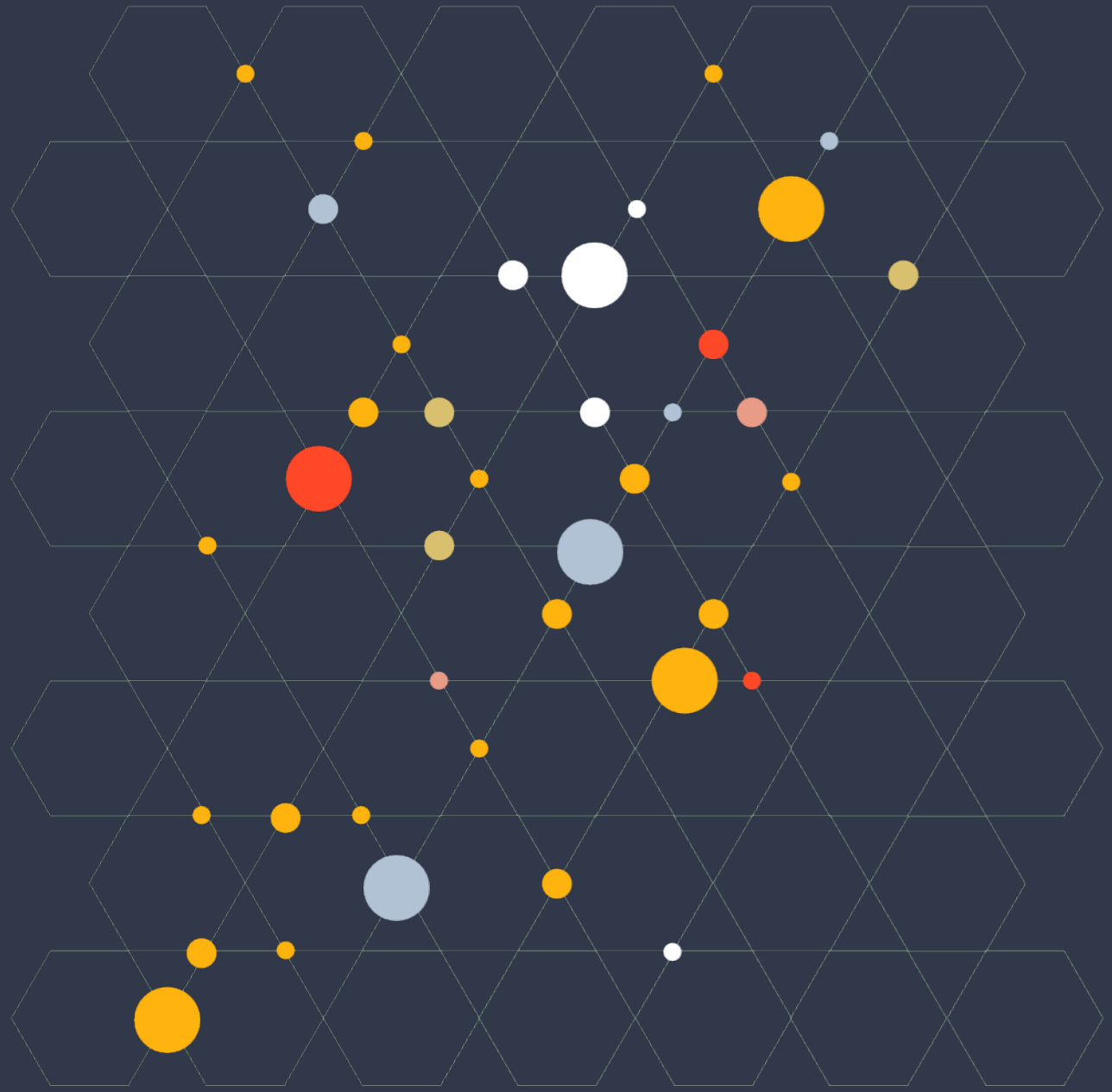
Carlos Fragoso & Mathieu Gaucheler

Barcelona Cybersecurity Congress



MALTEGO

Who am I?

Mathieu Gaucheler
Subject Matter Expert

mg@maltego.com

Location: Barcelona

Position: Subject Matter Expert at Maltego

Experience and Career:

I spent two years working in a cyber threat intelligence in a Barcelona startup. I then joined Maltego in March 2021, focusing first on cybersecurity then exploring other fields such as disinformation, SOCMINT and geolocation.

Who am I?

Carlos Fragoso
Subject Matter Expert

cf@maltego.com

Location: Barcelona

Passionate about investigations & OSINT

22 years working in Information Security :

- **Network & Operations Manager (7y)**
  High Performance Computing (HPC) & Network/IXP Backbone infrastructure
- **SOC/CSIRT/CTI Manager (5y)**
  Cybersecurity & Government Agencies
- **CTO & Incident Response & Investigation Lead (9y)**
  Managed Response & Forensics Service Provider
- **Public Speaker**

FIRST and APWG Communities Liaison
SANS Institute Instructor (SEC401, SEC504)

SOCMINT

Dmitry YURIEVICH a.k.a. "LOCKBITSUPP"

Getting information the Office of Foreign Assets Control (OFAC)

PRESS RELEASES

United States Sanctions Senior Leader of the LockBit Ransomware Group

May 7, 2024

The United States reveals the identity of and imposes sanctions on Dmitry Khoroshev, a senior leader of the LockBit ransomware group

Starting from the Office of Foreign Assets Control (OFAC)

PRESS RELEA

United S
of the Lo

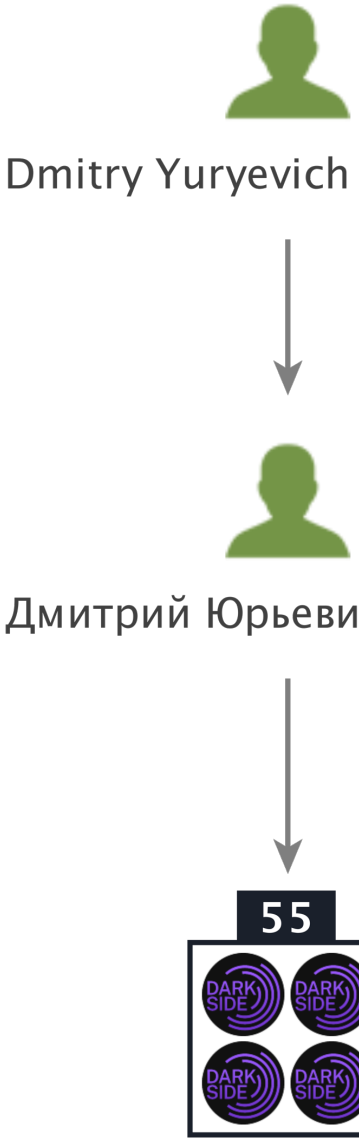
May 7, 2024

The United States re

The following individual has been added to OFAC's SDN List:

KHOROSHEV, Dmitry Yuryevich (a.k.a. KHOROSHEV, Dmitrii Yuryevich; a.k.a. KHOROSHEV, Dmitriy Yurevich; a.k.a. YURIEVICH, Dmitry; a.k.a. "LOCKBITSUPP"), Russia; DOB 17 Apr 1993; POB Russian Federation; nationality Russia; citizen Russia; Email Address khoroshev1@icloud.com; alt. Email Address sitedev5@yandex.ru; Gender Male; Digital Currency Address - XBT bc1qvhnfknw852ephxyc5hm4q520zmvf9maphetc9z; Secondary sanctions risk: Ukraine-/Russia-Related Sanctions Regulations, 31 CFR 589.201; Passport 2018278055 (Russia); alt. Passport 2006801524 (Russia); Tax ID No. 366110340670 (Russia) (individual) [CYBER2].

Let’s search his name in breach data



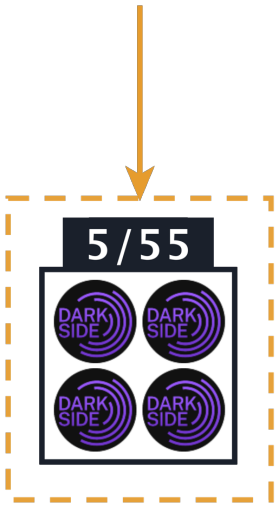
No results when using the **Latin transliteration** of his name. We need to use **Cyrillic**.

How are we going to find the relevant breaches and **avoid homonyms**?

Let’s search his name in breach data

Dmitry Yuryevich Khoroshev

Дмитрий Юрьевич Хорошев

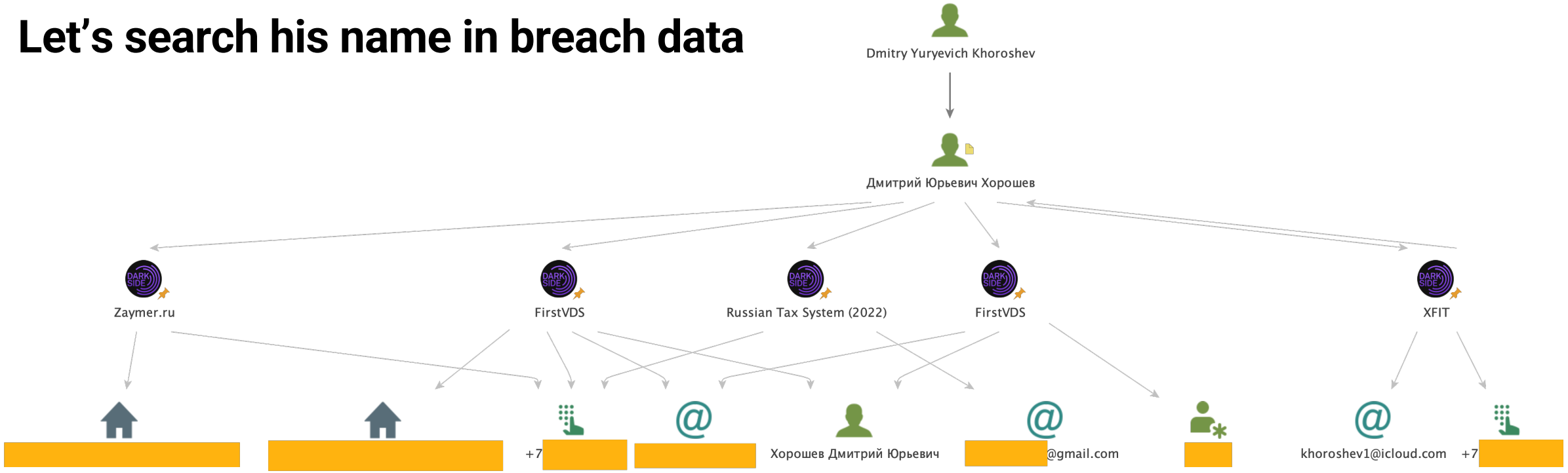


No results when using the **Latin transliteration** of his name. We need to use **Cyrillic**.

How are we going to find the relevant records and **avoid homonyms**?

Search for matching date of birth!

Let’s search his name in breach data



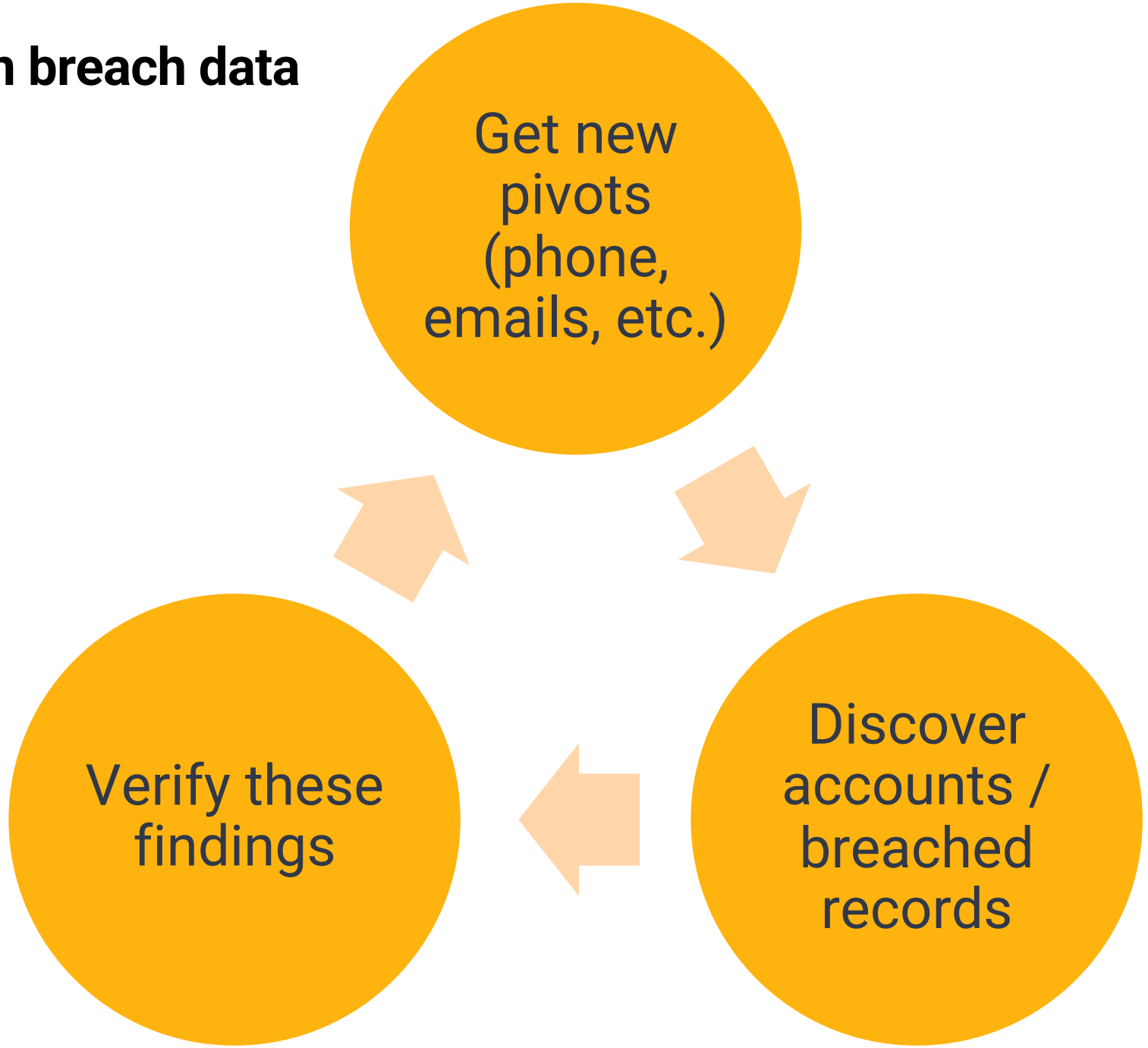
In one search:

- 2 addresses
- 2 new email addresses
- 2 phone number
- 1 alias

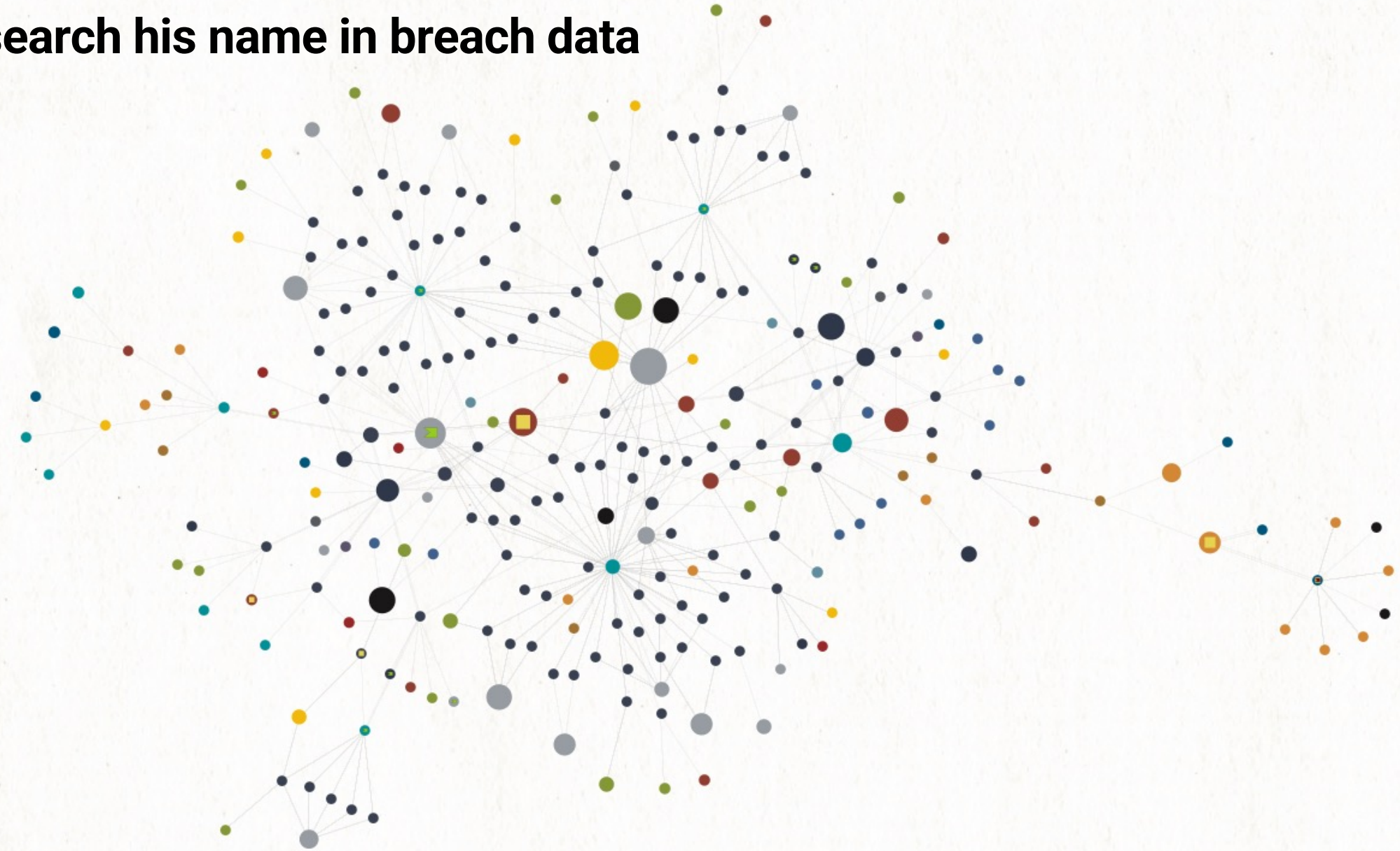
These are both **information that we seeked** and **new pivots** for our investigation

Let’s search his name in breach data

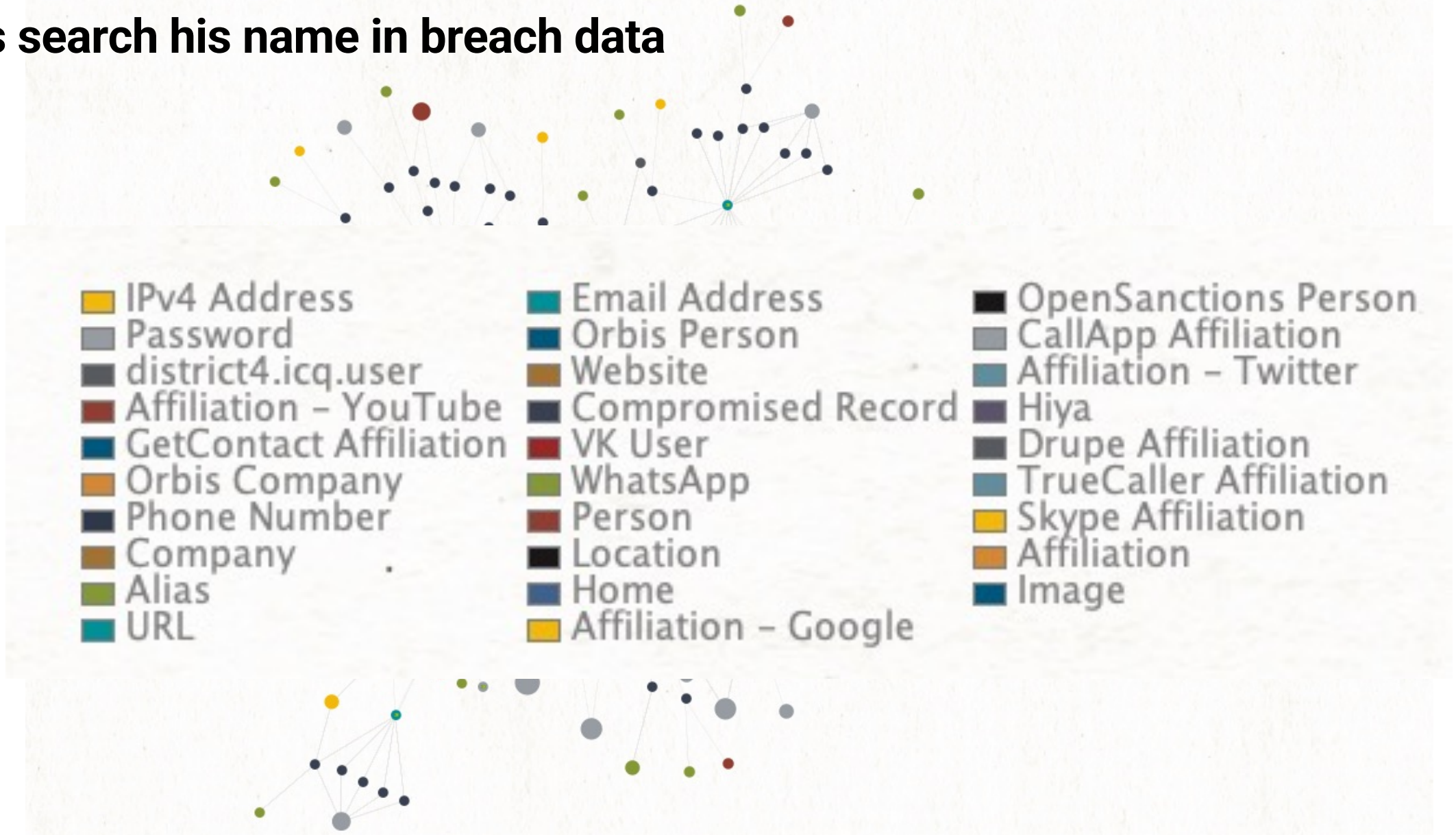
After 2 cycles of this process we end up with the following graph.

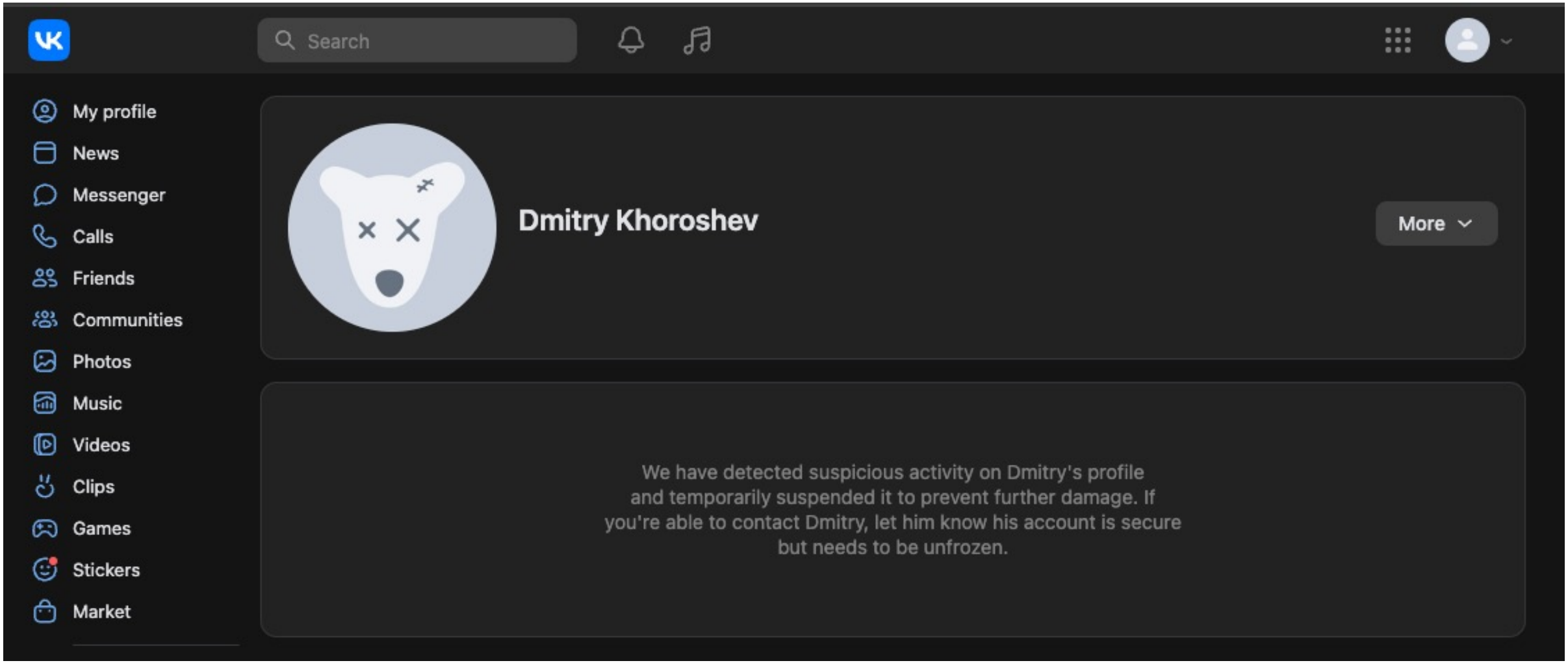


Let’s search his name in breach data



Let’s search his name in breach data

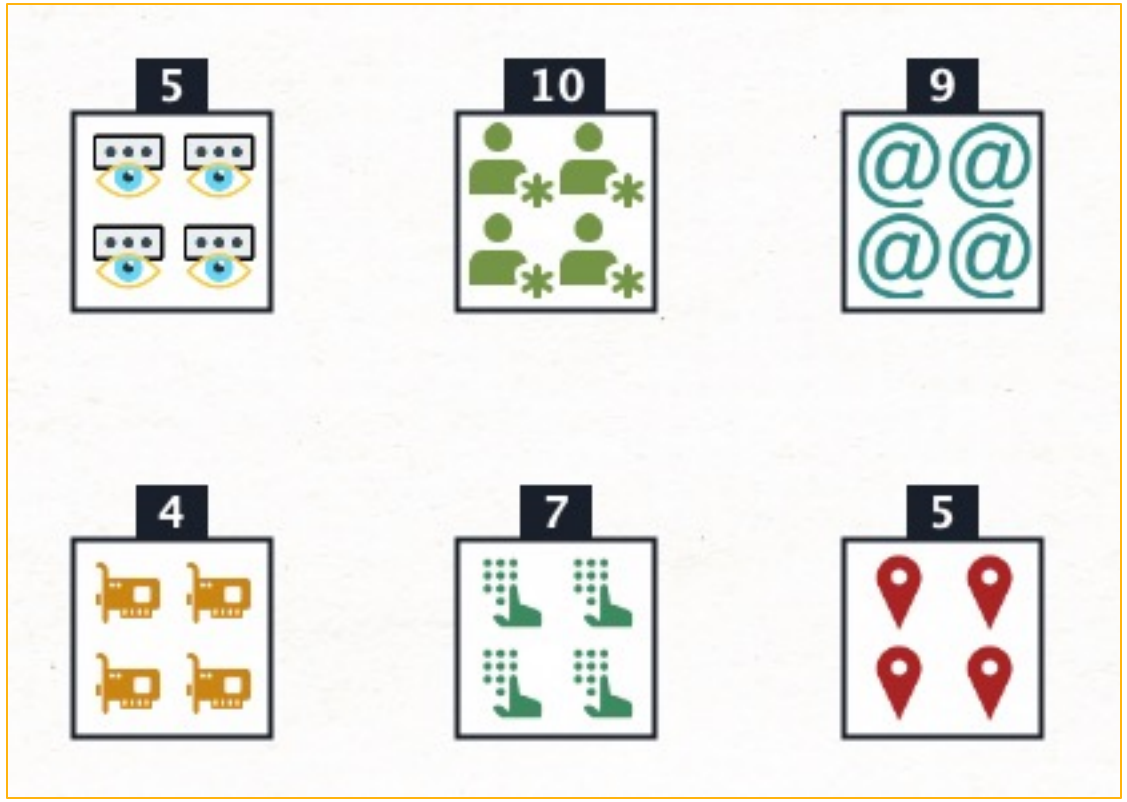



Search
My profile
News
Messenger
Calls
Friends
Communities
Photos
Music
Videos
Clips
Games
Stickers
Market
Dmitry Khoroshev
More
We have detected suspicious activity on Dmitry's profile and temporarily suspended it to prevent further damage. If you're able to contact Dmitry, let him know his account is secure but needs to be unfrozen.

What did we find in the end?

Aliases

Clear text password



Email addresses

IP addresses

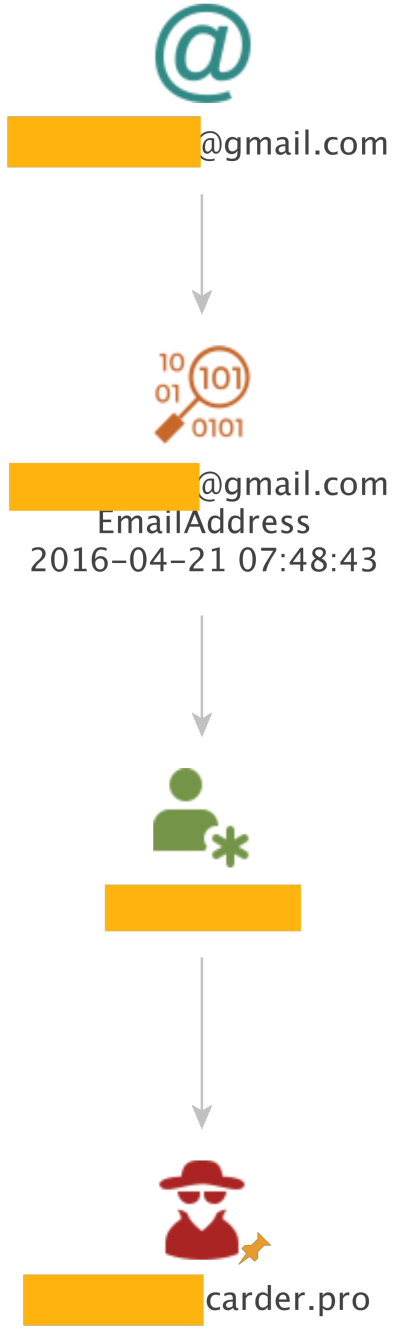
Addresses

Phone numbers

What do we do now?

We know that this person is a cyber criminal. Is there any presence on cybercrime forums?

Let’s find out using the IP and email addresses we found!



Email address we found

Intel 471 pivot

Threat actor profile on carding forum

Let’s see what they have been posting about!

[redacted]
korovka.name

Threat actor profile

БД игровово хостера
korovka.name
3

Thread they posted in

не актуально.
2011-10-29 01:49:27
[redacted]

Message they posted

Let’s see what they have been posting about!

korovka.name

Threat actor profile

БД игровово хостера korovka.name 3

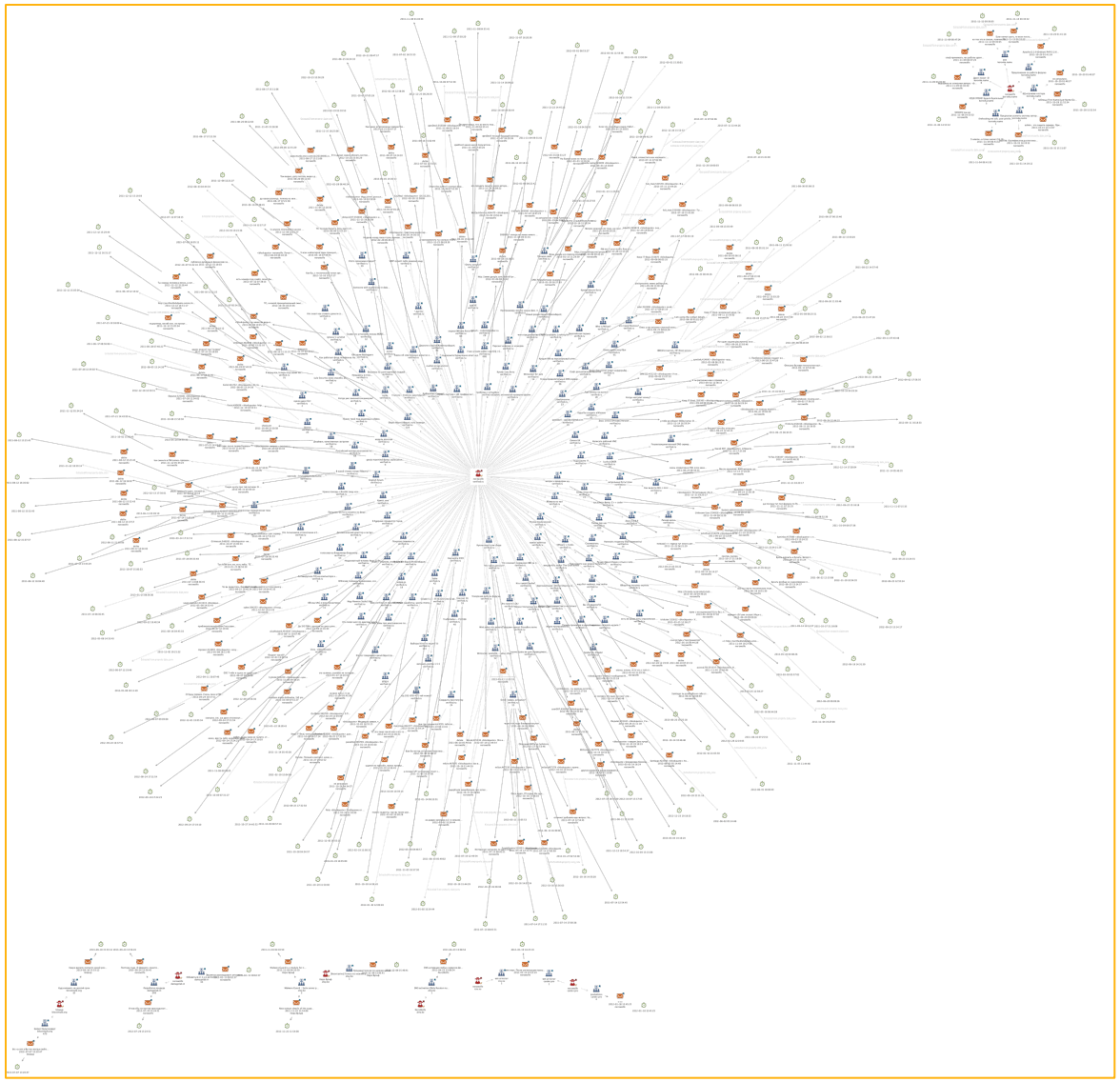
Thread they posted in

не актуально. 2011-10-29 01:49:27

Message they posted

Let’s repeat that process on our 11 threat actor profiles

Let’s see what they have been posting about!



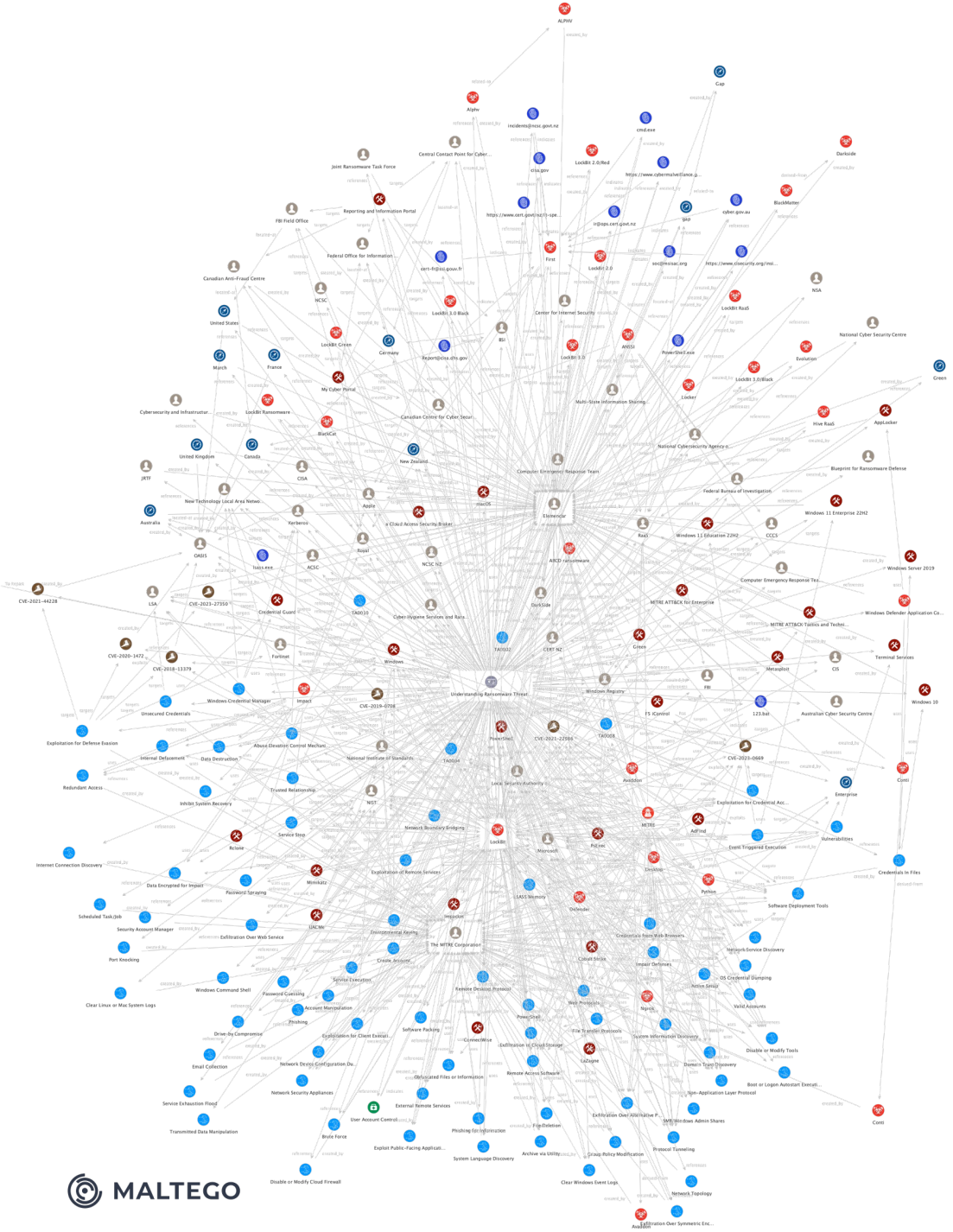
- 218 messages posted from 08-12-2010 to 24-09-2013
- 3 Jabber IDs discovered in messages
- Several tools and domains mentionned

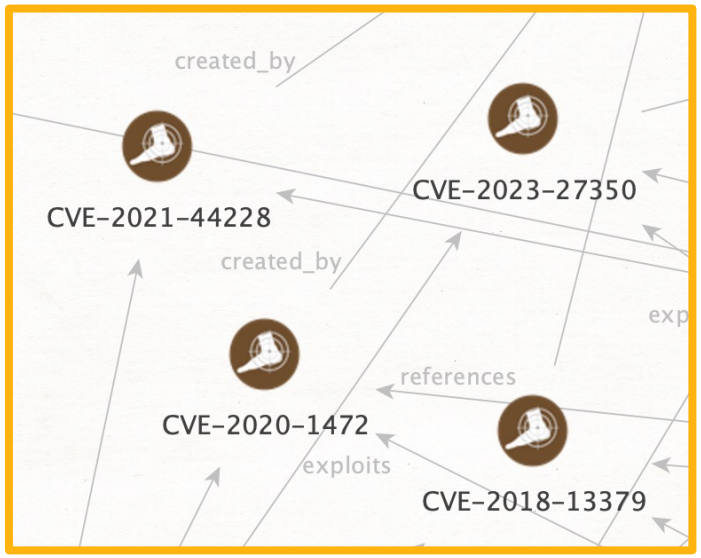
Malware Guard is a module for netfilter/iptables that can be used for filtering incoming/outgoing packets by their class. **The purpose of this product is regular collection of IP addresses that are actively engaged in fighting cybercrime and adding them to a database**. Low prices of database updates make Malware Guard an affordable **protection system for your admin panels**, setups and domains. […] All buyers must get verified on the forum via PM. If your reputation isn't good, we may refuse selling the product. […] Price list License for one server: USD 250 (this is the price for the beta version) Database update: USD 10 Contact details Jabber support@**********.com ICQ ********** This thread is only for reviews, all questions should be asked on Jabber. Mirror links: https://exploit.in/[...]

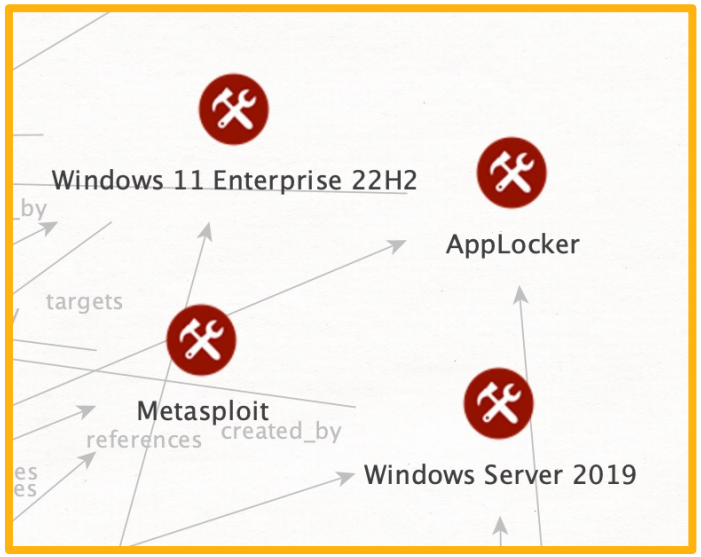
CTI: LOCKBIT

Let’s look at LockBit with Maltego

Automatic report parsing with Elemendar







MALTEGO

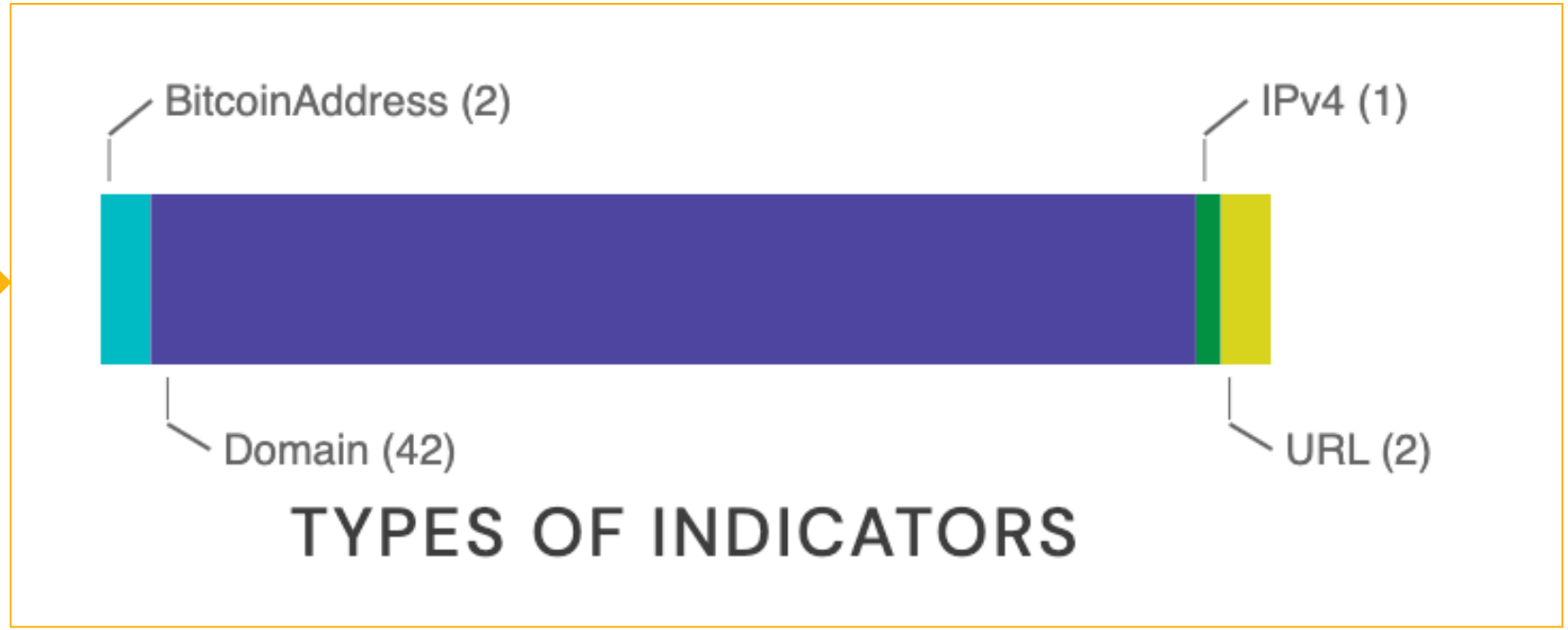
Let’s use VirusTotal to track LockBit – starting with OTX AlienVault

Return of LockBit

CREATED 7 DAYS AGO by Bheeshmar | Public | TLP: Green

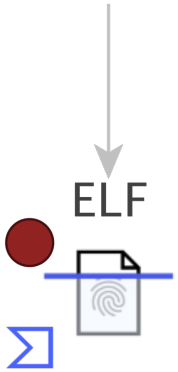
After the FBI/Europol Compromise, the LockBit Group bounced back with a fresh batch of victims and a new set of data leaks, here are some key details about their comeback: Research Article by Rakesh Krishnan.

REFERENCES: https://medium.com/coinmonks/the-return-of-lockbit-8d7bcb9b75fa
https://twitter.com/RakeshKrish12/status/1790614940551901410



Where do we go from this IP address ?

5.182.5.126



931cb123cda9cca9d655b9a5783d2b8...

To files that VirusTotal witnessed communicating with this IP address

ssyn.cf

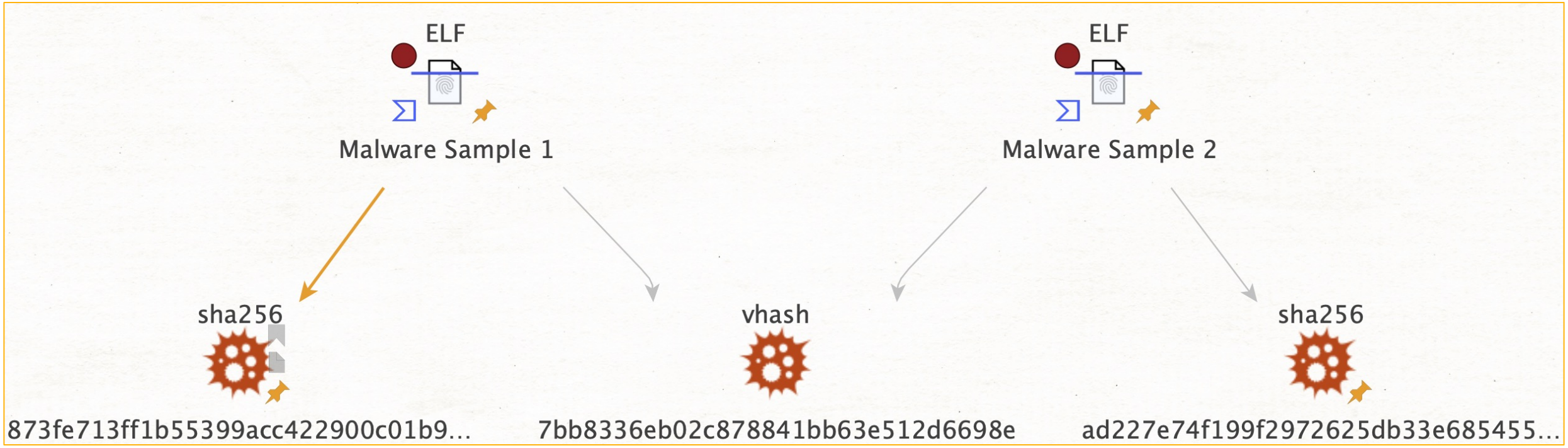
To domains that this file contacted according to VirusTotal

What is a vhash ?

https://docs.virustotal.com/reference/files

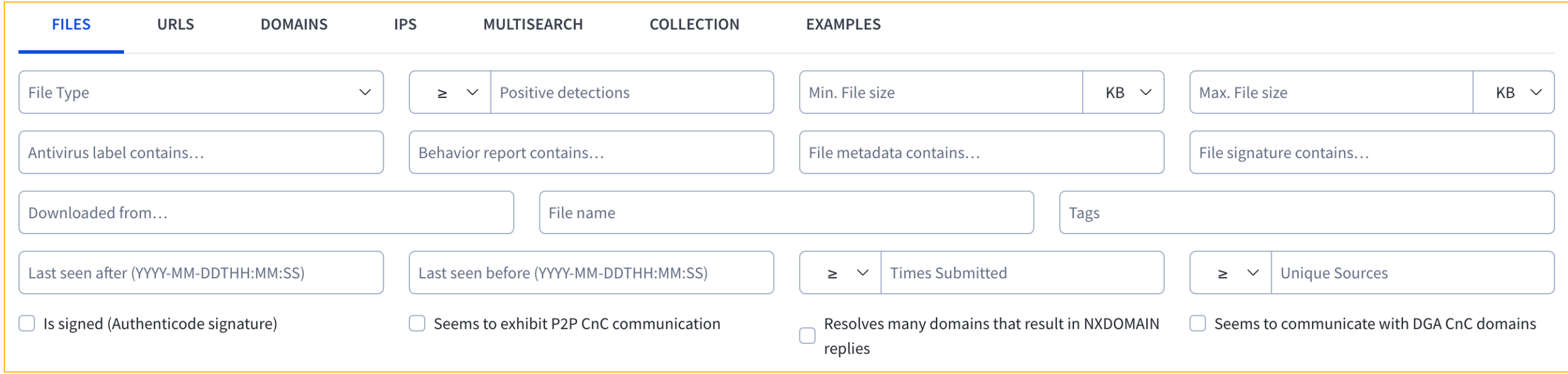
- `vhash` : <*string*> in-house similarity clustering algorithm value, based on a simple structural feature hash allows you to find similar files.

A vhash is calculated from a given file. Except that it isn't meant to represent ONLY ONE file. Similar files are meant to have the same vhash. Unlike "traditional" hashes like MD5 or SHA256.



Let’s use VT query syntax!

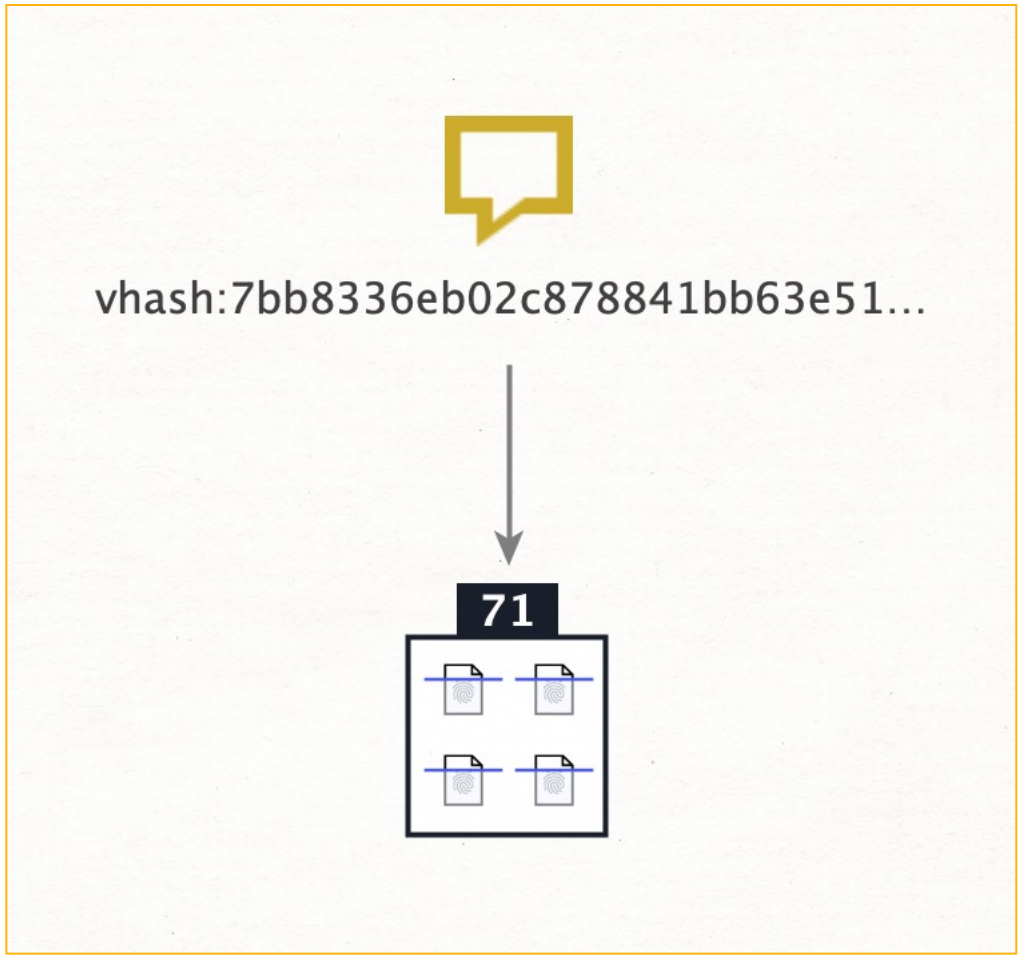
https://docs.virustotal.com/docs/file-search-modifiers



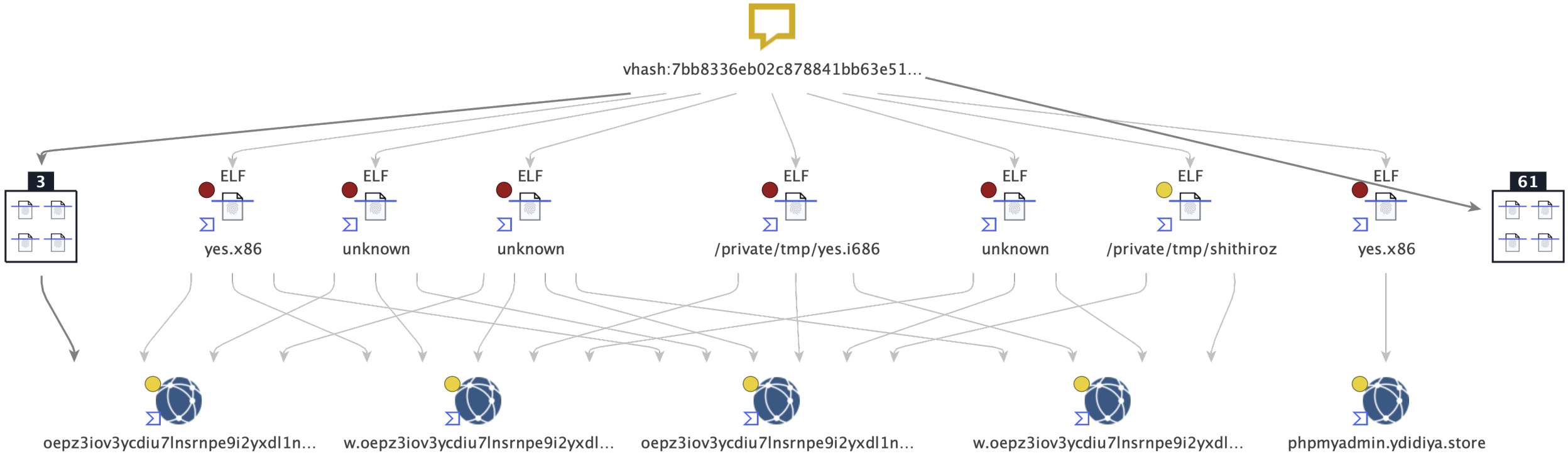
vhash:7bb8336eb02c878841bb63e512d6698e **fs**:7d+

Let’s use VT query syntax!

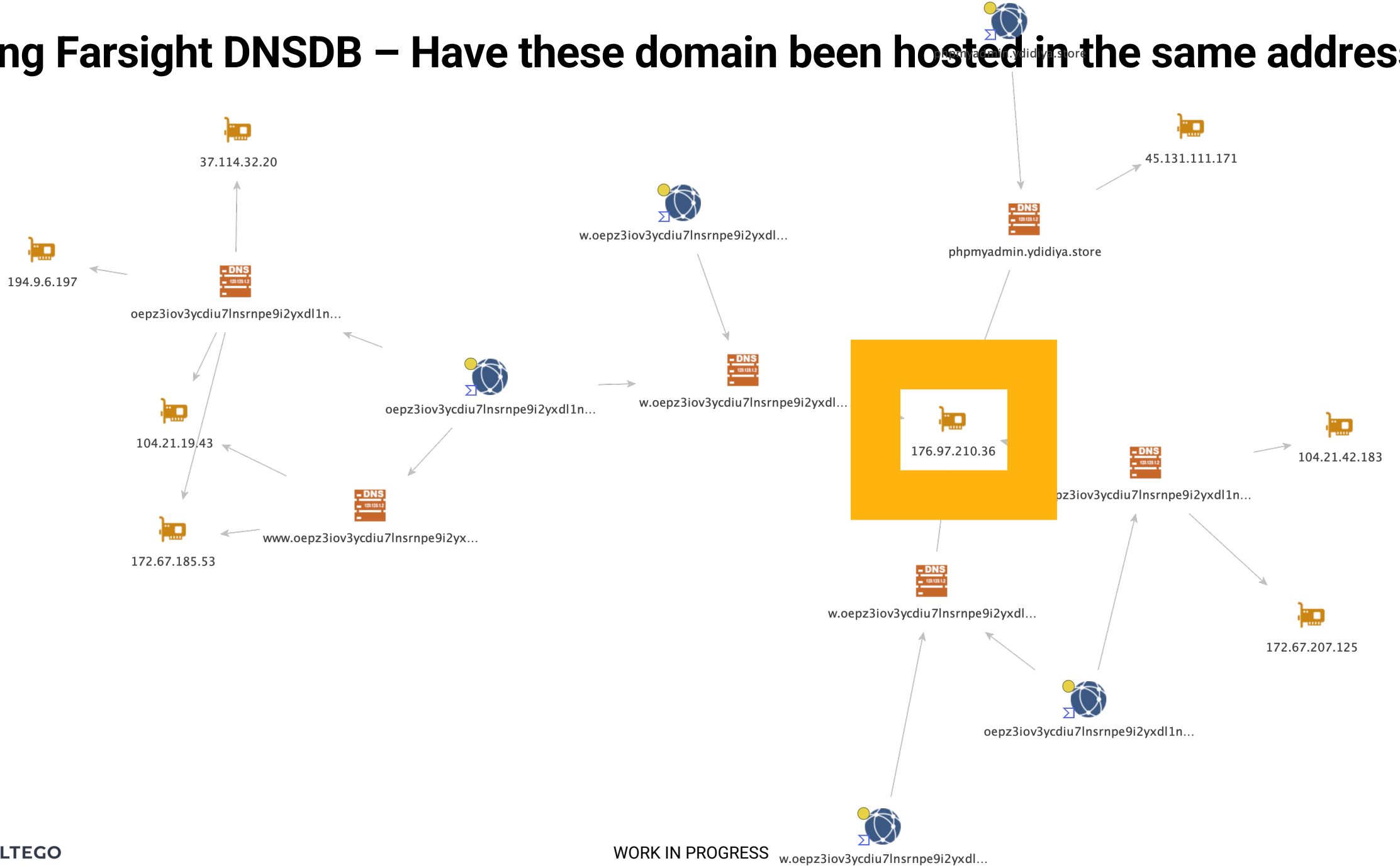
vhash:7bb8336eb02c878841bb63e512d6698e fs:7d+



Let’s see where these samples were downloaded from

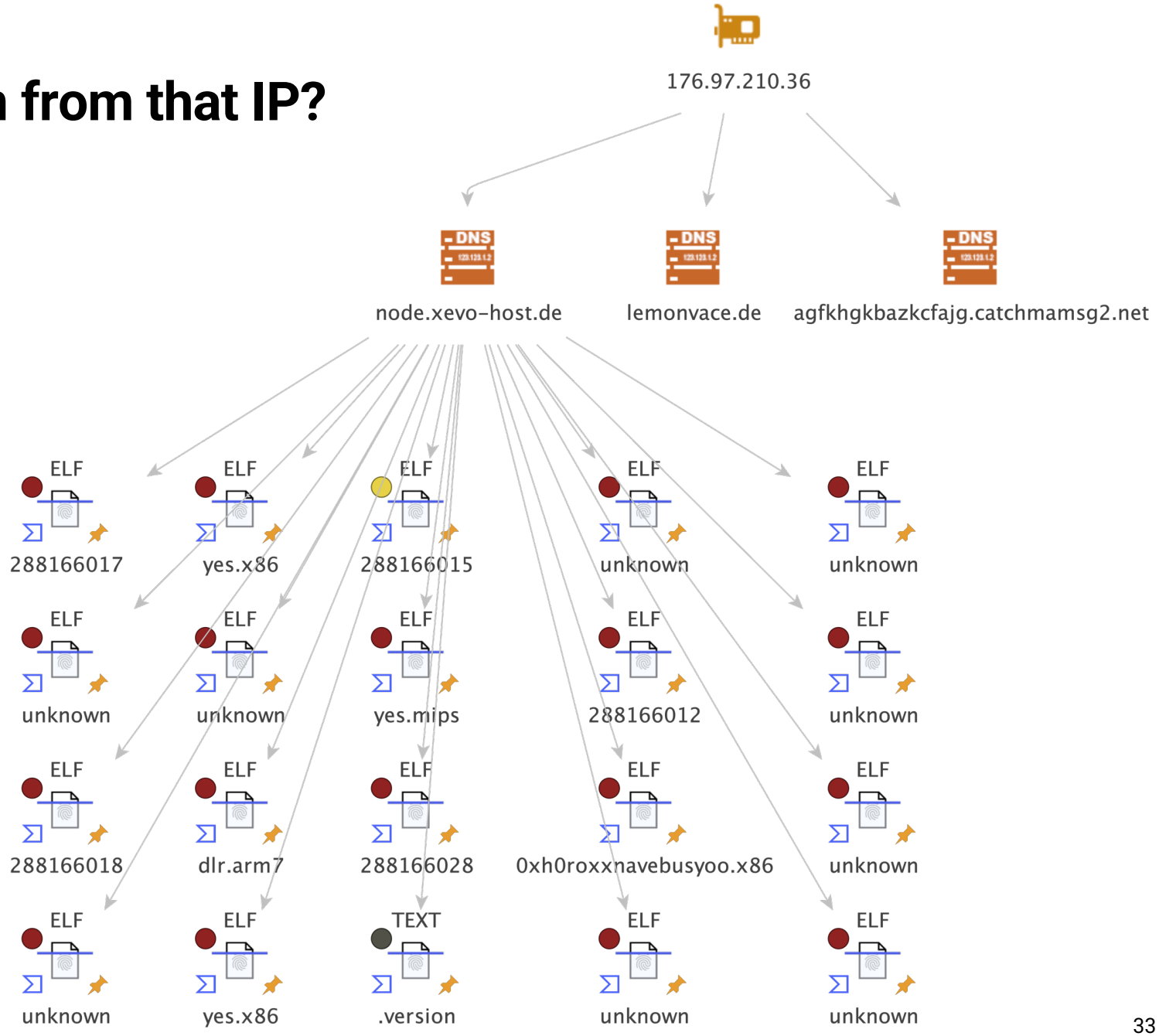


Using Farsight DNSDB – Have these domain been hosted in the same address?



Using Farsight DNSDB –
Can we discover more domain from that IP?

Using Farsight DNSDB –
Can we discover more domain from that IP?



THANK YOU

QUESTIONS?