CIRCL
Computer Incident
Response Center
Luxembourg

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

2025 Cyber Threat Intelligence Conference FIRSTCTI25 - Berlin, Germany

https://www.vulnerability-lookup.org

Alexandre Dulaunoy - alexandre.dulaunoy@circl.lu

April 23, 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.

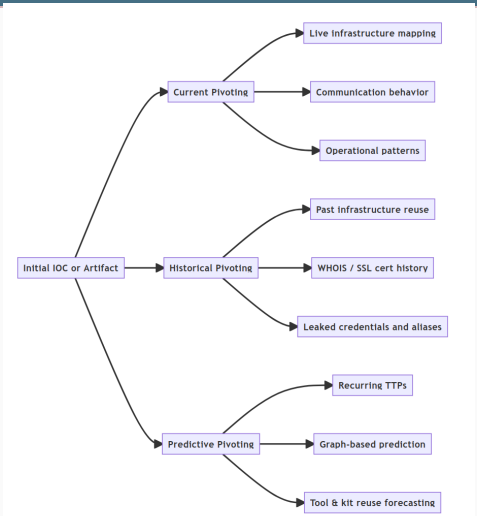
Six Degrees of Separation and Pivoting

- 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.



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?

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.

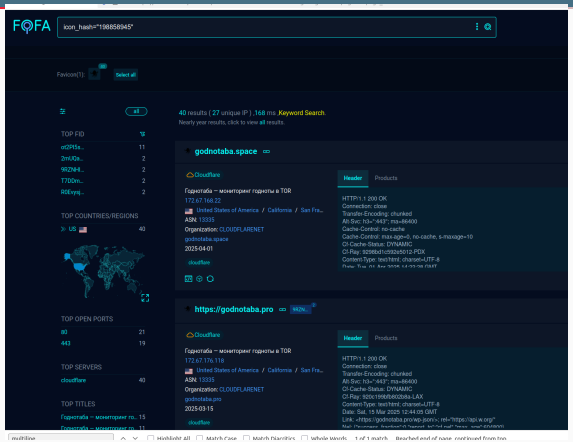
[4] https://ail-project.org/

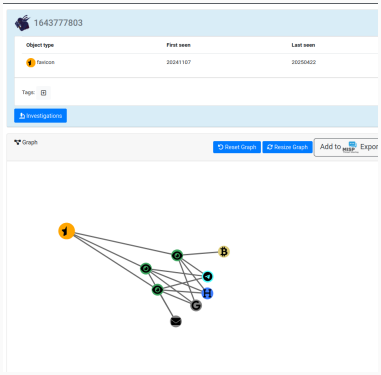
Looking at Broken Indicators—and Still Using Them

- 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



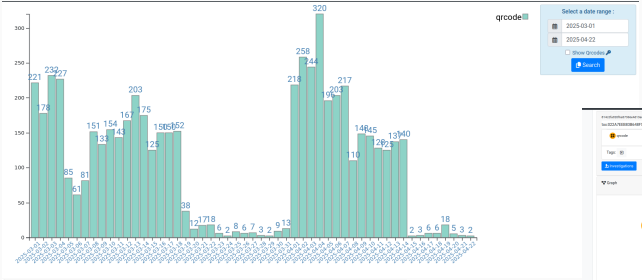


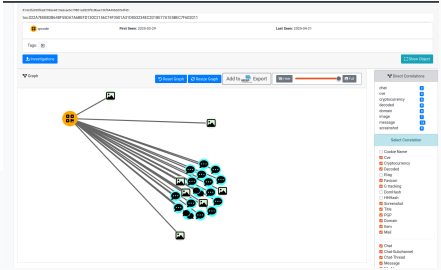
Even seemingly innocuous favicons can act as unique fingerprints—useful for correlating threat infrastructure across campaigns or layers (e.g., Tor vs. clear web).

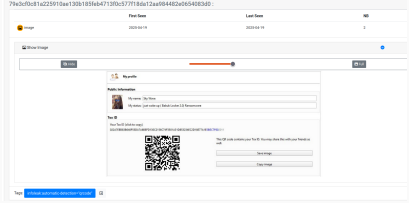
TLP:CLEAR

Uncommon Indicator Extraction: QR Codes

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

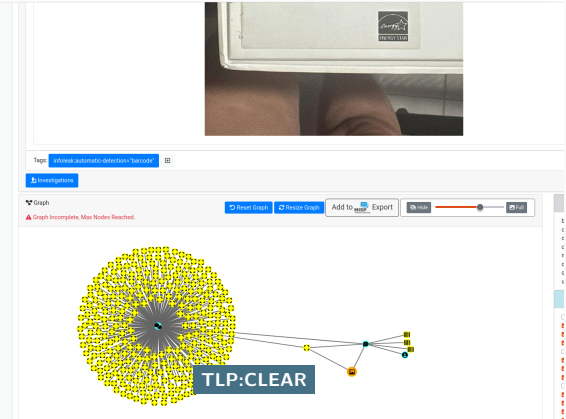






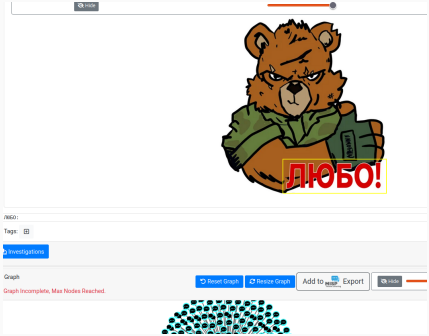
Uncommon Indicator Extraction from Images: Barcodes

- 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.



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.



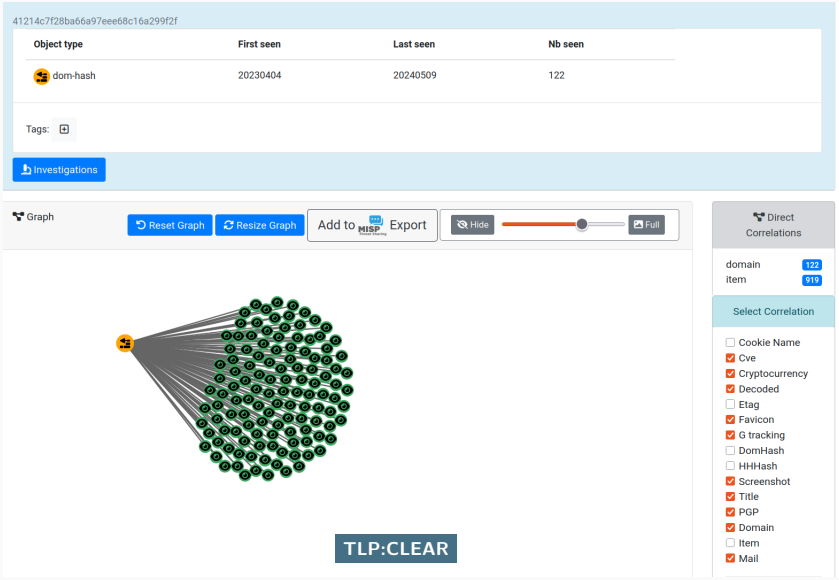
New Indicators from Common HTML Structures - dom-hash

- 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]
```

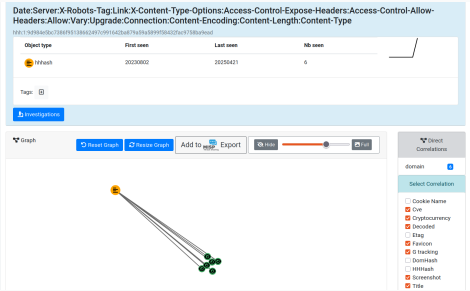
[6] Tested against LookyLoo dataset https://lookyloo.circl.lu

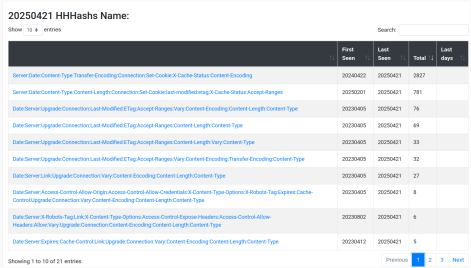
Fast Clustering of Tor Hidden Services using `dom-hash`



What Simple Correlations Are Often Missed? — HTTP Headers

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

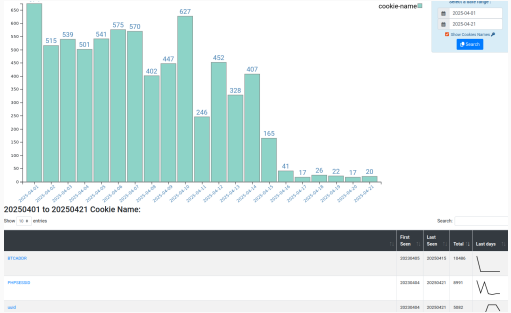




[7] https://www.foo.be/2023/07/HTTP-Headers-Hashing_HHHash

Another Simple Correlation? — Cookie Names

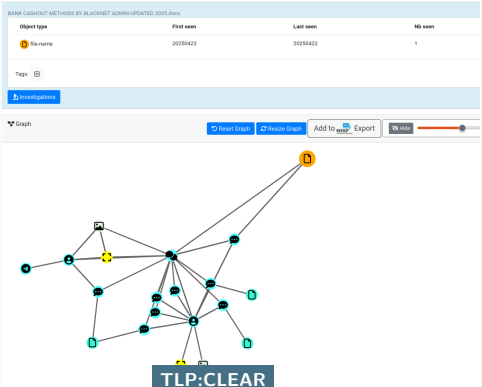
- Custom or reused cookie names[8] can serve as low-noise indicators for linking **attacker-controlled web infrastructure**.



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

An Even Simpler Correlation Indicator? — Filenames

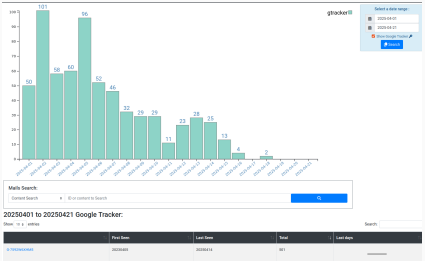
- In threat intelligence, filenames are often dismissed as unreliable or noisy indicators that may lead to false conclusions.
- However, in some cases—especially on social networks or in leak dumps—filenames can carry meaningful context that reveals key aspects of a threat actor's activity.



TLP:CLEAR

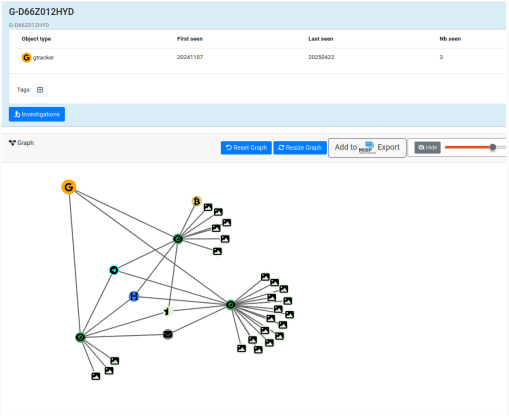
Indicators That Threat Actors Should Avoid—But Still Use

- 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.



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

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

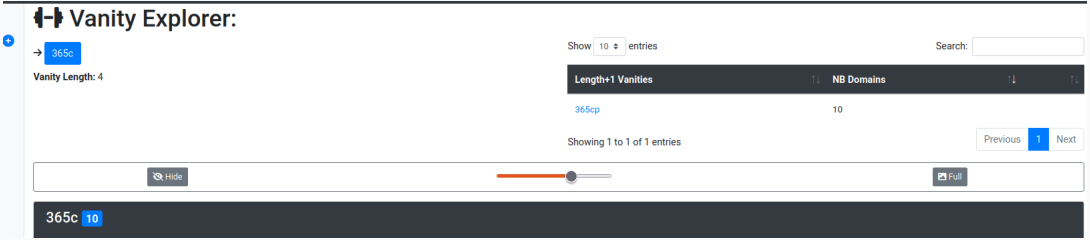


Why it matters:

- 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.

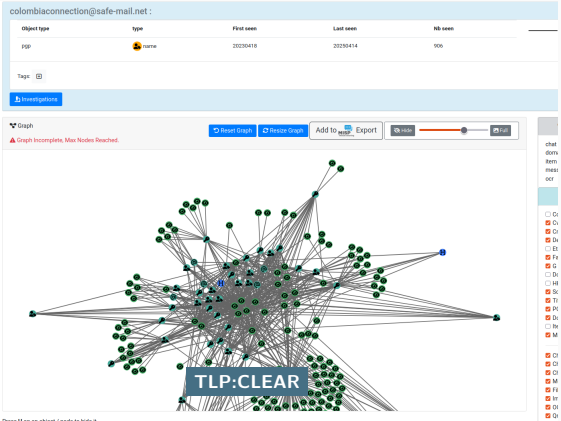
Unexpected Correlation from Cryptographic Materials

- 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.



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.



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

[10] 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.