The Art of Pivoting - How You Can Discover More from Adversaries with Existing Information

CIRCL - Virtual Summer School 2025

🏠 https://www.ail-project.org

Alexandre Dulaunoy - alexandre.dulaunoy@circl.lu / Aurelien Thirion - aurelien.thirion@circl.lu

July 17, 2025

CIRCL https://www.circl.lu

TLP:CLEAR

What is Defender's Pivoting?

- Pivoting[1] is the analytical process of using one known artifact (such as an indicator of compromise (IOC), behavioral fingerprint, or identity trace) to uncover additional, related elements within a threat actor's infrastructure, toolkit, service, or operation. This technique enables analysts to expand the scope of an investigation, uncover hidden connections, confirm or attribute activity, and anticipate future adversary behavior.

[1] The term "pivoting" can cause confusion. In this context, we refer to defender's pivoting using data points, distinct from the threat actor's lateral movement within a compromised infrastructure.

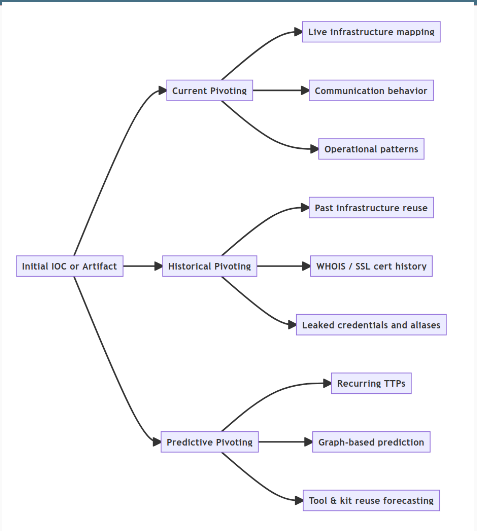
Six Degrees of Separation and Pivoting

- The concept of *six degrees of separation*[2] suggests that any two individuals are connected through a chain of six or fewer social relationships.
- Similarly, in threat intelligence, pivoting is an analyst's method for uncovering hidden relationships, much like navigating a social graph. Instead of people, we're connecting data points and observables.
- Just as social networks reveal how people are linked, threat intelligence graphs reveal how indicators, infrastructure, and behaviors are interrelated, enabling defenders to map out and understand adversary ecosystems.

[2] Also referenced in popular culture as the "Six Degrees of Kevin Bacon," or in academic contexts as the "Erdős number," which measures how many co-authorship links separate a researcher from mathematician Paul Erdős.

Analytical Benefits of Pivoting

- **Current:** Understand how a threat actor interacts, communicates, and operates in real time.
- **Historical:** Reveal past connections between threat actors and specific infrastructure or identities.
- **Predictive:** Anticipate future actions based on recurring patterns, techniques, and operational habits.



TLP:CLEAR

Is Pivoting Evolving?

- We strive to shift pivoting from an art to a science, making it reproducible, practical, and truly actionable for analysts.
- Yet, our perspective is sometimes clouded by **rigid models** or **legacy practices** that may no longer reflect today's threat landscape.
- Should we reconsider our reliance on models like the *Pyramid of Pain*, and critically assess how difficult it really is for adversaries to alter high-value indicators?
- Do threat actors always realize which traces they leave behind[3], and can they truly gauge the intelligence value of what they expose?

[3] Remember where the "Anna-Senpai" handle eventually led?

TLP:CLEAR

Re-evaluating Our Indicator Collection and Pivoting Practices

- In the AIL project[4], we collect a wide range of sources—from social networks and Tor hidden services to forums and specific web infrastructure used by threat actors.
- We've implemented a dynamic correlation engine that allows easy integration of new object types for pivoting and analysis.
- This required a mindset shift: **focusing more on outliers and overlooked data points**, while challenging and discarding some of our older assumptions.

[4] https://ail-project.org/

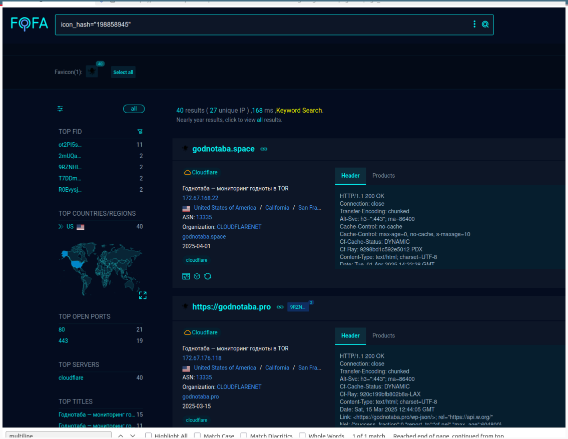
TLP:CLEAR

Looking at Broken Indicators—and Still Using Them

- MurmurHash3 is still widely used for favicon correlation. It enables quick discovery of Tor hidden services exposed on the clear web through simple hash-based pivoting.
- If MurmurHash3 is known to be flawed, why do we still use it? Because despite its weaknesses[5], it remains effective—and threat actors rarely think to modify their favicons.
- An interesting angle: some actors may attempt to create hash collisions. Correlating on *colliding* favicons can itself become a pivoting technique. So why stop calculating them?

[5] The same question can be asked about other algorithms used in threat intelligence processing.

Favicons as Differentiators and Composite Correlation Points



FOFA

icon_hash="198858945"

Favicon(1): 40 Select all

all

40 results (27 unique IP) ,168 ms ,Keyword Search.
Nearly year results, click to view all results.

TOP FID	
ot2PI5s...	11
2mUQa...	2
9RZNHI...	2
T7DDm...	2
R0Evysj...	2

TOP COUNTRIES/REGIONS	
US	40

TOP OPEN PORTS	
80	21
443	19

TOP SERVERS	
cloudflare	40

TOP TITLES	
Годнотаба — мониторинг го...	15
Годнотаба — мониторинг го...	11

godnotaba.space

Cloudflare

Годнотаба — мониторинг годноты в TOR
172.67.168.22
United States of America / California / San Fra...
ASN: 13335
Organization: CLOUDFLARENET
godnotaba.space
2025-04-01
cloudflare

Header | Products

```
HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Alt-Svc: h3=":443"; ma=86400
Cache-Control: no-cache
Cache-Control: max-age=0, no-cache, s-maxage=10
Cf-Cache-Status: DYNAMIC
Cf-Ray: 9298bd1c592e5012-PDX
Content-Type: text/html; charset=UTF-8
Date: Tue, 01 Apr 2025 14:22:28 GMT
```

https://godnotaba.pro 9RZN... 2

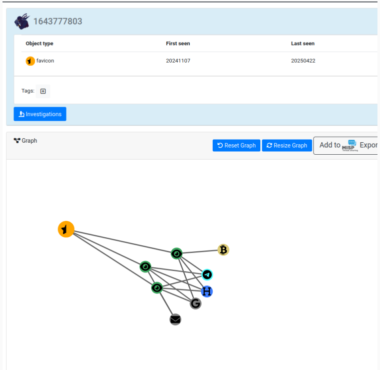
Cloudflare

Годнотаба — мониторинг годноты в TOR
172.67.176.118
United States of America / California / San Fra...
ASN: 13335
Organization: CLOUDFLARENET
godnotaba.pro
2025-03-15
cloudflare

Header | Products

```
HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Alt-Svc: h3=":443"; ma=86400
Cf-Cache-Status: DYNAMIC
Cf-Ray: 920c199bfb802b8a-LAX
Content-Type: text/html; charset=UTF-8
Date: Sat, 15 Mar 2025 12:44:05 GMT
Link: <https://godnotaba.pro/wp-json/>; rel="https://api.w.org/"
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
```

multiline ☐ Highlight All ☐ Match Case ☐ Match Diacritics ☐ Whole Words 1 of 1 match Reached end of page, continued from top



1643777803

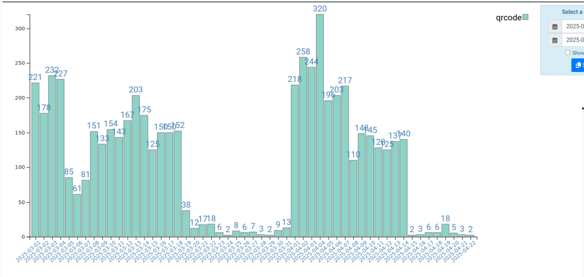
Object type	First seen	Last seen
favicon	20241107	20250422

Tags:

Even seemingly innocuous favicons can act as unique fingerprints—useful for correlating threat infrastructure across campaigns or layers (e.g., Tor vs. clear web).

Uncommon Indicator Extraction: QR Codes

- QR codes are increasingly seen across social networks, Tor hidden services, and even in ransomware negotiation pages.



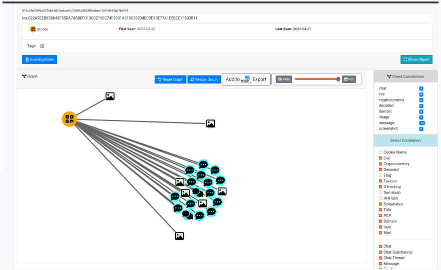
Select a date range :

2025-03-01

2025-04-22

□ Show Qrcodes

Search



814c2fa920f6a57366e4d13adcae5c79801a2823f9c8bae136f54443dd7b4f43 :

tox:022A7EEB83B648F55DA7A6BEFD130C2156C74F3501A31D853234EC2D18E77A1E5BEC7F602011

qrcode First Seen: 2025-03-29 Last Seen: 2025-04-21

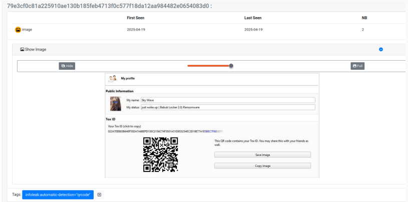
Tags: ⊞

chat	2
cve	0
cryptocurrency	0
decoded	0
domain	0
image	7
message	14
screenshot	0

Select Correlation

□ Cookie Name
☑ Cve
☑ Cryptocurrency
☑ Decoded
□ Etag
☑ Favicon
☑ G tracking
□ DomHash
□ HHHash
☑ Screenshot
☑ Title
☑ PGP
☑ Domain
☑ Item
☑ Mail

☑ Chat
☑ Chat-Subchannel
☑ Chat-Thread
☑ Message



79e3cf0c81a225910ae130b185feb4713f0c577f18da12aa984482e0654083d0 :

	First Seen	Last Seen	NB
image	2025-04-19	2025-04-19	2

My profile

Public Information

My name: Sky Wave

My status: just woke up (Babuk Locker 2.0) Ransomware

Tox ID

Your Tox ID (click to copy)

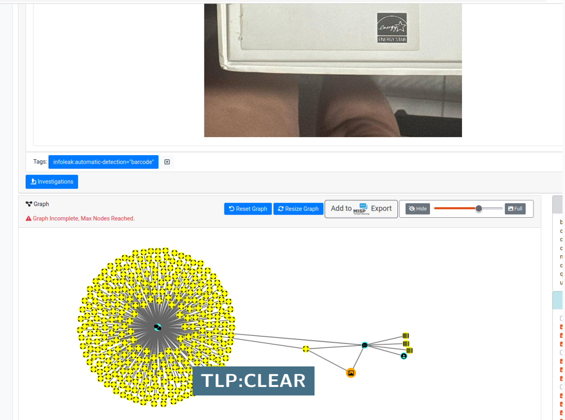
022A7EEB83B648F55DA7A6BEFD130C2156C74F3501A31D853234EC2D18E77A1E5BEC7F602011

This QR code contains your Tox ID. You may share this with your friends as well.

Tags: infoleak:automatic-detection="qrcode" ⊞

Uncommon Indicator Extraction from Images: Barcodes

- Following a request from law enforcement, we implemented barcode extraction (Code 128, Code 39, Code 93, etc.).
- Barcodes turned out to be **valuable correlation points**, not only in large data leaks, but also in social media interactions involving threat actors.



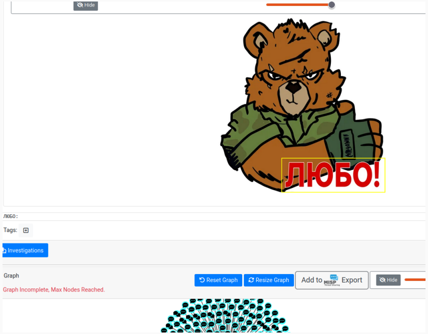
Tags: infoleak:automatic-detection="barcode"

Graph Incomplete, Max Nodes Reached.

TLP:CLEAR

Semantic and Textual Information in Images

- **Images often contain valuable textual data**, such as device numbers, identifiers, and embedded messages, that can be extracted for analysis.
- CRNN-based OCR models perform well and are highly efficient on modern hardware, making large-scale image parsing feasible.



ЛЮБО :

Tags:

Graph

Graph Incomplete, Max Nodes Reached.

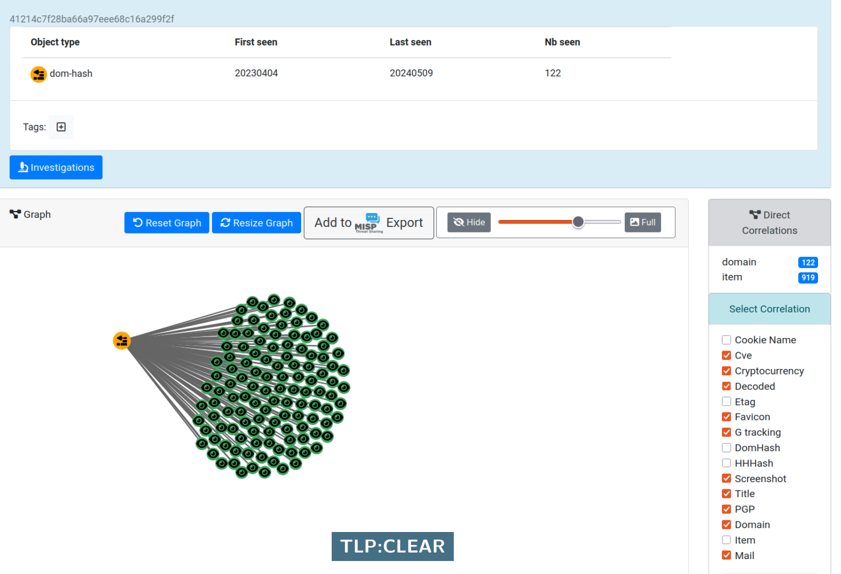
New Indicators from Common HTML Structures - dom-hash

- Has everything already been explored in HTML document classification, hashing, or structural similarity detection?
- Following a discussion with CERT-PL, we discovered that a **simple strategy yields excellent results**[6] and led to the development of the dom-hash algorithm.

```python
def _compute_dom_hash(html_content):
    soup = BeautifulSoup(html_content, "lxml")
    to_hash = "|".join(t.name for t in soup.findAll()).encode()
    return sha256(to_hash).hexdigest()[:32]
```

[6] Tested against LookyLoo dataset https://lookyloo.circl.lu

Fast Clustering of Tor Hidden Services using `dom-hash`



41214c7f28ba66a97eee68c16a299f2f

Object type	First seen	Last seen	Nb seen
dom-hash	20230404	20240509	122

Tags: ⊞

Direct Correlations

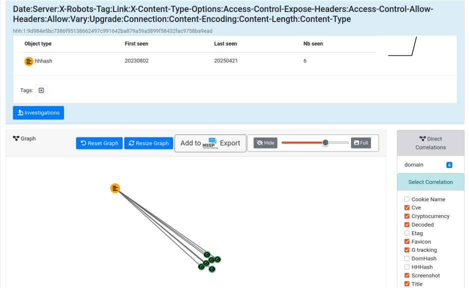
domain	122
item	919

- ☐ Cookie Name
- ☑ Cve
- ☑ Cryptocurrency
- ☑ Decoded
- ☐ Etag
- ☑ Favicon
- ☑ G tracking
- ☐ DomHash
- ☐ HHHash
- ☑ Screenshot
- ☑ Title
- ☑ PGP
- ☑ Domain
- ☐ Item
- ☑ Mail

TLP:CLEAR

What Simple Correlations Are Often Missed? — HTTP Headers

HTTP (version 1) response headers can act as subtle fingerprints (HHHash)[7] for linking threat infrastructure.



Date:Server:X-Robots-Tag:Link:X-Content-Type-Options:Access-Control-Expose-Headers:Access-Control-Allow-Headers:Allow:Vary:Upgrade:Connection:Content-Encoding:Content-Length:Content-Type

hhh:1:9d984e5bc7386f95138662497c991642ba879a59a5899f58432fac9758ba9ead

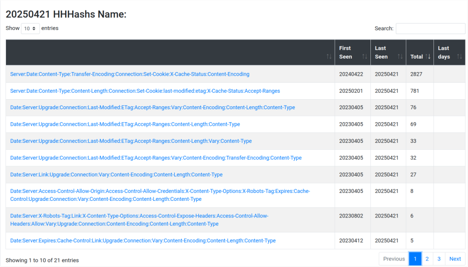
Object type	First seen	Last seen	Nb seen
hhhash	20230802	20250421	6

Tags:

domain 6

Select Correlation

- □ Cookie Name
- ☑ Cve
- ☑ Cryptocurrency
- ☑ Decoded
- □ Etag
- ☑ Favicon
- ☑ G tracking
- □ DomHash
- □ HHHash
- ☑ Screenshot
- ☑ Title



20250421 HHHashs Name:

Show 10 entries Search:

	First Seen	Last Seen	Total	Last days
Server:Date:Content-Type:Transfer-Encoding:Connection:Set-Cookie:X-Cache-Status:Content-Encoding	20240422	20250421	2827	
Server:Date:Content-Type:Content-Length:Connection:Set-Cookie:last-modified:etag:X-Cache-Status:Accept-Ranges	20250201	20250421	781	
Date:Server:Upgrade:Connection:Last-Modified:ETag:Accept-Ranges:Vary:Content-Encoding:Content-Length:Content-Type	20230405	20250421	76	
Date:Server:Upgrade:Connection:Last-Modified:ETag:Accept-Ranges:Content-Length:Content-Type	20230405	20250421	69	
Date:Server:Upgrade:Connection:Last-Modified:ETag:Accept-Ranges:Content-Length:Vary:Content-Type	20230405	20250421	33	
Date:Server:Upgrade:Connection:Last-Modified:ETag:Accept-Ranges:Vary:Content-Encoding:Transfer-Encoding:Content-Type	20230405	20250421	32	
Date:Server:Link:Upgrade:Connection:Vary:Content-Encoding:Content-Length:Content-Type	20230405	20250421	27	
Date:Server:Access-Control-Allow-Origin:Access-Control-Allow-Credentials:X-Content-Type-Options:X-Robots-Tag:Expires:Cache-Control:Upgrade:Connection:Vary:Content-Encoding:Content-Length:Content-Type	20230405	20250421	8	
Date:Server:X-Robots-Tag:Link:X-Content-Type-Options:Access-Control-Expose-Headers:Access-Control-Allow-Headers:Allow:Vary:Upgrade:Connection:Content-Encoding:Content-Length:Content-Type	20230802	20250421	6	
Date:Server:Expires:Cache-Control:Link:Upgrade:Connection:Vary:Content-Encoding:Content-Length:Content-Type	20230412	20250421	5	

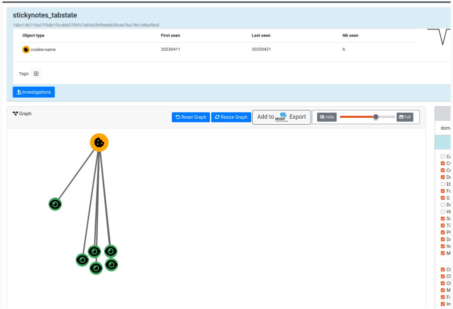
Showing 1 to 10 of 21 entries

[7] https://www.foo.be/2023/07/HTTP-Headers-Hashing_HHHash

TLP:CLEAR

Another Simple Correlation? — Cookie Names

- Custom or reused cookie names[8] can serve as low-noise indicators for linking **attacker-controlled web infrastructure**.

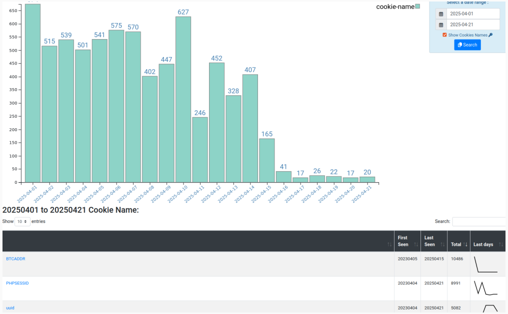


stickynotes_tabstate

16bc14b715a27f5db1f3cdd437f0f27a95e2fbf9e8d65fa4e7be7961d9bef8e5

Object type	First seen	Last seen	Nb seen
cookie-name	20230411	20250421	6

Tags:



Select a date range :

2025-04-01

2025-04-21

☑ Show Cookies Names

20250401 to 20250421 Cookie Name:

Show 10 entries

Search:

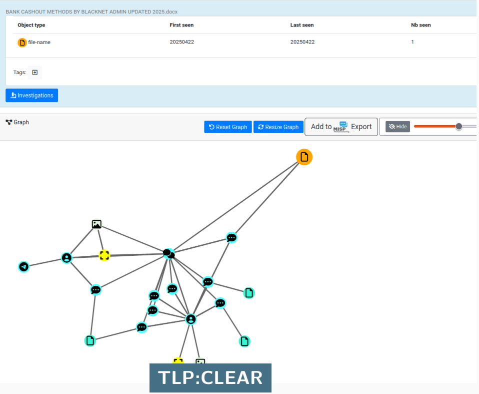
	First Seen	Last Seen	Total	Last days
BTCADDR	20230405	20250415	10486	
PHPSESSID	20230404	20250421	8991	
uuid	20230404	20250421	5082	

[8] The value of the cookie are also interesting but correlation cannot be used as it without further processing

TLP:CLEAR

An Even Simpler Correlation Indicator? — Filenames

- In threat intelligence, filenames are often dismissed as unreliable or noisy indicators that may lead to false conclusions.
- However, in some cases, especially on social networks or in leak dumps, filenames can carry meaningful context that reveals key aspects of a threat actor's activity.



BANK CASHOUT METHODS BY BLACKNET ADMIN UPDATED 2025.docx

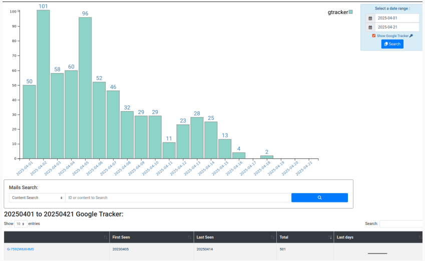
Object type	First seen	Last seen	Nb seen
file-name	20250422	20250422	1

Tags:

TLP:CLEAR

Indicators That Threat Actors Should Avoid—But Still Use

- It is **commonly assumed that threat actors avoid including labels or metadata** that could link their infrastructure or even their operational teams.
- However, our regular crawling of Tor hidden services revealed that Google Analytics tracking codes[9] were reused across multiple sites, uncovering unexpected and meaningful correlations.



Select a date range :

2025-04-01

2025-04-21

☑ Show Google Tracker

Mails Search:

ID or content to Search

20250401 to 20250421 Google Tracker:

Show 10 entries

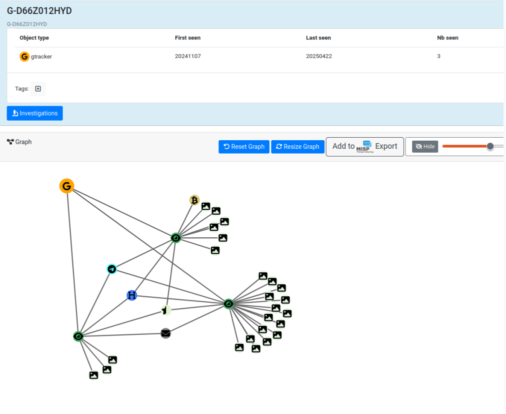
Search:

	First Seen	Last Seen	Total	Last days
G-7592W6XHM5	20230405	20250414	501	

[9] Based on monthly crawling of Tor hidden services, which explains the distribution shown in the graph.

TLP:CLEAR

Even ”Weak” Indicators Like Google Analytics Can Be Powerful in Composite Correlation



G-D66Z012HYD

G-D66Z012HYD

Object type	First seen	Last seen	Nb seen
G gtracker	20241107	20250422	3

Tags: ⊞

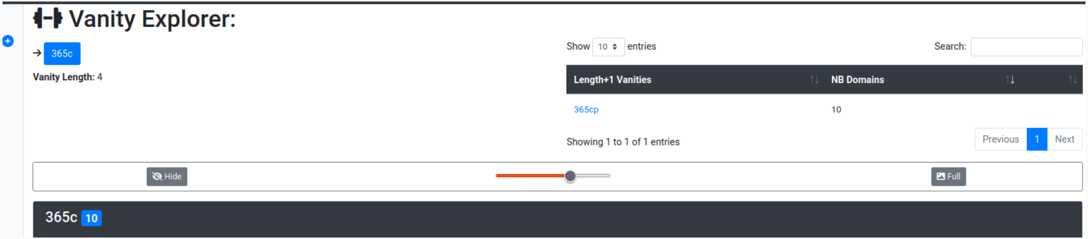
Why it matters:

- Google Analytics tracking IDs are often reused across phishing domains, malicious sites, or cloned templates.
- While GA IDs alone may not prove attribution, when combined with other indicators (e.g., favicon hash, `dom-hash`, or TLS cert), they help cluster infrastructure belonging to the same threat actor or Tor operator.
- Many actors underestimate the traceability of third-party embedded analytics even Ransomware groups.

TLP:CLEAR

Unexpected Correlation from Cryptographic Materials

- Threat actors often simplify their operations by generating Tor onion services with custom "vanity" addresses—based on recognizable prefixes derived from cryptographic key fingerprints.
- While the exact logic behind the generation is not always disclosed, building a tree or graph structure of these vanity addresses can **reveal shared patterns** and uncover related services.



Vanity Explorer:

→ 365c

Vanity Length: 4

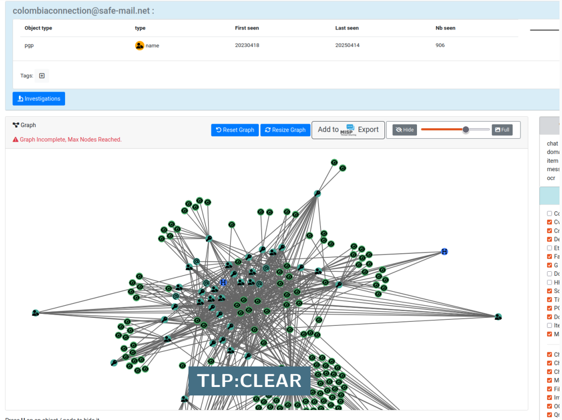
Show 10 entries Search:

Length+1 Vanities	NB Domains
365cp	10

Showing 1 to 1 of 1 entries

Pivoting on Encrypted Messages and Metadata

- Sometimes, **collecting encrypted messages or public keys** can reveal unexpected links, especially when metadata is extracted from PGP blocks.
- Elements such as key IDs, user IDs, creation dates, or repeated usage of the same key across services can all serve as valuable pivot points.



colombiaconnection@safe-mail.net :

Object type	type	First seen	Last seen	Nb seen
pgp	name	20230418	20250414	906

Tags: ⊞

Graph

Graph Incomplete, Max Nodes Reached.

Press H on an object / node to hide it.

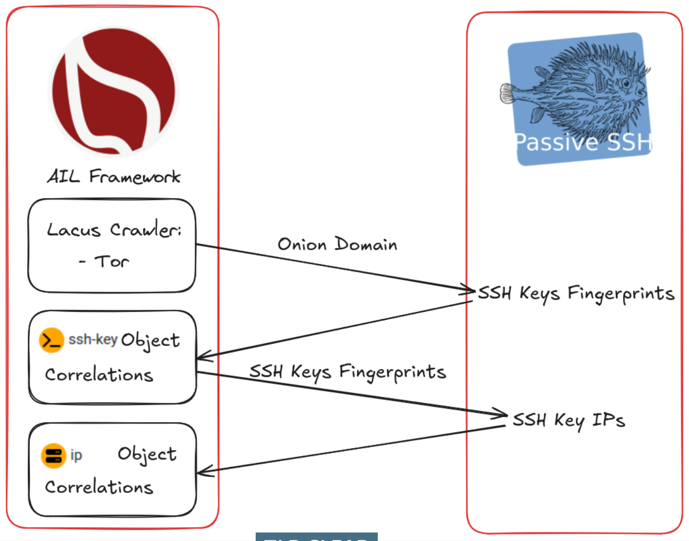
TLP:CLEAR

Passive SSH[11]

- Open-source **passive-ssh** scanner & database[10]
- Captures: public keys, banners, **hassh** fingerprints
- Maintains full host–SSH history (who → where, when)
- Lean ReST API – lookup by key / hassh / banner
- Deanomize onions

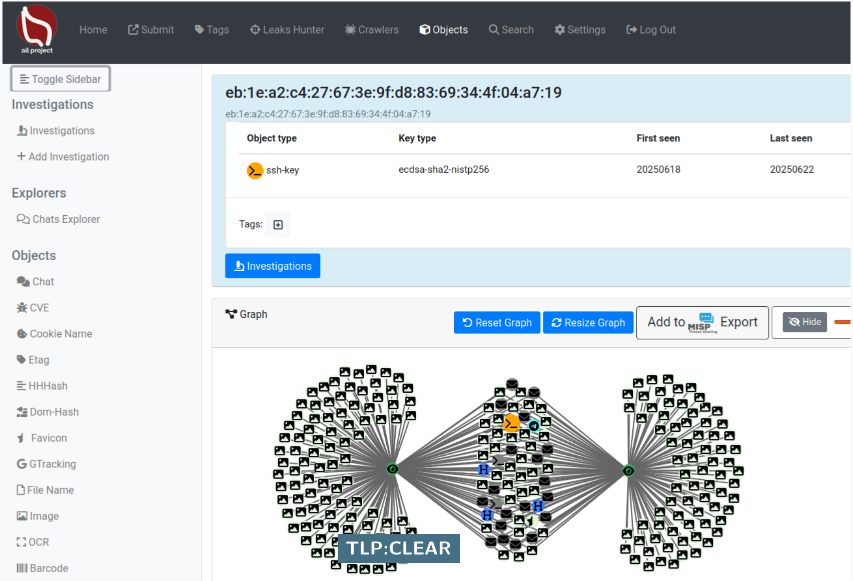
[10] https://github.com/D4-project/passive-ssh
[11] https://github.com/D4-project/passive-ssh

AIL - Passive SSH



TLP:CLEAR

AIL - SSH Correlation - Shared fingerprints



eb:1e:a2:c4:27:67:3e:9f:d8:83:69:34:4f:04:a7:19

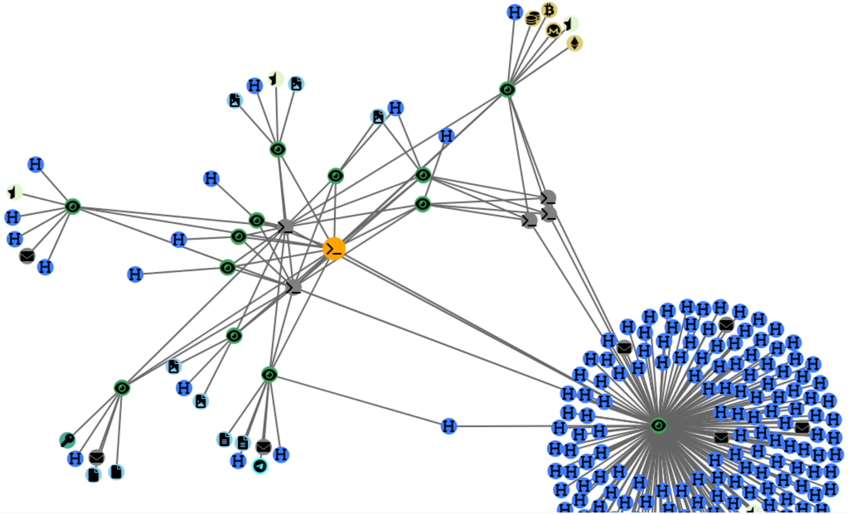
eb:1e:a2:c4:27:67:3e:9f:d8:83:69:34:4f:04:a7:19

Object type	Key type	First seen	Last seen
ssh-key	ecdsa-sha2-nistp256	20250618	20250622

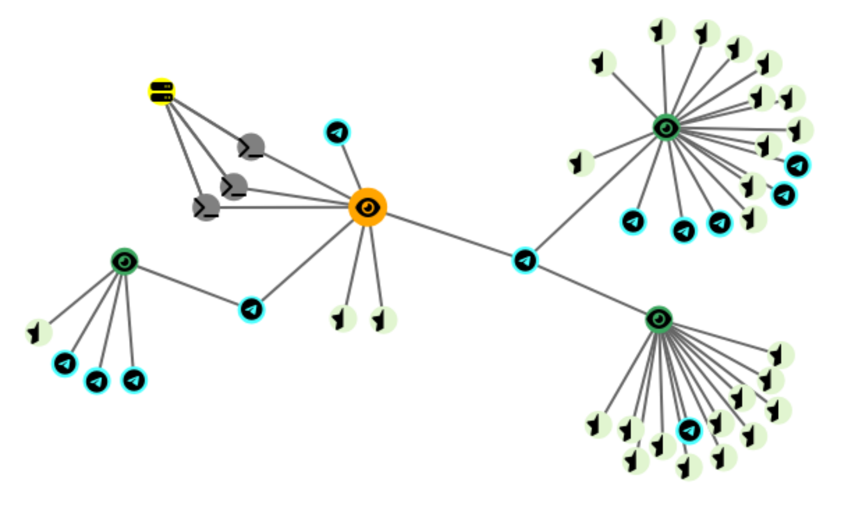
Tags:

TLP:CLEAR

AIL - SSH Correlation - Shared fingerprints



AIL - Deanomized Onions through shared fingerprints



TLP:CLEAR

Conclusion

- Pivoting is evolving from a manual, intuition-driven process into a reproducible, data-driven discipline—supported by open-source platforms like MISP and AIL.
- Uncommon indicators matter just as much as traditional ones, they often reveal what others overlook.
- Imperfect doesn't mean useless. Even outdated or colliding indicators can still provide valuable correlations.
- **Creativity is essential**, experimenting with new correlation methods leads to deeper insights and better threat discovery.

Thank you for your attention

- AIL project[12] : https://github.com/ail-project/ail-framework
- For questions, contact: info@circl.lu

[12] All techniques and indicators mentioned in these slides are implemented in the AIL project, using an instance backed by a three-year dataset collected from Tor hidden services and various social networks.