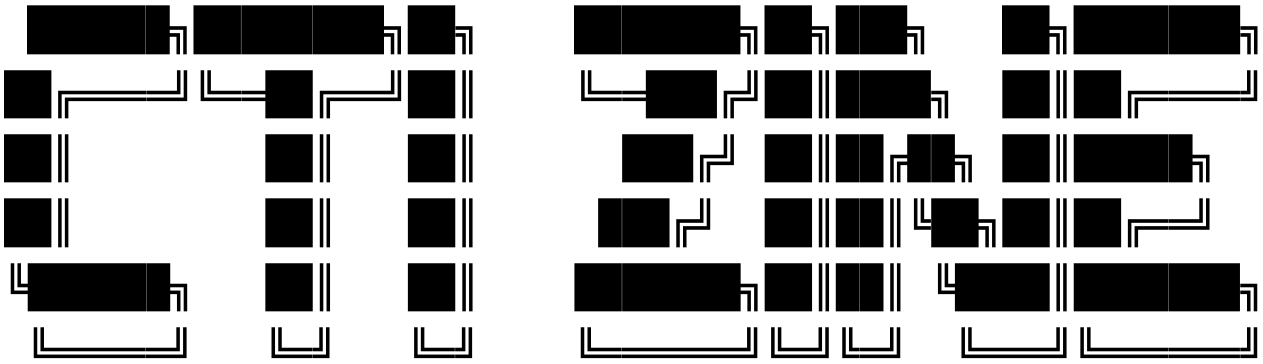


TOOL EDITION: Shodan/Censys

INTRODUCTION

Shodan and Censys are two companies that provide internet scanning services. They both scan the entire IPv4 space on the most commonly used ports and try to identify the services (websites, administrative interfaces, mail servers, etc.) running on each IP address.

The collected data is indexed and available for request. Companies can use these services to monitor their exposed infrastructure. However, attackers and defenders could also use this data to detect vulnerable infrastructure or identify malicious infrastructure that should be blocked.

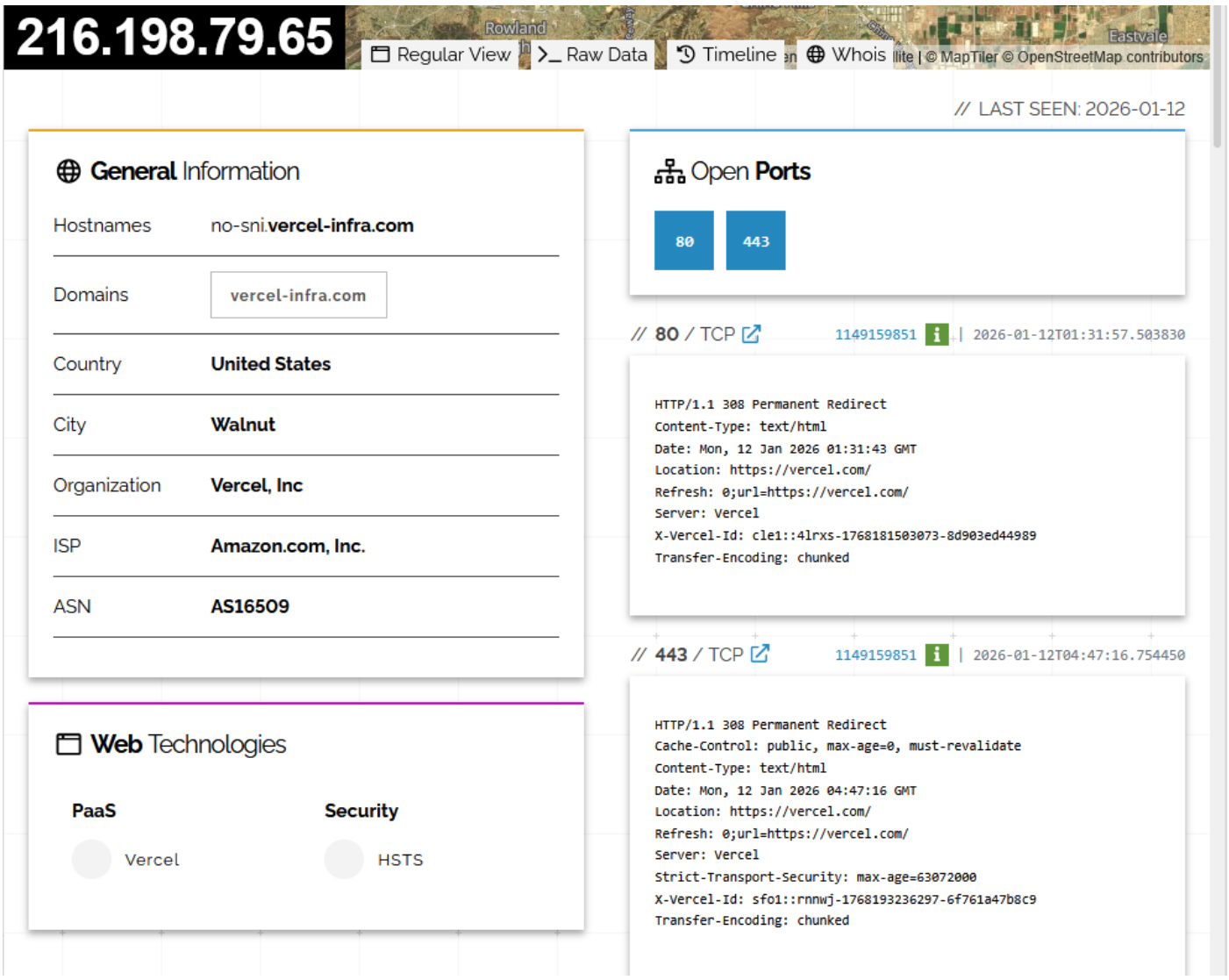
These platforms also contain data related to autonomous systems (AS) and SSL certificates, which can be found elsewhere. However, having all this data in one place allows for powerful correlations and pivots.

This Zine details some use cases of Shodan for threat intelligence. Similar services exist, such as FOFA, ZoomEye, and Onyphe, but I can’t detail them because I don’t use them. The focus is on Shodan because it offers a basic account for $5, which allows everyone to access most of its data. While this offer is interesting, the results are often less complete compared to Censys. Hence, a mapping table for Censys queries is provided at the end.

TELL ME WHAT YOU HOST, AND I WILL TELL YOU WHAT YOU ARE

IDENTIFY RUNNING SERVICES

This is the most basic use of Shodan. Search an IP, get rewarded by a web page containing all the information on it. Usually passive scanners fingerprints services such as common web frameworks, servers type, brand or product name. These fingerprints could be queried thanks to the `product` modifier.



Once you know which services are running on a host, you can use Shodan to identify the purpose of an IP address. Is it shared or dedicated hosting? Does it belong to a corporate environment or an ISP? Is the IP address likely to be compromised? The answers to these questions often depend on the context, but here are some things to consider!

IDENTIFY IP TYPE

Once you know services running on a host, you can use Shodan to determine the type of an IP address. Is it shared or dedicated hosting? Does it belong to a corporate environment or an ISP? Is the IP address likely to be compromised? The answers to these questions often depend on the context, but here are some things to consider!

Question	Infos	Comments
Shared or Dedicated?	AS Number, hosted domains, number of opened ports	The presence of many domains with no clear pattern on an hoster-related AS tends to indicate shared infrastructure. Few domains on the same IP are often seen in phishing or scams infrastructure, and could help collect indicators for a campaign.
Corporate?	domains hosted, type of services	Few services, all associated to the same domain often indicates legit small corporate infrastructure. Check

Question	Infos	Comments
		for the associated company online footprint. Exposed corporate services are usually limited to pretty common ones such HTTPS (website and software management interfaces), FTP, SMB, emails...
Compromised?	type of services	IoT, SOHO routers often expose services that allows to identify the device's models. If you see many of such items when working on a set of IP, there is a realistic probability that they are part of a botnet.
Vulnerable?	type of services, services version	Some vendors reporting vulnerability give a **Common Platform Enumeration** (CPE) number searching for it facilitate vulnerable infrastructure (`cpe` modifier). Observe banners in search of versions numbers. Some vulnerabilities might also be displayed if identified.
Honeypot?	Number of services	The presence of a large number of open ports, each with a distinct banner, likely indicates a honeypot.

PIVOTS

Pivots	Modifier	Comments
HTML Page title	`http.html_title`	Useful to identify login pages, malware panels, ransomware leak sites... Likely to generate false positive.
Favicon	`http.favicon.hash`	Useful to identify login pages, malware panels, ransomware leak sites... Likely to generate false positive.
HTML content	`http.html`	Search for specific sentences, style sheets and scripts filenames.
Domain's real IP address	`ssl.cert.subject.cn`	Searching for a domain protected by Cloudflare or similar services may reveal the de-anonymized IP address.
Multi-domains certificate	`ssl.cert.subject.cn`	Some certificates are valid for several domains. By requesting all the domains, you may find new, related domains.
Self-signed Certificate	`ssl.cert.subject.cn`	Some threat actors use self-signed certificates that exhibit distinct patterns. Search for them!

SHODAN-CENSYS EQUIVALENCE

Censys recently released a new web interface called Censys Platform, that is the successor of Censys Search. This new platform has its own query syntax.

Shodan	Censys Search (Legacy)	Censy Platform

`product`	`services.software.product`
	`services.software.vendor`
		`host.services.hardware.product`
		`host.services.software.product`
		`host.services.software.vendor`
		`web.software.product`

`cpe`	`services.software.uniform_resource_identifier`	`host.services.software.cpe` `host.services.hardware.cpe`
`has_vuln` OR `vuln`	`services.software.vulns`	`host.services.vulns`
N.A	`services.port:80 AND services.port:8081`	`services.port:80 AND services.port:8081 AND service_count:2`

Shodan	Censys Search (Legacy)	Censy Platform
	`AND service_count:2`	
`ssl.cert.subject.cn:*.top`	`services.tls.certificates.leaf_data.subject.common_name:*.top`	`host.services.cert.parsed.subject.common_name=~".*\\.top$"`
`http.title`	`services.http.response.html_title`	`host.services.http.response.html_title`
`"Location: *.org"`	`services.http.response.headers: (key: "Location" and value.headers: "http://*.org")`	`host.services.endpoints.http.headers:(key:"Location" and value:"http://*.org")`
`http.favicon.hash`	`services.http.response.favicons.shodan_hash`	`host.services.endpoints.http.favicons.hash_shodan`

Based on:

- Shodan: https://www.shodan.io/search/filters
- Censys Search: https://search.censys.io/search/definitions?resource=hosts
- Censys Platform: https://platform.censys.io/home/definitions