OPEN-SOURCE INTELLIGENCE
Summit & Training

SANS Summits

Leveraging VIPs' Attack Surface Through OSINT

Ygor Maximo (@mxm0z)

PenTest magazine

OSINT ON PENTEST TARGETS

OSINT for Pentesting

Utilizing OSINT Tooling for Penetration Testing

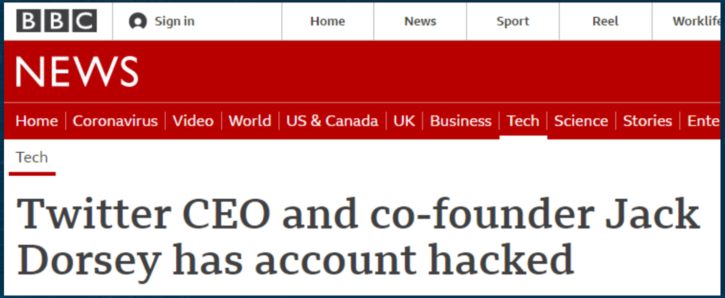
Leveraging Open-Source Intelligence in Proactive Cyber Defence

Leveraging VIPs Attack Surface Through OSINT

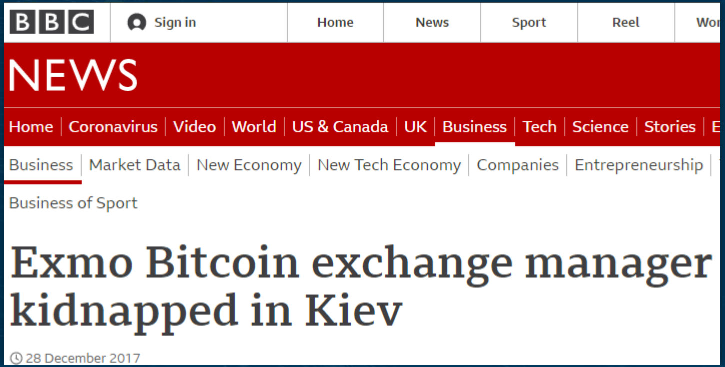
08/2020 ISSN: 2084-1117

- Originally published on PenTest Magazine
- 08/2020 Edition

Before we start...


BBC
Sign in
Home
News
Sport
Reel
Worklife
NEWS
Home | Coronavirus | Video | World | US & Canada | UK | Business | Tech | Science | Stories | Ente
Tech

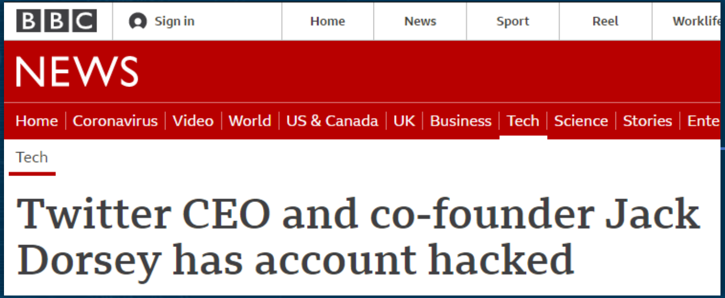
Twitter CEO and co-founder Jack Dorsey has account hacked


BBC
Sign in
Home
News
Sport
Reel
Wor
NEWS
Home | Coronavirus | Video | World | US & Canada | UK | Business | Tech | Science | Stories | E
Business | Market Data | New Economy | New Tech Economy | Companies | Entrepreneurship |
Business of Sport

Exmo Bitcoin exchange manager kidnapped in Kiev

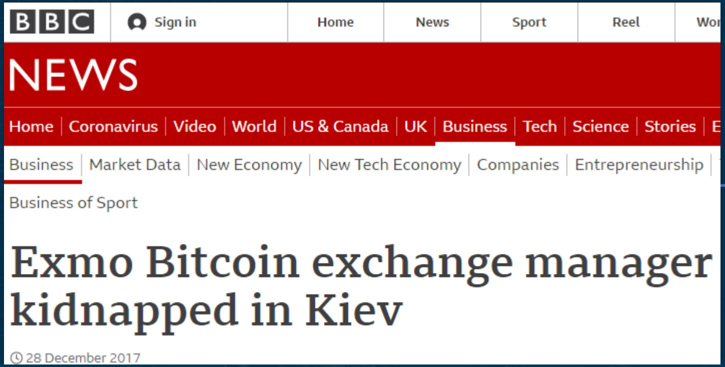
28 December 2017

Before we start...



Twitter CEO and co-founder Jack Dorsey has account hacked

SIM Swapping

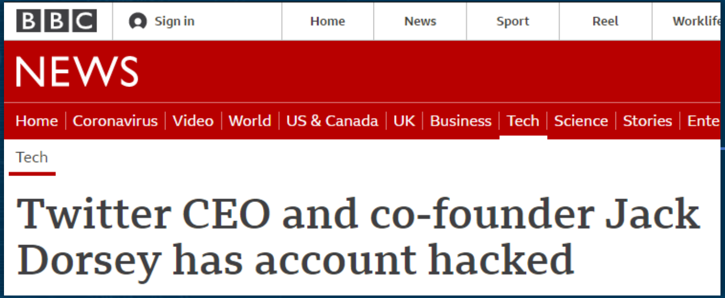


Exmo Bitcoin exchange manager kidnapped in Kiev

28 December 2017

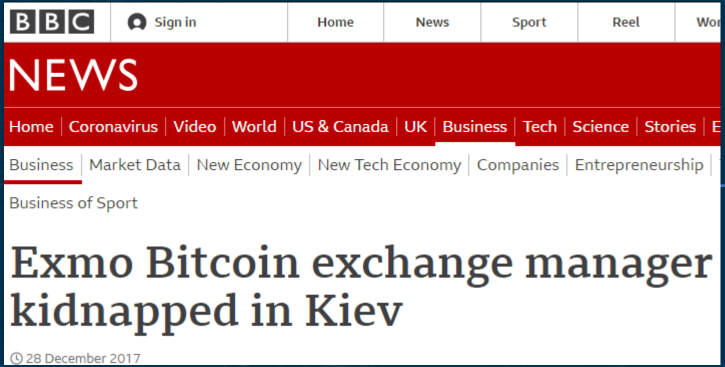
Leaked travel plans

Before we start...


BBC
Sign in
Home
News
Sport
Reel
Worklife
NEWS
Home | Coronavirus | Video | World | US & Canada | UK | Business | Tech | Science | Stories | Ente
Tech

Twitter CEO and co-founder Jack Dorsey has account hacked

→ SIM Swapping


BBC
Sign in
Home
News
Sport
Reel
Wor
NEWS
Home | Coronavirus | Video | World | US & Canada | UK | Business | Tech | Science | Stories | E
Business | Market Data | New Economy | New Tech Economy | Companies | Entrepreneurship
Business of Sport

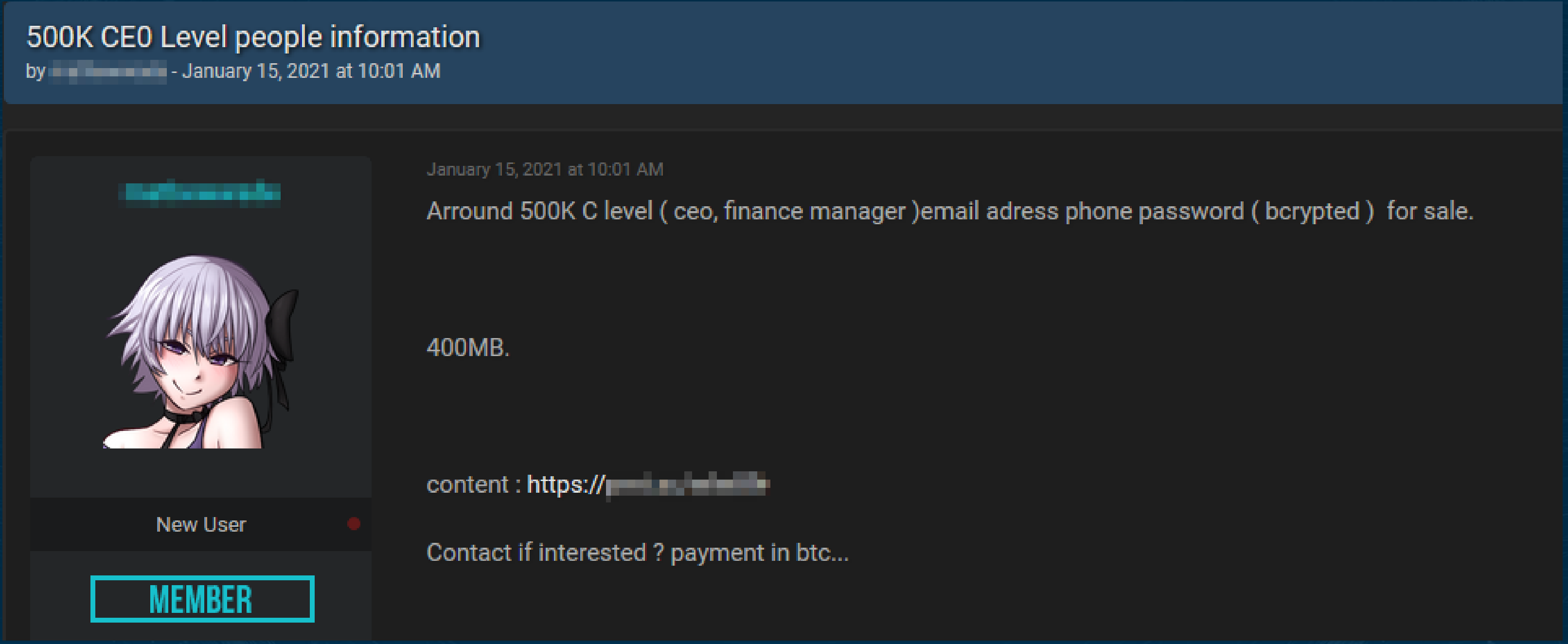
Exmo Bitcoin exchange manager kidnapped in Kiev

28 December 2017

→ Leaked travel plans

} Exposed/Leaked Personal Identifiable Information

Example from Dark Web forum



500K CEO Level people information

by [redacted] - January 15, 2021 at 10:01 AM

[redacted]

January 15, 2021 at 10:01 AM

Arround 500K C level (ceo, finance manager)email adress phone password (bcrypted) for sale.

400MB.

content : https://[redacted]

Contact if interested ? payment in btc...

About me

Ygor Maximo (@mxm0z)

Threat & Dark Web Intelligence at iSecurity Inc.

OSINT Investigator

Certified Threat Intelligence Analyst (EC-Council)

Agenda

1. Introduction
2. Methodology of Collection and Analysis
3. Collecting VIPs data through OSINT
4. Tools and Techniques
5. Conclusion

Introduction

VIPs: Who Are They? What They Do? How They Live? What They Eat?

Introduction

VIPs: Who Are They? What They Do? How They Live? What They Eat?

C-Level, Partners, Managers

Introduction

VIPs: Who Are They? What They Do? How They Live? What They Eat?

C-Level, Partners, Managers

Board of Directors

Introduction

VIPs: Who Are They? What They Do? How They Live? What They Eat?

C-Level, Partners, Managers

Board of Directors

Basically the decision making people..

Introduction

VIPs: Who Are They? What They Do? How They Live? What Do They Eat?

C-Level, Partners, Managers

Board of Directors

Aren't we forgetting someone?

Introduction

VIPs: Who Are They? What They Do? How They Live? What They Eat?

C-Level, Partners, Managers

Board of Directors

NETWORK ADMIN
We may be strange, but we know what you surf for during lunch.

Methodology of Collection and Analysis

Some key questions

- What is the purpose of your investigation?
- What are you trying to accomplish?
- What questions do you/your customer want answered?

Methodology of Collection and Analysis

What data can be collected?

- Name
- Picture
- Description
- Email Address
- Telephone Number
- VIP Assistant Contact Details

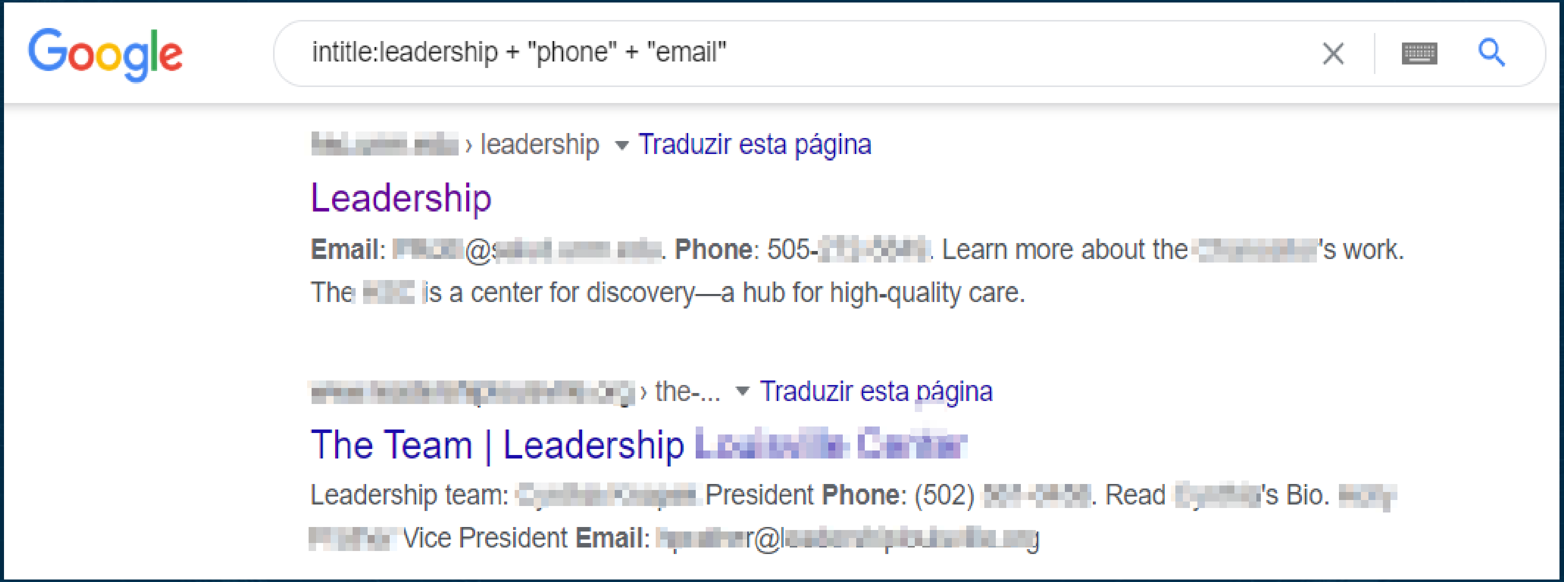
Tips for efficient data collection phase

- Answer key questions (requirements)
- Follow a well-defined process/framework
- MindMaps (i.e. XMind.net)

The amount of data is directly proportional to the chance of you getting lost if you decide to not follow a process

Collecting VIPs’ data through OSINT

Common Web Pages Displaying Contact Details of VIPs



intitle:leadership + "phone" + "email"

[redacted] › leadership ▾ Traduzir esta página

Leadership

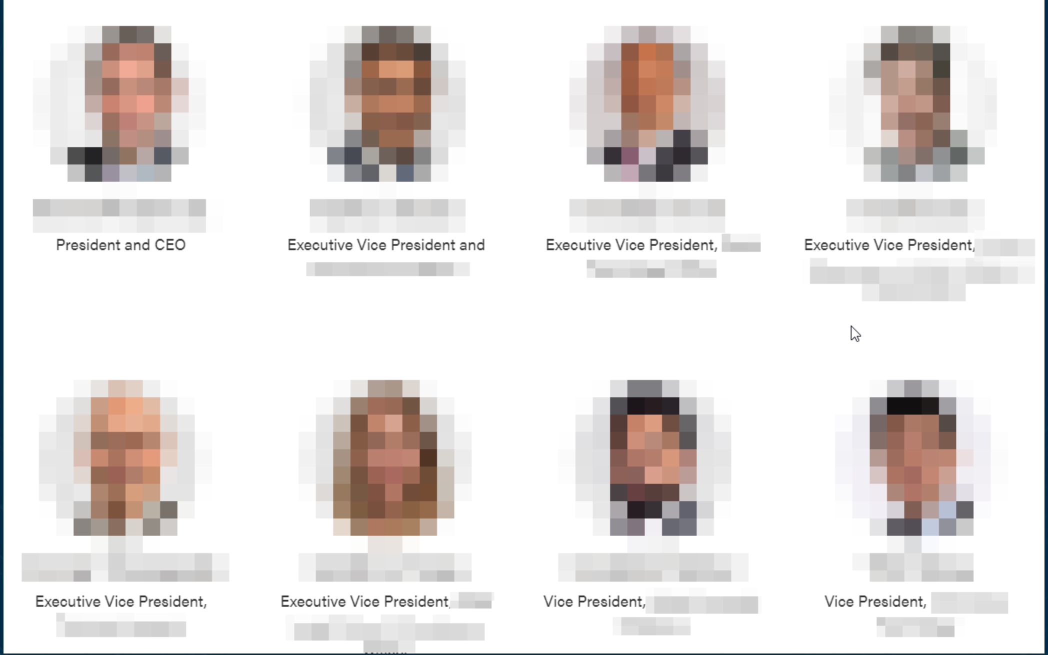
Email: [redacted]@[redacted]. **Phone**: 505-[redacted]. Learn more about the [redacted]'s work. The [redacted] is a center for discovery—a hub for high-quality care.

[redacted] › the-... ▾ Traduzir esta página

The Team | Leadership [redacted]

Leadership team: [redacted] President **Phone**: (502) [redacted]. Read [redacted]'s Bio. [redacted] Vice President **Email**: [redacted]r@[redacted]

Collecting VIPs' data through OSINT



President and CEO

Executive Vice President and

Executive Vice President,

Executive Vice President,

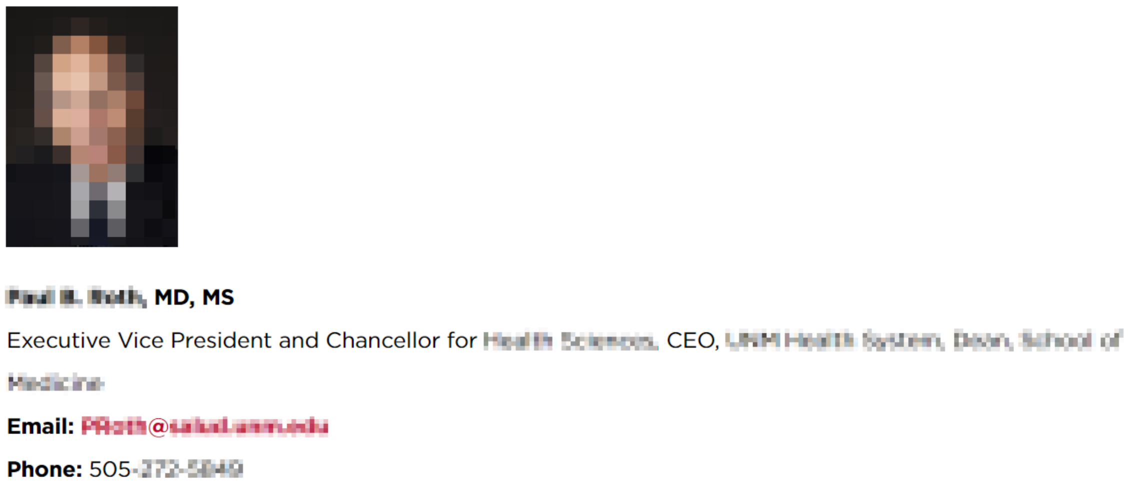
Executive Vice President,

Executive Vice President,

Vice President,

Vice President,

Collecting VIPs’ data through OSINT



[redacted], MD, MS

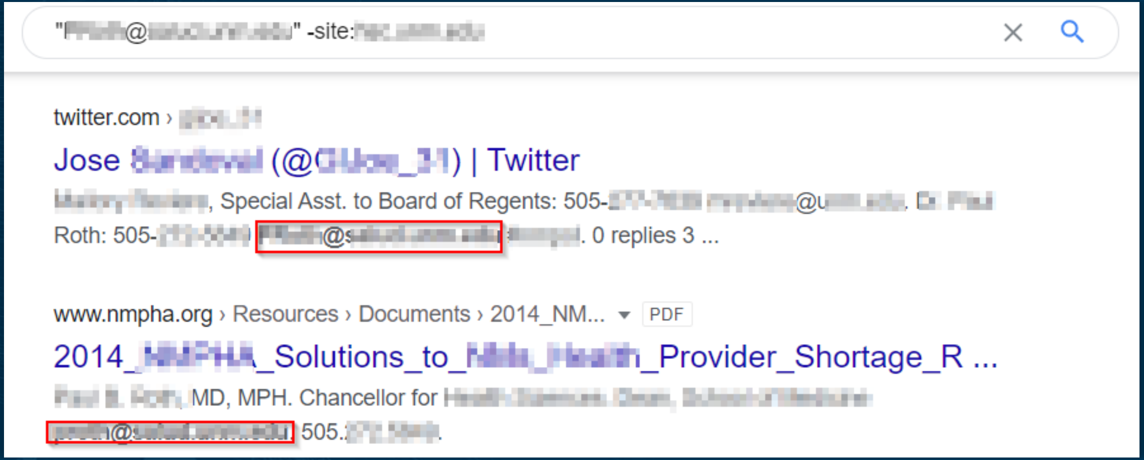
Executive Vice President and Chancellor for [redacted], CEO, [redacted]

Email: [redacted]

Phone: 505-[redacted]

Collecting VIPs' data through OSINT

Finding Personal Social Media of VIPs



"[redacted]@[redacted]" -site:[redacted]

twitter.com › [redacted]

Jose [redacted] (@[redacted]) | Twitter

[redacted], Special Asst. to Board of Regents: 505-[redacted] [redacted]@u[redacted]. [redacted]
Roth: 505-[redacted] [redacted] [redacted]. 0 replies 3 ...

www.nmpha.org › Resources › Documents › 2014_NM... ▾ PDF

2014_[redacted]_Solutions_to_[redacted]_Provider_Shortage_R ...

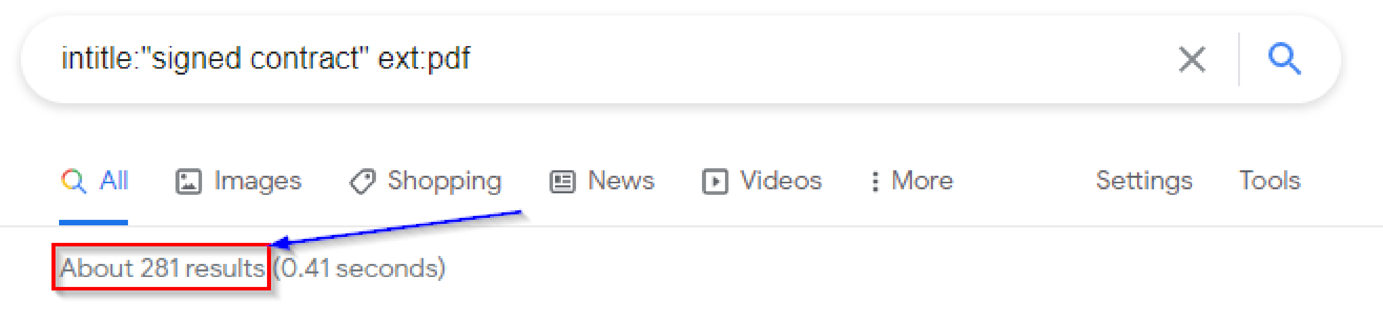
[redacted] MD, MPH. Chancellor for [redacted]
[redacted] 505.[redacted].

VIPs social media can be used on:

- Social Engineering
- Collect Unintentionally Published Personal Information
- Any Additional and Useful Info

Collecting VIPs’ data through OSINT

Signed Contracts Indexed on Google Exposing VIPs Signatures



intitle:"signed contract" ext:pdf

About 281 results (0.41 seconds)

VIPs contract signatures can be used to:

- Increase level of legitimicy of phishing emails
- Documeny forgery for Cyber Attacks
- Executive Impersonation

Tools and Techniques

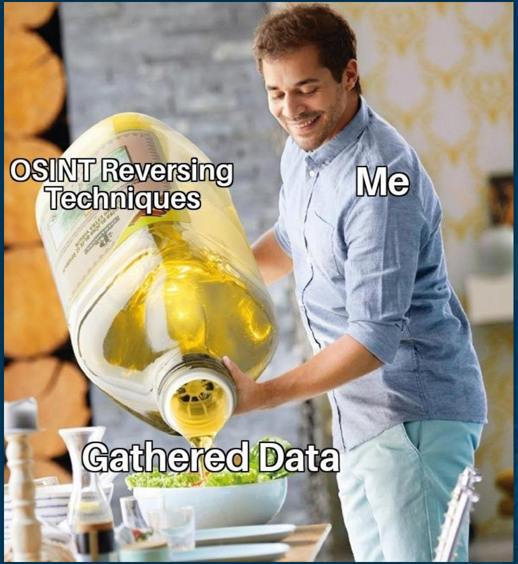
How To Leverage The Collected Data

- Name
- Picture
- Description
- Email Address
- Telephone Number
- VIP Assistant Contact Details

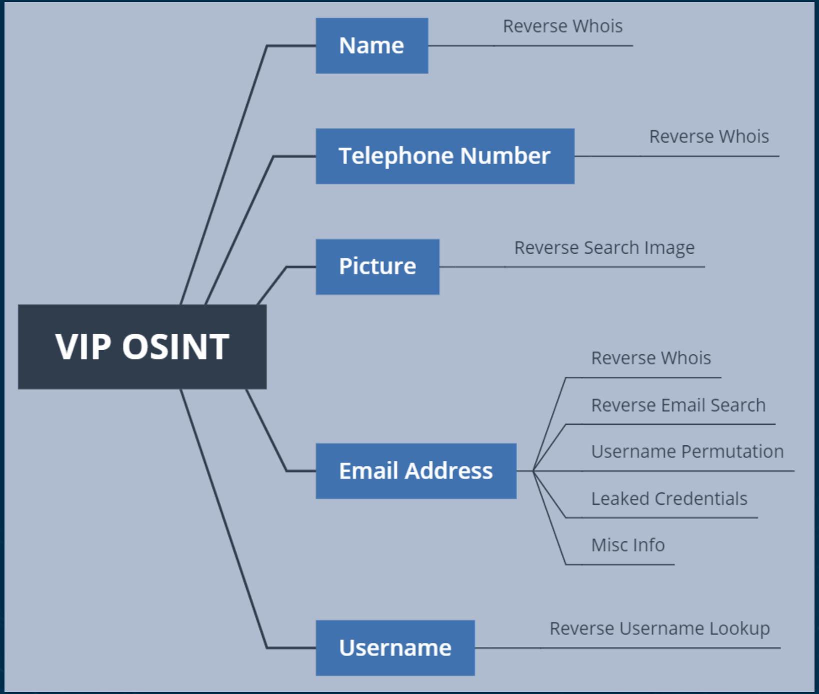
Tools and Techniques

Let’s Reverse Things... OSINT Style

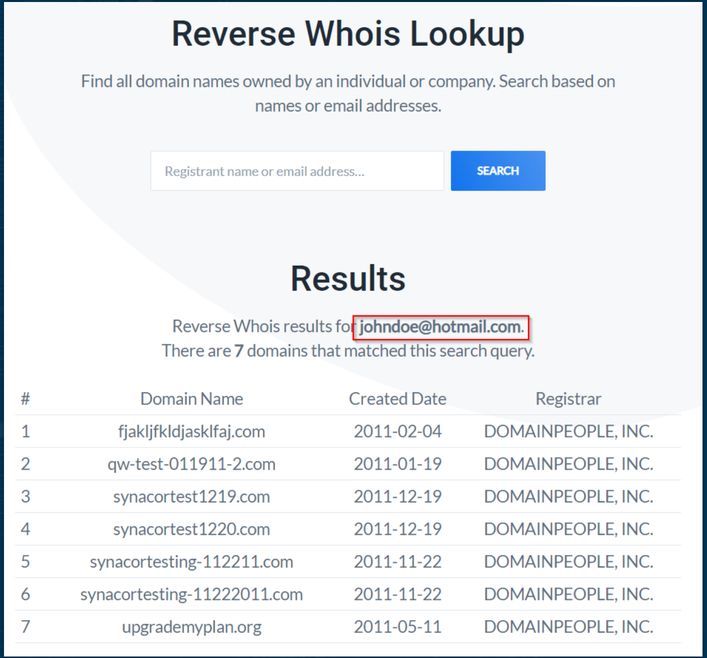
- Reverse Whois Search
- Reverse Image Search
- Reverse Username Lookup
- Reverse Email Search
- Username Permutation



Tools and Techniques



Tools and Techniques



Reverse Whois Lookup

Find all domain names owned by an individual or company. Search based on names or email addresses.

Results

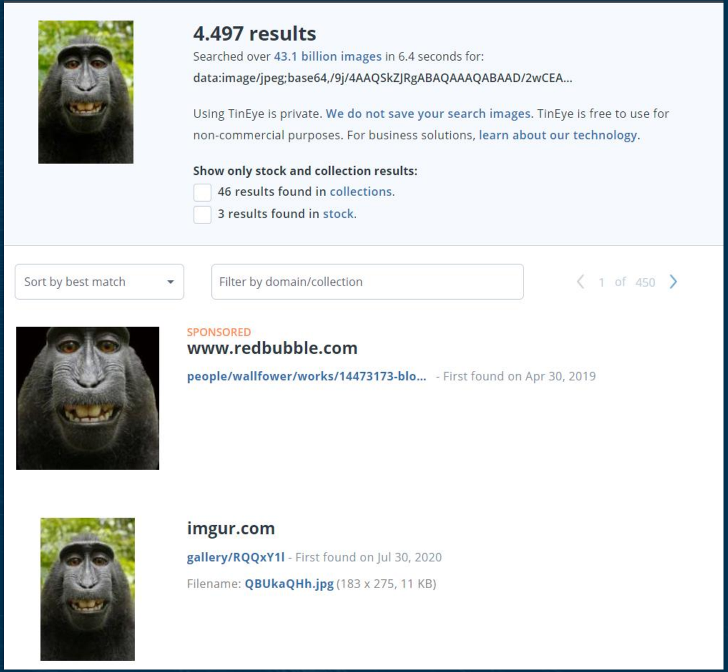
Reverse Whois results for johndoe@hotmail.com.
There are **7** domains that matched this search query.

#	Domain Name	Created Date	Registrar
1	fjakljfkldjasklfaj.com	2011-02-04	DOMAINPEOPLE, INC.
2	qw-test-011911-2.com	2011-01-19	DOMAINPEOPLE, INC.
3	synacortest1219.com	2011-12-19	DOMAINPEOPLE, INC.
4	synacortest1220.com	2011-12-19	DOMAINPEOPLE, INC.
5	synacortesting-112211.com	2011-11-22	DOMAINPEOPLE, INC.
6	synacortesting-11222011.com	2011-11-22	DOMAINPEOPLE, INC.
7	upgrademyplan.org	2011-05-11	DOMAINPEOPLE, INC.

ReverseWhois.io – Reverse Whois Lookup

- **Find domain names tied to the targeted VIP**
- **Potentially new email adresses**
- **New vulnerable web application**
- **Personal blogs revealing useful info**

Tools and Techniques



4.497 results

Searched over 43.1 billion images in 6.4 seconds for:

data:image/jpeg;base64,/9j/4AAQSkZJRgABAQAAAQABAAD/2wCEA...

Using TinEye is private. We do not save your search images. TinEye is free to use for non-commercial purposes. For business solutions, learn about our technology.

Show only stock and collection results:

□ 46 results found in collections.

□ 3 results found in stock.

Sort by best match

Filter by domain/collection

1 of 450

SPONSORED

www.redbubble.com

people/wallfower/works/14473173-blo... - First found on Apr 30, 2019

imgur.com

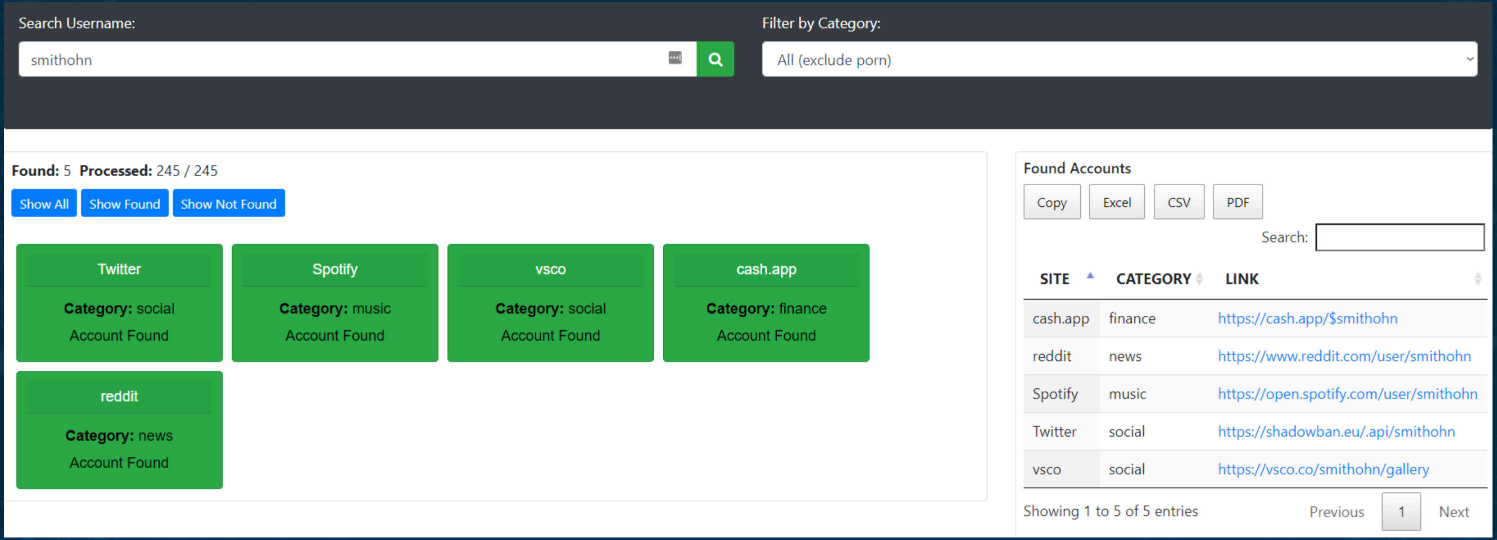
gallery/RQQxY1l - First found on Jul 30, 2020

Filename: QBUkaQHh.jpg (183 x 275, 11 KB)

TinEye – Reverse Image Search

- Find third-party sources where the same picture is hosted
- Find Picture being published by someone close to the target

Tools and Techniques



Search Username: smithohn

Filter by Category: All (exclude porn)

Found: 5 **Processed:** 245 / 245

Twitter
Category: social
Account Found

Spotify
Category: music
Account Found

vsco
Category: social
Account Found

cash.app
Category: finance
Account Found

reddit
Category: news
Account Found

Found Accounts

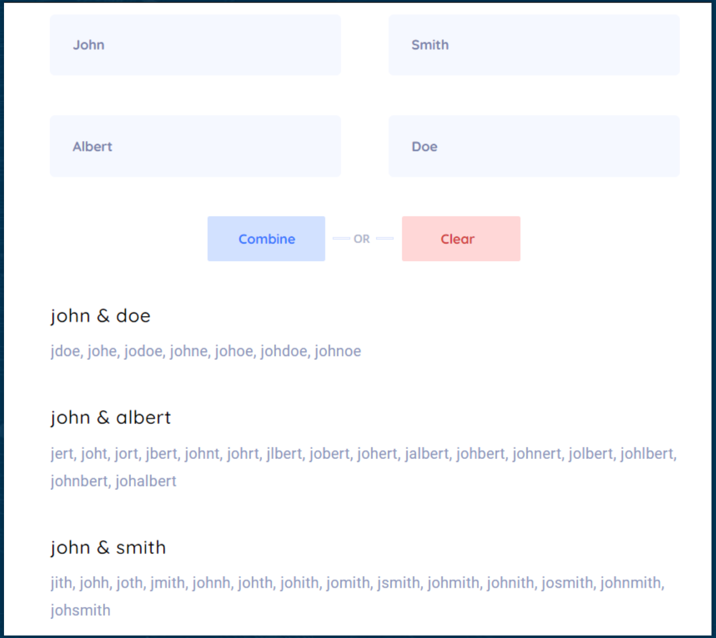
SITE	CATEGORY	LINK
cash.app	finance	https://cash.app/$smithohn
reddit	news	https://www.reddit.com/user/smithohn
Spotify	music	https://open.spotify.com/user/smithohn
Twitter	social	https://shadowban.eu/.api/smithohn
vsco	social	https://vsco.co/smithohn/gallery

Showing 1 to 5 of 5 entries

WhatsMyName.app

- Username as the searched item

Tools and Techniques



John

Smith

Albert

Doe

john & doe

jdoe, johe, jodoe, johne, johoe, johdoe, johnoe

john & albert

jert, joht, jort, jbert, johnt, johrt, jlbert, jobert, johert, jalbert, johbert, johnert, jolbert, johlbert, johnbert, johalbert

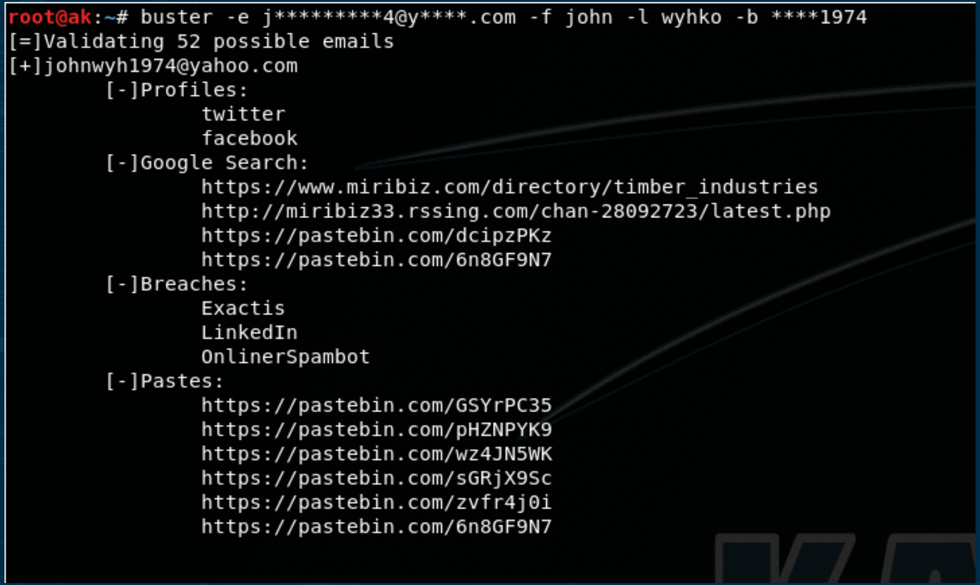
john & smith

jith, johh, joth, jmith, johnh, johth, johith, jomith, jsmith, johmith, johnith, josmith, johnmith, johsmith

NameCombiner.com – Username Permutation

- Generate usernames based on VIPs name
- Several email addresses combinations

Tools and Techniques



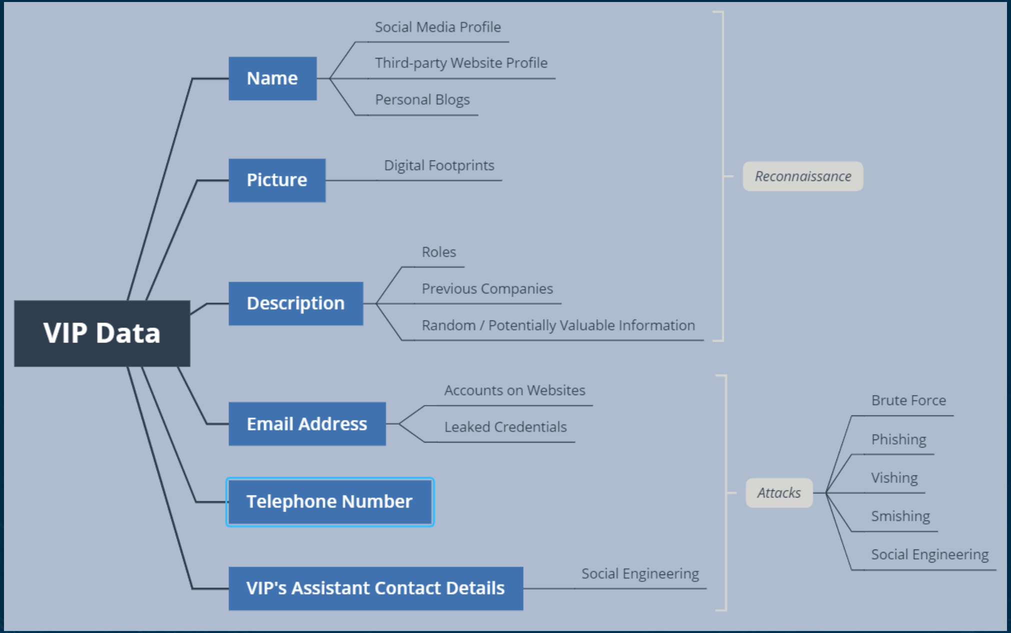
```
root@ak:~# buster -e j*********4@y****.com -f john -l wyhko -b ****1974
[=]Validating 52 possible emails
[+]johnwyh1974@yahoo.com
        [-]Profiles:
                twitter
                facebook
        [-]Google Search:
                https://www.miribiz.com/directory/timber_industries
                http://miribiz33.rssing.com/chan-28092723/latest.php
                https://pastebin.com/dcipzPKz
                https://pastebin.com/6n8GF9N7
        [-]Breaches:
                Exactis
                LinkedIn
                OnlinerSpambot
        [-]Pastes:
                https://pastebin.com/GSYrPC35
                https://pastebin.com/pHZNPYK9
                https://pastebin.com/wz4JN5WK
                https://pastebin.com/sGRjX9Sc
                https://pastebin.com/zvfr4j0i
                https://pastebin.com/6n8GF9N7
```

Buster (GitHub)

- Perform Google searches
- Breached databases
- Pastes on Pastebin
- Email address as the search

Tools and Techniques

How To Leverage The Collected Data



Conclusion

What we have covered and learned in this talk:

- Executive digital exposure could lead to physical risks
- VIPs are not just C-Level / Executives / Directors
- Tools and Techniques to leverage VIP data through offensive OSINT
- Non-technical flaws can also lead to a company breach

Links and References

- https://www.bbc.com/news/business-42505261
- https://www.bbc.com/news/technology-49532244
- https://xmind.net
- https://pastebeen.com
- https://namecombiner.com
- https://reversewhois.io
- https://whatsmyname.app
- https://tineye.com
- https://osintframework.com
- https://github.com/harleo/knockknock

Thanks!
Questions?

Twitter: @mxm0z

LinkedIn: /in/ygormaximo

GitHub: /mxm0z

E: ygormaximo@pm.me