Practical Queries for Identifying Malware Infrastructure

embee-research.ghost.io/shodan-censys-queries/

Matthew June 7, 2023

intel

An informal page for storing Censys/Shodan queries

An informal page for storing Censys/Shodan queries that have returned interesting results.

Including examples for -

> AsyncRAT, Solarmarker, Amadey, Quasar, Laplas, Sliver, Mythic, Qakbot + more

AsyncRAT - Common x509 Certificates

Hardcoded values in x509 certificates used for TLS communication.

```
services.tls.certificates.leaf_data.subject.common_name:"AsyncRAT Server" or services.tls.certificates.leaf_data.issuer.common_name:"AsyncRAT Server"
```
(Link)

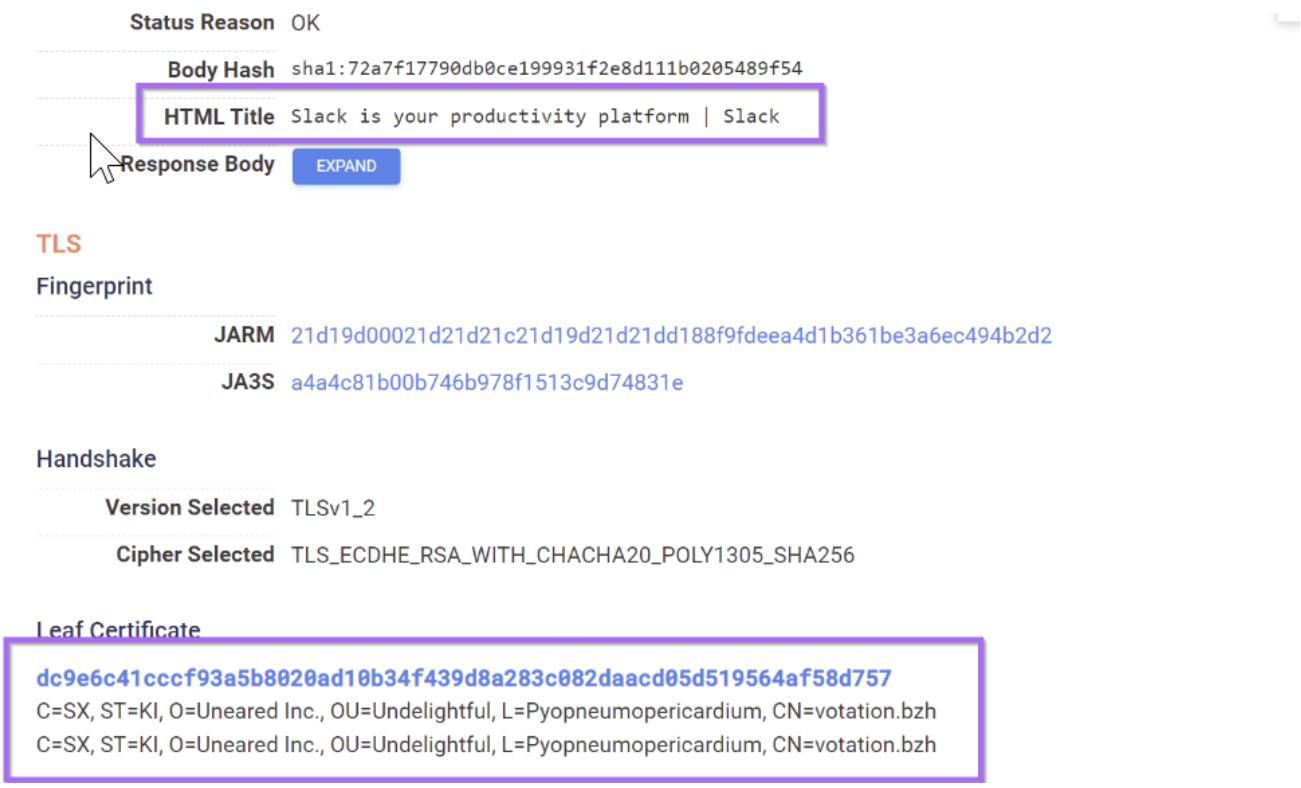
Commonalities between ssh host key and running ports. Typically only ports 22 and 80. SSH host key is the primary piece here.

```
services:(ssh.server_host_key.fingerprint_sha256 = "c655bae831ca57a857b26d76a7c98a56a65d00fdab7d234a64addf8166e3cd09" and port = 22) and services:(service_name:HTTP and port:80) and not services.port:993
```

Qakbot (Possibly Pikabot) - Masquerading as Slack

Qakbot C2's masquerading as a slack-related site. It is also possible that this is Pikabot which uses similar tactics.

```
not dns.reverse_dns.names:* and services.http.response.html_title:"Slack is your productivity platform | Slack"
```
(Link)



Cobalt Strike - Default Certificate Values

Very generic Cobalt strike indicators based on default certificate values. Likely very unsophisticated actors.

- `services.tls.certificates.leaf_data.issuer.common_name="Major Cobalt Strike"` (Link)
- `services.tls.certificates.leaf_data.issuer.organization="cobaltstrike"` (Link)
- `services.tls.certificates.leaf_data.issuer.organizational_unit="AdvancedPenTesting"` (Link)
- `services.tls.certificates.leaf_data.subject.province="Cyberspace" and services.tls.certificates.leaf_data.subject.country="Earth"` (Link)
- `ssl.cert.subject.cn:"Major Cobalt Strike"` (Link)
- `ssl.cert.issuer.cn:"Major Cobalt Strike"` (Link)

Remcos - Re-Used SSH Host Key and Usage of Hestia Control Panel

At least two of these servers are related to Remcos rat. There is a re-used ssh host key that is also related to Jupyter/Solarmarker.

```
services:(ssh.server_host_key.fingerprint_sha256 = "c655bae831ca57a857b26d76a7c98a56a65d00fdab7d234a64addf8166e3cd09" and port = 22) and  services:(http.response.html_title:hestia)
```
(Link)

Amadey Bot - Re-used Certificate Values

Re-used CN name in TLS certificates, as well as unique and re-used HTTP response body containing Russian swear words. Full Analysis Here.

- `services.tls.certificates.leaf_data.subject.common_name:"desas.digital"` (Link)
- `services.http.response.body_hash:"sha1:e084a66d16925abf43390c59d783f7a2fb49752d"`

Quasar RAT - Re-used Certificate Values

Re-used CN name used in TLS certificates. Full Analysis Here.

`services.tls.certificates.leaf_data.subject.common_name: "Quasar Server CA"` (Link)

Laplas Clipper - Re-used Certificate Values

Re-used CN name used in TLS certificates. Full Analysis here.

`services.tls.certificates.leaf_data.subject.common_name:"Laplas.app" or services.tls.certificates.leaf_data.issuer.common_name:"Laplas.app"` (Link)

Sliver C2 - Re-used Certificate Values

Re-used CN names in tls certificates. Twitter Post

`services:(tls.certificates.leaf_data.subject.common_name:multiplayer and tls.certificates.leaf_data.issuer.common_name:operators)` (Link)

Mythic C2 - Default HTML Title + Default Favicon

Default HTML Titles, favicon hash and CN name.

`(services.http.response.html_title="Mythic") or services.http.response.favicons.md5_hash="6be63470c32ef458926abb198356006c" or services.tls.certificates.leaf_data.subject.common_name="Mythic"` (Link)

Members Only Section

There are 10+ additional queries below. Consider signing up for the site to continue reading.

Signing up is free! and gives you early access to future posts and bonus content.

This post is for subscribers only

Subscribe now

Already have an account? Sign in