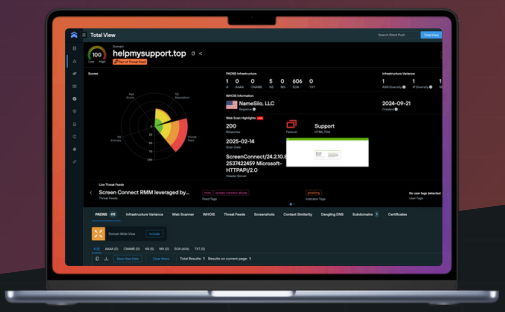
SILENT PUSH
QUERY EXAMPLES

SILENT **PUSH**

SILENT PUSH
QUERY EXAMPLES

SILENT PUSH



1. Email Addresses in WHOIS Records

The process of registering a domain typically requires an email address to be registered and associated with the WHOIS record.

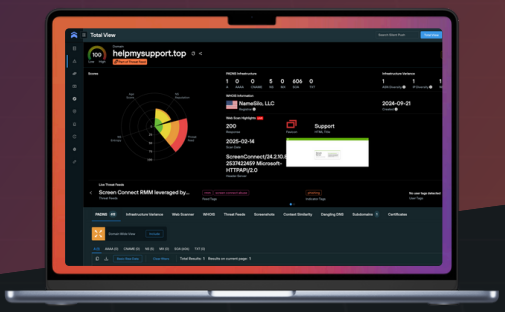
Threat actors often re-use email addresses during this WHOIS registration process, leaving behind an valuable indicator that can be used to link related domains.

Silent Push indexes these WHOIS records and exposes all fields via the WHOIS index of our Web Scanner.

A short example can be seen below, where a unique email address linked to a Lumma Stealer domain can be used to pivot to related infrastructure via re-use of the same email address.

SILENT PUSH
QUERY EXAMPLES

SILENT PUSH



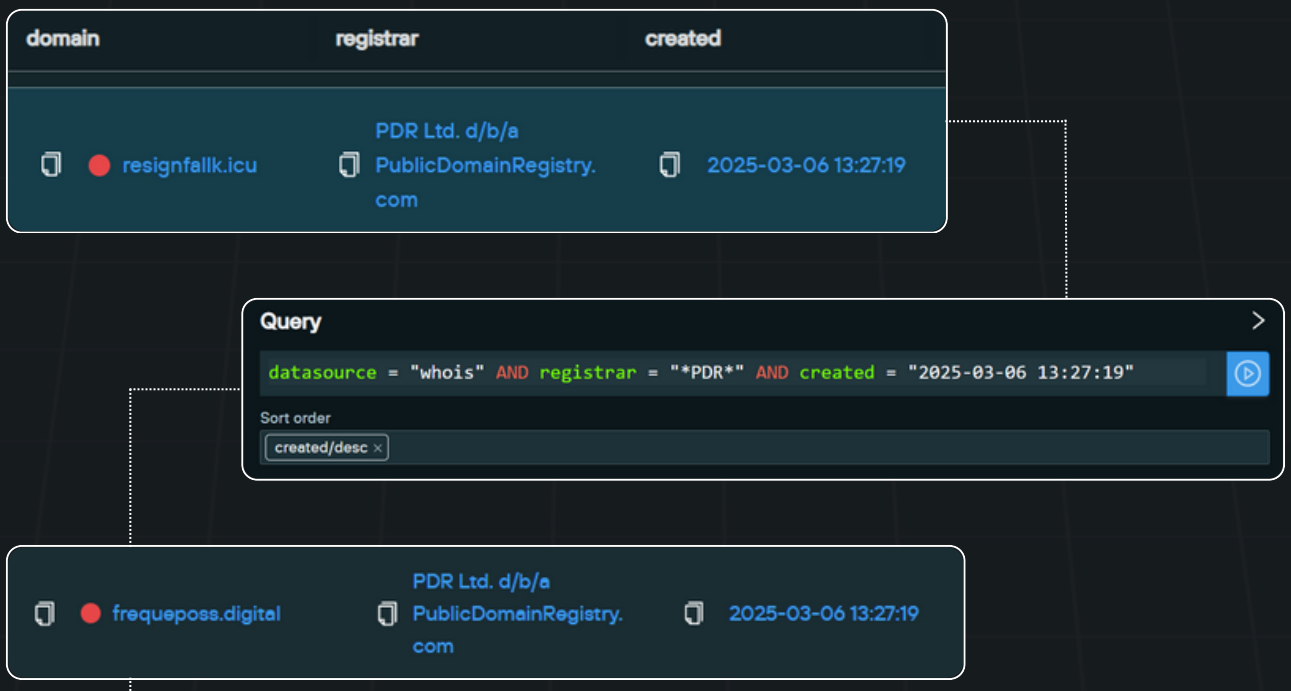
2. WHOIS Registration Times

Threat actors will often create domains in bulk by using automated scripts and tooling, this results in batches of clusters that share an exact (or near exact) creation timestamp within their respective WHOIS records.

Silent Push tracks these creation times as well as the complete WHOIS record, with all values being searchable. Searched timestamps can be exact, or a window of time can be specified to look for closely matching values.

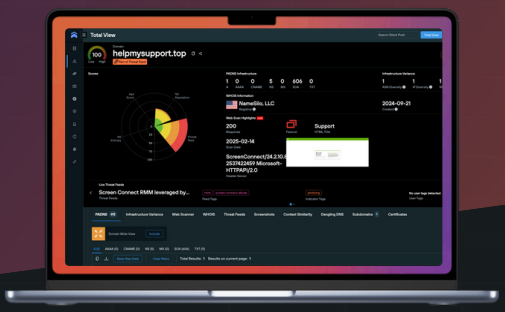
This timestamp technique is most effective when combined with a registrar.

Below we have taken a malicious domain, and discovered related infrastructure by searching for the exact same registration timestamp on the same PDR registrar.



SILENT PUSH
QUERY EXAMPLES

SILENT PUSH



3. Changes in Nameserver Infrastructure

Threat actors will often move infrastructure between nameserver providers. Although the nameservers themselves can be benign, the occurence of a change between specific nameservers can be a unique indicator used to cluster infrastructure.

Silent Push stores nameserver data for all known domains, and exposes both the records and the change as searchable metrics.

Below is an example where an actor temporarily used dyna-ns.net nameservers, before switching them to Cloudflare for the primary malicious activity. This change was recorded by Silent Push, and allowed us to cluster related domains.

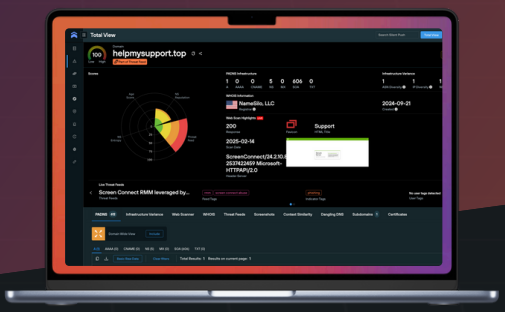
Query	Answer	First Seen	Last Seen
bikedtwittg.shop	zac.ns.cloudflare.com	2025-01-14 12:04:27	2025-04-17 04:23:59
bikedtwittg.shop	clara.ns.cloudflare.com	2025-01-14 12:04:27	2025-04-17 04:23:59
bikedtwittg.shop	ns2.dyna-ns.net	2025-01-11 18:02:39	2025-01-14 06:53:22
bikedtwittg.shop	ns1.dyna-ns.net	2025-01-11 18:02:39	2025-01-14 06:53:22

from_ns	to_ns
ns1.dyna-ns.net	clara.ns.cloudflare.com


```
change_date: "2025-01-15",
domain: "busheprettuv.shop",
newnshash: "aac34d4dadaf5d35d2a4a8925cde9335",
▾ newnsrecs: [
  "clara.ns.cloudflare.com",
  "zac.ns.cloudflare.com"
],
oldnshash: "7f812fff8c43fa008fdcb73b21df15b1",
▾ oldnsrecs: [
  "ns1.dyna-ns.net",
```

SILENT PUSH
QUERY EXAMPLES

SILENT PUSH

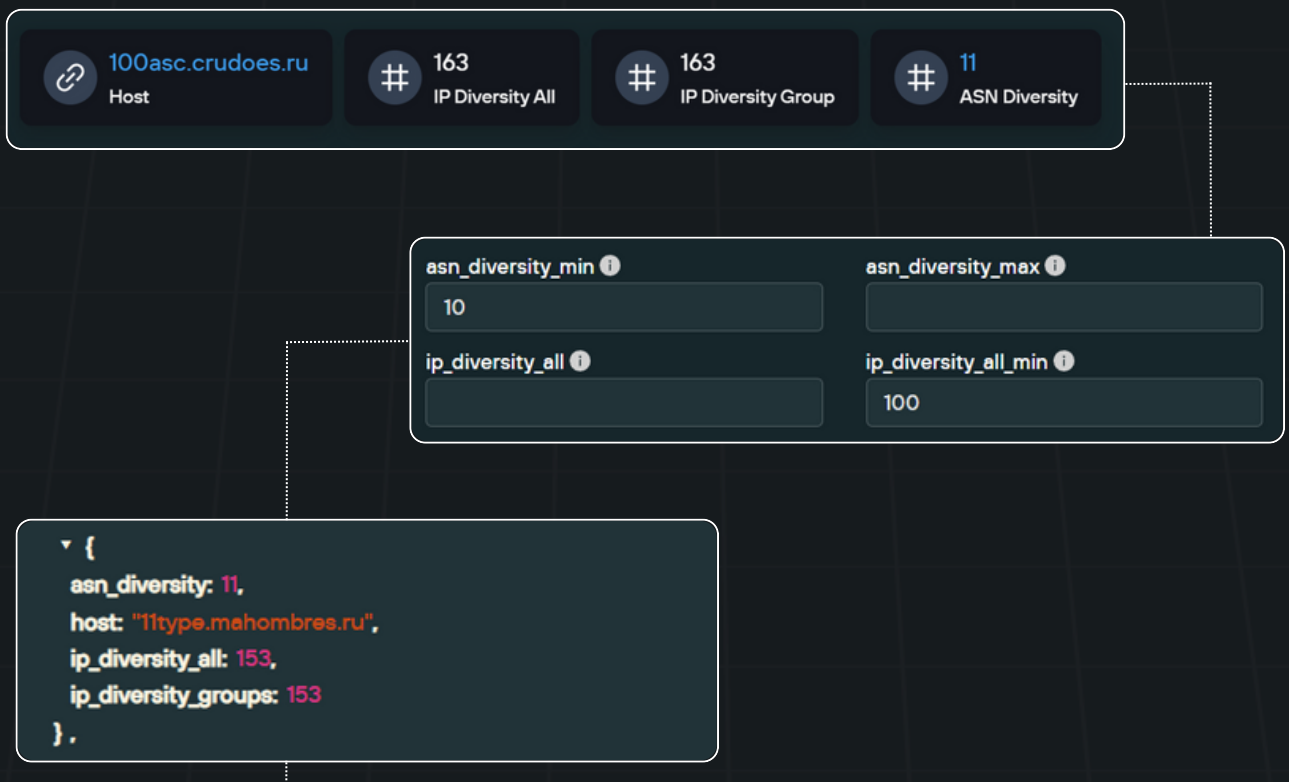


4. IP and ASN Diversity Metrics (Fast Flux)

Threat actors may utilize a technique known a “fast flux”, where a domain rapidly rotates between IP addresses to avoid traditional blocking and detection methods.

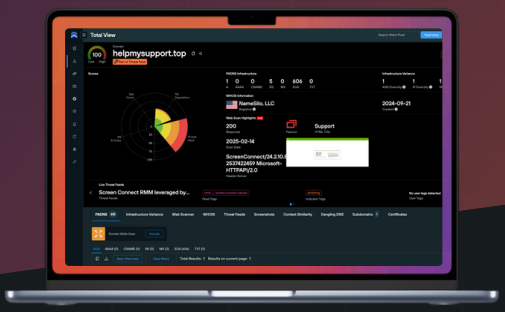
Silent Push records IPv4 and ASN changes, and creates proprietary metrics known as IP and ASN Diversity. These metrics track the number of times that a domain has changed infrastructure within a given time period.

The diversity metrics are then searchable to analysts, allowing them to discover adversary infrastructure using the fast flux method. In the case below, we have used this to link pieces of Gamaredon infrastructure via their high rotation of ASNs and IP addresses.



SILENT PUSH
QUERY EXAMPLES

SILENT PUSH



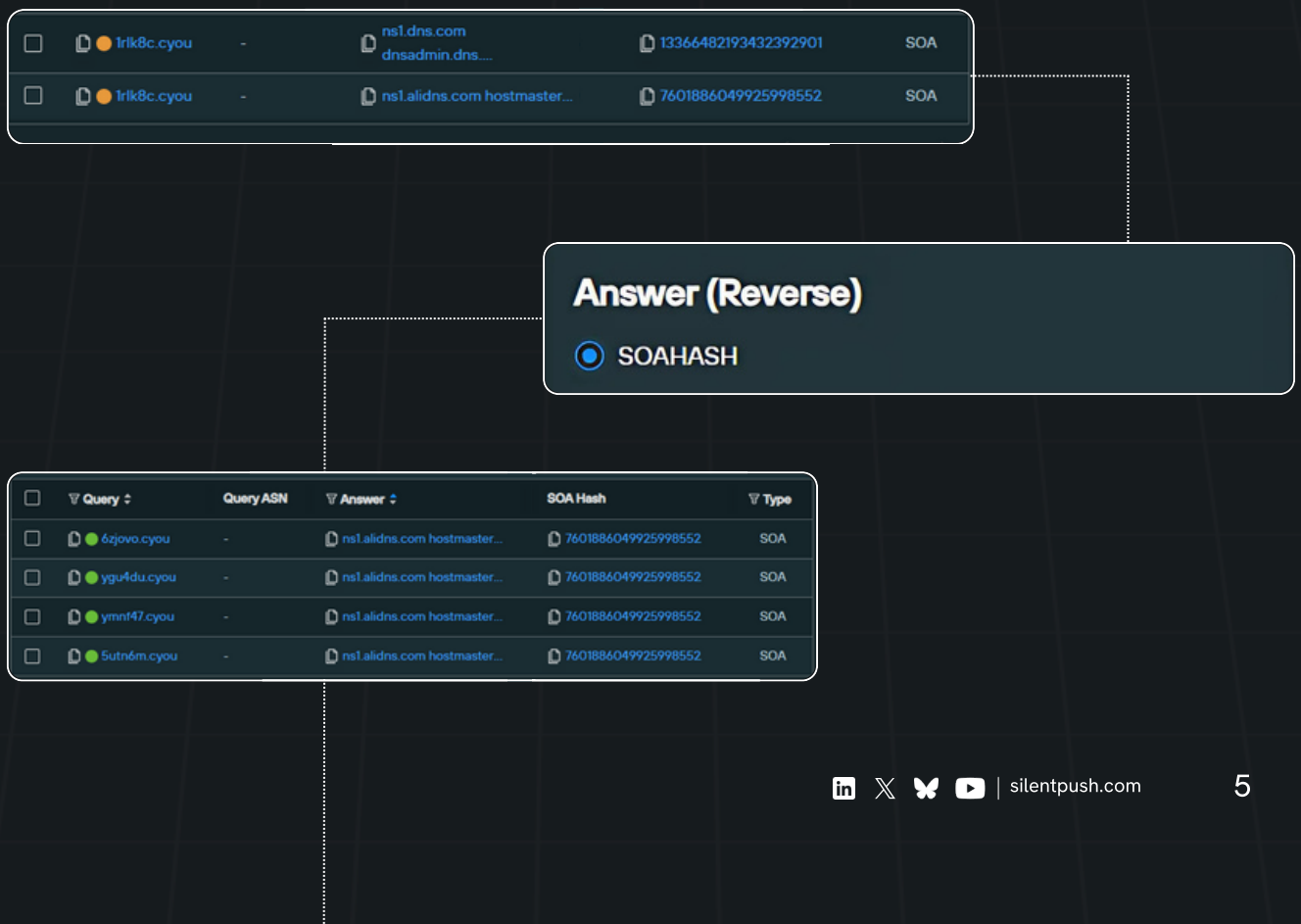
5. Start of Authority (SOA) Hashes

Start of Authority (SOA) records are created as part of the DNS registration process and are administrative records used to track zones and refresh times.

SOA records must contain a serial number and email address, which threat actors will often re-use or copy when registering multiple domains at the same time.

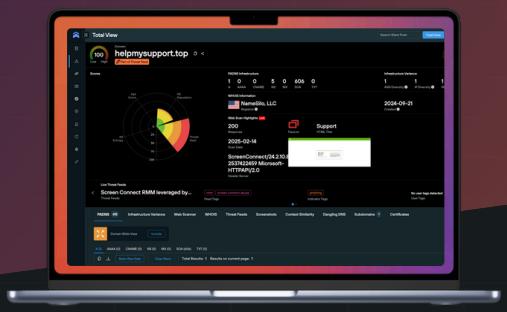
Silent Push tracks these SOA values both individually and as an entire hashed value known as the SOA Hash.

Below is an example where an SOA hash was used to link Ursnif infrastructure.



SILENT PUSH
QUERY EXAMPLES

SILENT PUSH



6. Hashes of JavaScript Files

Threat actors will often re-use page templates across infrastructure, especially on phishing and login related pages.

When an actor re-uses a template, they sometimes (unintentionally) re-use the same JavaScript libraries and files. This leaves a unique fingerprint opportunity which can be used to track infrastructure.

Silent Push indexes JavaScript files on web pages, and creates a unique fingerprint known as the Script Hash Value (SHV).

Below is an example where Silent Push was able to link a darknet (.onion) ransomware site to its clearnet IP via this SHV value.

hostname	htmltitle	body_analysis.SHV
vanhelqmjstkvlhrjwzgjzpq422iku6wlggiz5y5r3rmfdeiaj3ljaid.onion	VanHelsing Chat	c54df2a198f656ce9e2916492d

Query

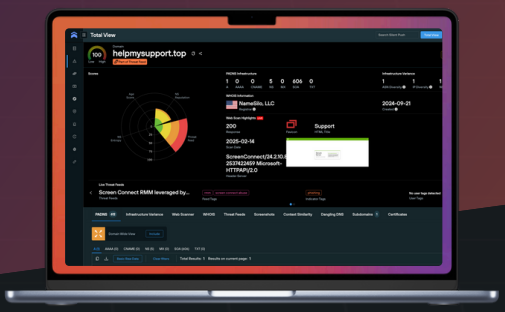
```
datasource = ["webscan", "torscan"] AND body_analysis.SHV = "c54df2a198f656ce9e2916492d"
```

Sort order: scan_date/asc

hostname	htmltitle	body_analysis.SHV
193.37.69.225	VanHelsing	c54df2a198f656ce9e2916492d

SILENT PUSH
QUERY EXAMPLES

SILENT PUSH



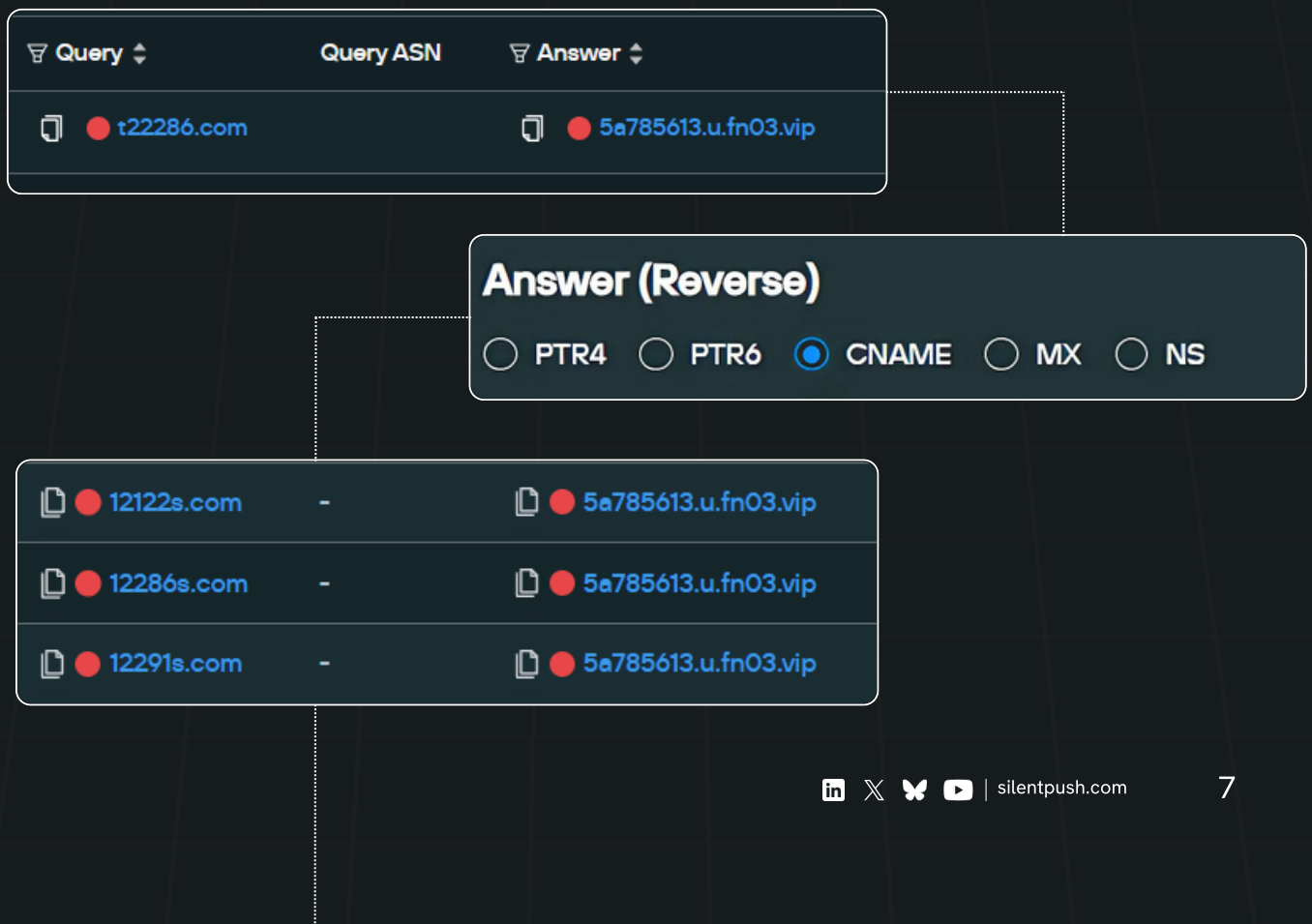
7. Reverse CNAME Lookups

CNAME records are a component of DNS infrastructure and allow a site to have an “alias” where the domain can be redirected.

Threat actors often use this to redirect multiple domains to one piece of malicious infrastructure. For an actor to do this, they must place the same CNAME record across multiple pieces of infrastructure.

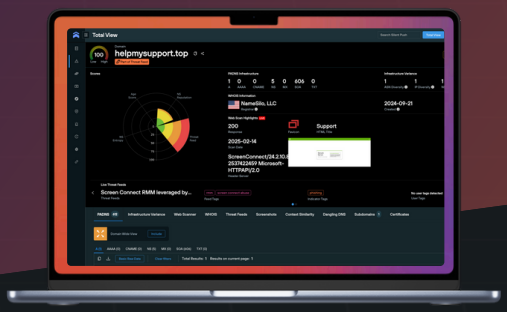
Silent Push tracks these CNAME records and allows for full lookups on the values.

Below is an example where FUNNULL domains could be identified by performing reverse lookups on CNAME values discovered in one piece of infrastructure.



SILENT PUSH
QUERY EXAMPLES

SILENT PUSH



8. Patterns in External File References

Threat actors will often compromise legitimate sites and inject their own malicious code into the legitimate page.

This often results in sites that have an externally loaded file, where that file has a unique name, or follows a naming pattern that can be captured with a regular expression.

Silent Push captures and flags these externally loaded files, and exposes them for searching via regular expressions or exact matches.

Below is an example of a legitimate site containing a reference to external malicious code. Silent Push tracked this code and was able to identify new infrastructure by applying a regular expression on the naming of the external files.

hostname	resource_url
econclubchi.org	https://skatkat.com/5r4y.js

Query

```
datasource = ["webresources"] AND resource_url ~= ".*.com\/[0-9][a-z][0-9][a-z]\.js$" AND external = "true"
```

Sort order: scan_date/asc

autura.com	https://skatkat.com/5r4y.js
sphera.com	https://jagsrus.com/5r6y.js
sphera.com	https://jagsrus.com/5r6y.js
econclubchi.org	https://skatkat.com/5r4y.js

SILENT PUSH

REGISTER FOR FREE COMMUNITY EDITION

explore.silentpush.com/register

PREEMPTIVE CYBER INTELLIGENCE WITH INDICATORS OF FUTURE ATTACK™

Silent Push provides preemptive cyber intelligence exposing threat actor infrastructure as it's being set up. Our Indicators of Future Attack™ (IOFA™) act as an early warning system to defend against threats. We go beyond stale IOCs and create a unique digital fingerprint of adversary behavior enabling you to proactively block hidden attacks before they're launched.

Get started today.

silentpush.com