn account of our target – or has been in the past.



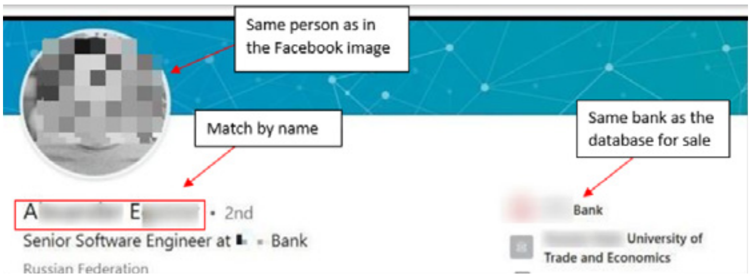
```
root@kali:~/Desktop/WhatBreach# python whatbreach.py -e "[redacted]"

                         WhatBreach..?
         Find emails and their associated leaked databases.. v0.0.2

[ i ] starting search on single email address: [redacted]
[ i ] searching breached accounts on HIBP related to: [redacted]
[ i ] searching for paste dumps on HIBP related to: [redacted]
[ i ] found a total of 4 database breach(es) pertaining to: [redacted]
--------------------------------------------------------------------------
Breach/Paste:          | Database/Paste Link:
Lastfm                 | https://www.dehashed.com/search?query=Lastfm
HauteLook              | https://www.dehashed.com/search?query=HauteLook
Adobe                  | https://www.dehashed.com/search?query=Adobe
LinkedIn               | https://www.dehashed.com/search?query=LinkedIn
--------------------------------------------------------------------------
root@kali:~/Desktop/WhatBreach# ▌
```

Figure 21: Tracking LinkedIn Breached Accounts



https://www.linkedin.com/sales/gmail/profile/viewByEmail/[redacted]
SALES NAVIGATOR
A[redacted]
E[redacted] · 2nd
Senior Software Engineer at [redacted]
Bank
Russia
Save as lead
Email from LinkedIn breach

Figure 22: https://github.com/Ekultek/WhatBreach



Same person as in the Facebook image
Match by name
Same bank as the database for sale
A[redacted] E[redacted] • 2nd
Senior Software Engineer at [redacted] • Bank
Russian Federation
Bank
University of Trade and Economics

Figure 23: LinkedIn Investigations

The email address could be verified using LinkedIn's Sales Navigator, using this format, where "targetmail" is the user's email address: https://www.linkedin.com/sales/gmail/profile/viewByEmail/targetmail@mail.com

This revealed that a registered account was associated with the email address that is part of the LinkedIn breach. The name matched the email name format "Alexander E***ov" who works as a Senior Software Engineer at **** Bank in Russia– the same bank, from which the hacker in the underground forum sold an internal database.

We could also use other tools for scraping profile data from LinkedIn, such as:

- https://github.com/0x09AL/raven – Scrapes the names of all users in a company that are listed on LinkedIn
- https://github.com/initstring/linkedin2username – Generates usernames based on companies on LinkedIn

Additional tactics include finding potential work email addresses in Linkedin profiles. For example, FTL – Find That Lead – a Chrome add-on.

BOTTOM LINE: HACKER'S IDENTITY EXPOSED

The investigation of this example can be summarized as follows:

- Successful connection between the GitHub account of the hacker by Username ->
- Extracted email address from GitHub ->
- Email address connected to an empty Facebook account ->
- Using advanced Facebook search operators, one image was found that had been deleted by the hacker ->
- The same image was found on vk.com, under a different name - >
- The phone number was scraped from the vk.com account ->
- The phone number was researched in different databases ->
- The phone number was found to be registered as "last name + bank"
- This generated potential first name and last name assumptions for email addresses - >
- There were 3 email addresses with the same passwords from compromised databases ->
- One of the email addresses that was part of the LinkedIn databases breach led us to the hacker's real identity ->
- We could see that this hacker works in the same bank, which was the source of the database he was selling on underground hacker forums.

The investigation revealed additional data about the target, including:

- Username variations – one from a forum, and a second one from Telegram
- Groups of activity – i.e., identifying which groups the hacker is part of in Telegram, which was helpful in our external searches of the target's associations with groups
- Language, origin, and country of residence
- Points of interest – hacking, malware, exploits, etc.
- Private email addresses and potential work email addresses to be generated based on the email format used in the company
- Password of email addresses
- Database breaches that the target's email was in – indicative of other platforms that the target is part of
- Professional profile on LinkedIn – with connections, shares, posts, etc.
- Social platforms with images of the target

HOW OSINT IS CHANGING

OSINT is fundamental to this type of investigation flow. Yet, there may be shifts in the kind of information available online, due to issues such as statutory regulation of some OSINT-related capabilities, including the regulation of professional ethics for private-sector companies working in OSINT, the widening of definitions of sensitive information, and more. Changes include:

- Decreased commitment to freedom of information, with the trend toward populist and semi-authoritarian regimes reflected, for example, in decreased commitment to government transparency.
- Better InfoSec, with the widespread adoption of end-to-end encryption in all commonly used social media and messenger applications, and increasingly decentralized, private online chat environments.

One example of how OSINT is changing is the recent changes to Facebook Graph Search. The loss of this tool has an impact on how investigations are run online.

SIGNIFICANCE OF OSINT IN VIRTUAL-HUMINT METHODOLOGIES & TECHNIQUES

In this investigation flow, the use of OSINT methodologies and techniques allowed us to gather enough data to engage with the hacker or threat actor and extract additional data – perhaps about the database itself, for example.

The tools and techniques presented in this investigation flow are unique to this case, and the methodology is different for each target and for each investigation.

What is common to all of the investigation flows used is that by leveraging Virtual-HUMINT, OSINT analysts are able to glean information online that is crucial to protecting organizations – allowing cybersecurity professionals to more effectively combat cyberattacks and threats.

ABOUT CYBERPROOF

CyberProof aims to give clarity and confidence to businesses worldwide with a new approach to running and operating security operations centers. CyberProof is part of UST Global, serving some of the world's largest enterprises with their digital transformations.

As trusted partners throughout the entire cyber journey, we promise companies around the world operational efficiency with complete transparency.

For further information, visit www.cyberproof.com.

LOCATIONS

Aliso Viejo | London | Singapore | Tel Aviv | Trivandrum