VALIDIN

Validin's Top 7 Pivots

Effective threat hunting starts with pivoting. This resource explores seven techniques to help uncover hidden infrastructure and expand known indicators. Using real-world examples from Validin investigations, we show how these methods expose connections others may miss.

Bulk DNS & Passive DNS (PDNS) Pivoting

What it is

This approach starts with a set of known indicators (domains or IPs) and uses DNS history data to see which additional domains or hosts have shared the IP addresses, Name Server records, or other DNS attributes over time.

Because Validin continuously collects billions of DNS snapshots, analysts can quickly see when - and how often - a particular piece of infrastructure was used.

How it's used

- In "Hunting Lazarus: Expanding Indicators with Historic DNS," we demonstrate how to identify good pivots using historic DNS, how to identify bad pivots using historic DNS, and how to detect wildcarded DNS zones.

- In the blog post "X Phishing: 6 Pivoting Techniques for Threat Hunting," we begin by searching indicators using the Bulk Search tool to reveal related IPs and domain names from a combined historical DNS view.

- Additional examples and expanded techniques using Passive DNS are demonstrated in "Practical Examples Of Malware Infrastructure Discovery With Passive DNS" and "Revealing Australian Toll Spammer Infrastructure With PDNS."

HTML Meta Tag & Title Tag Pivoting

What it is

By extracting and pivoting on meta tags (e.g., <meta name="description"> or <meta name="author">) and title tags from HTML responses, analysts can find other domains that share webpage characteristics.

Because many adversaries reuse the same or similar descriptive text across compromised or fraudulent sites, these attributes serve as effective "connectors."

How it's used

- In "Lazarus APT: Techniques for Hunting Contagious Interview," we show how to use HTML meta tags to identify domain names related to the Contagious Interview campaign.

- In "Poseidon Analysis - Quick and Intuitive Workflows with Validin," we show how HTML title tags can be used to quickly identify sites related to Poseidon.

- In "X Phishing: 6 Pivoting Techniques for Threat Hunting," we show how pivoting on an extracted meta tag value (or title tag) immediately reveals additional domains that share similar HTML content.

Favicon Hash Pivoting

What it is

Every website typically serves a favicon - a small icon shown in the browser's tab.

Validin computes the hash of this favicon image, allowing analysts to search for other sites that use the exact same icon.

Since adversaries sometimes reuse favicons (either for consistency or by mistake), this attribute can help link a large number of domains.

How it's used

- The "X Phishing: 6 Pivoting Techniques for Threat Hunting" post demonstrates pivoting on the favicon hash (e.g. 9d99a2372bbd5b28ef4b2eaecac8c805).
- Additional examples of using this technique to identify both malicious and benign infrastructure (e.g., for finding public instances of popular software) are detailed in "Using Favicon Hashes to Expand Threat Knowledge".

Class Hash Pivoting

What it is

Webpages often include CSS class definitions that can be "fingerprinted." Validin computes a hash based on key CSS class names found in a webpage's source.

Adversaries may use a unique set of CSS classes (in a phishing kit, for example), allowing us to pivot on these "class hashes" to reveal other sites that share the same design attributes even if the content is significantly different from site to site.

How it's used

- In "X Phishing: 6 Pivoting Techniques for Threat Hunting", we explain how class hashes were used to identify a concise subset of domains that were likely related to an X Phishing campaign targeting high-profile accounts.

Registration Details Pivoting

What it is

Domain registration data (such as the exact or approximate time of registration, the registrar used, or even registration details like a “bogus” state field) can be indexed and pivoted on.

If several domains are registered with exactly the same characteristics, it may suggest that the same adversary is behind them.

How it’s used

- In “Pulling the Threads on the Phish of Troy Hunt,” we show examples of how bogus, highly unique “state” values provided unique pivots that enabled the discovery of additional domains. Similarly, in “Not Reality: Exploring Meta-themed Phishing with Validin,” a typo in the “state” field enabled discovery of hundreds of Meta-themed phishing domains.

- Despite privacy guards and data redaction, registration time pivots are still effective pivots for some malicious domain infrastructure, as seen in “Not Reality: Exploring Meta-themed Phishing with Validin.”

Host Response Feature Pivoting (HTTP Banner/Header Hashes)

What it is

When a web server responds to a request, it sends back HTTP headers (including the server type, banner information, and sometimes even parts of the HTML body).

Validin generates fingerprints (hashes) for these responses.

Pivots based on these features can link sites that are running identical or very similar server software or configurations (even if the IP addresses differ).

How it's used

- "Lazarus Group Bybit Heist: C2 forensics" highlights how rare banner hashes (such as b21405ce3c3456214ad8fc5263eeabb1) and header hashes were used to uncover additional domains that shared the same server responses and were likely controlled by the same group responsible for the $1.4 billion Bybit Heist. In this post, applying filters - such as adding a title tag filter - further narrowed down the search to reveal distinct clusters of adversary infrastructure.

- In "Hunting Pandas," we use HTTP banner pivots to identify IPs that are strongly associated with PlugX, RedDelta (Mustang Panda), and APT41.

- In "Tycoon 2FA: Analyzing and Hunting Phishing-as-a-Service Domains," we show how HTTP banner hashes can reveal large networks of domain and IP infrastructure for highly prolific phishing threat actors.

- In "Tracking a Malicious Blogspot Redirection Campaign to ApateWeb," we show a unique server configuration redirecting to Google, intended to throw threat hunters off the trail, was used to identify and track thousands of domains related to the ApateWeb redirection campaign. This post also shows how to use active scanning for additional pivots and indicator validation.

Lookalike Domain & Regex-based Pivoting

What it is

Adversaries often register domains that mimic legitimate brands or follow specific naming patterns.

Using regex (regular expressions) and lookalike searches to target common keywords (like “willo,” “hiring,” “talent,” etc.) can uncover additional infrastructure that might not have been detected by IP or DNS history alone.

How it’s used

- In “Finding Booking.com themed ClickFix domains using Validin,” a lookalike regex search is used to identify newly-created second-stage domains domains that match known adversary naming patterns.

- In “Lazarus APT: Techniques for Hunting Contagious Interview,” the post describes using custom regex searches to capture a broad set of domains whose names follow adversary-chosen pattern themed around recruitment, interviewing and cryptocurrency, adding a valuable dimension to the threat hunt.

- In “Corralling SCATTERED SPIDER with DNS History,” lookalike regex searches are suggested for tracking newly-created domains based on a consistent and predictable naming pattern used by SCATTERED SPIDER.

VALIDIN

About Validin

Validin is a global DNS and public infrastructure intelligence company leading the way to world-class proactive internet data and insights. Validin leverages a proprietary method to thoroughly map and index the public DNS space multiple times daily to build a unique, comprehensive repository of the current and historical global DNS state and dozens of unique insights.

Try our Community Edition for free

Explore Paid Editions

> Validin's comprehensive data has been **crucial** for our work at SentinelLabs, especially in tracking new malicious infrastructure quickly and efficiently. Their enterprise features **integrate seamlessly** with our internal tooling, allowing us to pivot faster and dive deeper into APT and crimeware threat activity.
> - Tom Hegel, Distinguished Threat Researcher at SentinelLabs