

Conclusion		Information Disclosure	
Type of Services	Type of Promotional Services	Vulnerable Services Version	Number of Vulnerable Services
for the associated company online footprint. Exposed corporate services are usually limited to pretty common ones such as HTTPS (website and software management interfaces), FTP, SMB, emails..	DOT, SHO routes often expose services that allows to identify the device's models. If you see many of such items when working on a set of devices, it probably means when working on a botnet.	Some vendors reporting vulnerability for it facilitate unrepeatable searching for its number (CFE). Observe banners in search of versions numbers. Some vulnerabilities might also be displayed if identified.	The presence of a large number of open ports, each with a distinct banner, likely indicates a honeypot.
for the assessment of the organization	for the assessment of the organization	Services with a honeypot	Number of honeypots

PIVOTS

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

SHODAN-CENSYS EQUIVALENCE

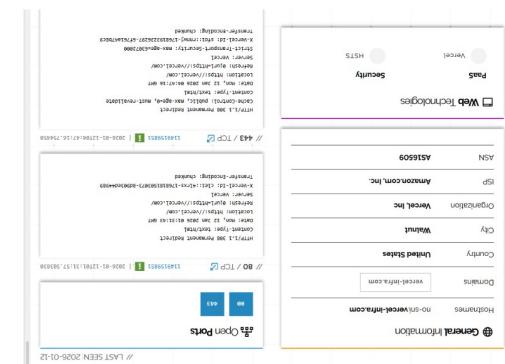
Censys recently released a new web interface called Censys Platform, that is the successor of Censys Search. This new platform has its own query syntax.

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

IDENTIFY IP TYPE

Once you know which server is dedicated hosting? Does an ISP often ask these questions often or do they consider it?

Questions	Answers
Comments	<p>The presence of many domains with no clear pattern on a single infrastructure tends to indicate shared hosting.</p> <p>Few domains on the same IP often seen in phishing or scams</p> <p>Institutional, and could help collect indicators for a campaign.</p> <p>Few services, all associated to the same domain often indicates legit ports</p> <p>number of opened ports</p> <p>hosted domains, clear pattern on many domains with no shared or AS Number.</p>
Corporate?	<p>domains hosted, few services, all associated to the same domain often indicates legitimate corporate infrastructure.</p> <p>small corporate infrastructure. Check if type of services</p>



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

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.valid.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.endpoint.http.headers:(key: "Location" and value:"http://*.org")
http.favicon.hash	services.http.response.favicons.shodan_hash	host.services.endpoint.http.favicons.hash.shodan

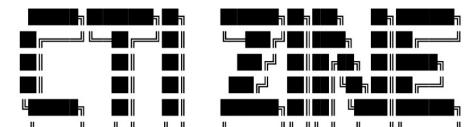
Based on

- 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>

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 infrastructures 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 between similar services exist, such as FOFA, ZOOMEYE, and OnPhrase, but I can't detail them because I don't use them. The focus is on Shodan details, 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.

INTRODUCTION



TOOL EDITION: Shodan/Censys