Threat Intelligence Query Examples - Real World Queries for Identifying Malware Infrastructure

By Matthew

Published: 2023-06-07 · Archived: 2026-04-05 12:48:17 UTC

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_da
```

(Link)

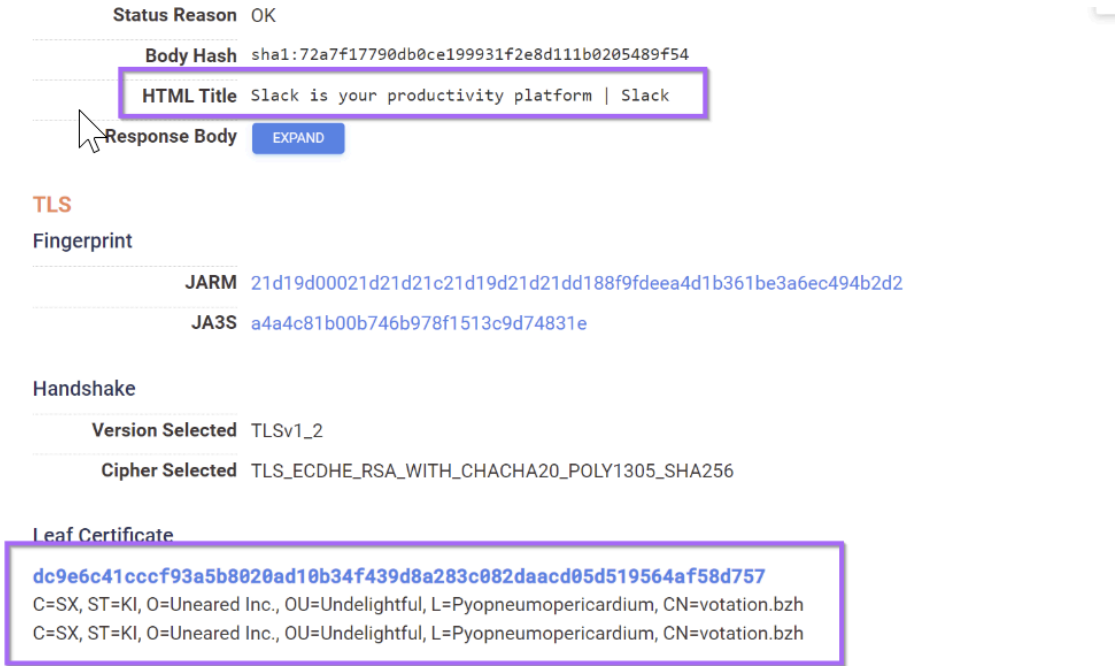
Commonalities between ssh host key and running ports. Typically only ports 22 and 80. SSH host key is the primary piece here.

```
services:(ssh.server_host_key.fingerprint_sha256 = "c655bae831ca57a857b26d76a7c98a56a65d00fdab7d234a64addf8166
```

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"
```



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 = "c655bae831ca57a857b26d76a7c98a56a65d00fdab7d234a64addf8166
```

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"
```

```
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.iss
```

- (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.comm
```

- (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="6be63470c32ef458926ab
```

- (Link)

Viper Servers - Default String + Favicon Hash

Queries based on "Viper" string in html title and response. Not 100% sure what viper is.

A lot of Viper servers seem to have cobalt strike running on alternate ports.

- `http.html_hash:-1250764086` (Link)
- `+http.title:"viper" +http.html:viper +"Content-Length: 69"` (Link)
- `services.http.response.favicons.md5_hash="a7469955bff5e489d2270d9b389064e1"` (Link)

- `services:(http.response.html_title:"Viper" and http.response.body:Viper and http.response.headers.content_length:69)` (Link)

Cobalt Strike - Ja3 + Empty Certificate Values

Overlapping ja3s and lack of issuer/common names in certificate.
Unconfirmed if all are cobalt strike but at least a few were sucessful hits.

```
services:(tls.ja3s:475c9302dc42b2751db9edcac3b74891 and tls.certificates.leaf_data.subject.common_name="" and t
```

- (Link)

Open Directories - .exe files on port 8000

Open directories residing on port 8000 and containing at least one .exe file. Reasonable number of false positives, but a lot of interesting results. eg servers containing `revshell.exe` and similar.

```
services:(http.response.html_title:"Directory Listing" and http.response.body:*.exe and port:8000) and not serv
```

Open Directories - Referencing Netcat

Open directories containing references to netcat `nc.exe`

```
services.http.response.body:"nc.exe" or services.http.response.body:"ncat.exe"
```

Open Directories - Referencing Common Attack Tooling

Open Directories Containing references to attack tooling. `procdump.exe` , `nc.exe` , `ngrok.exe` etc.

```
services.http.response.body:"procdump.exe" or services.http.response.body:"nc.exe" or services.http.response.bo
```

Open Directories - Referencing Powershell Scripts

Open directories containing a file with `.ps1` extension. Most of these contain suspicious Powershell scripts.

- (Any .ps1 script)

```
services:(http.response.body:*.ps1 and http.response.html_title:"Directory Listing" and banner:Python)
```

```
services:(http.response.html_title:"Directory Listing" and http.response.body:?.ps1)
```

(Single char .ps1 name)

Open Directories - Referencing Anydesk Remote Access Tooling

Open directories with references to Anydesk (remote access tooling). Typically in the form of `anydesk.exe` or `anydesk.bat` and coupled with other suspicious files.

```
services:((http.response.body:anydesk.*) and http.response.html_title:"Directory listing")
```

Open Directories - Short Executable Names

Open directories containing `.exe` files with single or double character exe names.

```
services:(http.response.html_title:"Directory Listing" and http.response.body:??.exe)
```

```
services:(http.response.html_title:"Directory Listing" and http.response.body:?.exe)
```

Open Directories - Single Char Batch Scripts

Suspicious single-character `.bat` files inside of open directories. eg `1.bat`

```
services:(http.response.html_title:"Directory Listing" and http.response.body:?.bat)
```

Open Directories - Executable and Script Files

Open directories containing a `.exe` file and at least one of `.vbs,.ps1,.bat`. Mostly malicious.

```
services:(http.response.body:.exe and (http.response.body:.vbs or http.response.body:ps1 or http.response.body
```

ProtonVPN Behind Dynamic DNS - Observed in AsyncRAT

Dynamic dns resolving to protonVPN instances. Observed with AsyncRAT `fresh03.ddns[.net]` resolving to (VPN) `46.166.182[.]34`. Difficult to confirm the nature of results as minimal services are running and port forwarding likely used.

```
services.tls.certificates.leaf_data.subject.common_name:*protonvpn.net and dns.names:*.ddns.net
```

WhiteSnake Stealer - Common Patterns in HTTP Response

Common patterns in http responses for WhiteSnake stealer control panels.
Original IP that inspired query is from RussianPanda's blog.

```
services:(http.response.body:DutchCoders and http.response.body:keybase and http.response.body:Virustotal)
```

Sign up for Embee Research

Malware Analysis and Threat Intelligence Research

No spam. Unsubscribe anytime.
