

Practical Queries for Malware Infrastructure - Part 3 (Advanced Examples)

By Matthew

Published: 2023-11-22 · Archived: 2026-04-05 17:54:12 UTC

[Threat Intelligence Guides](#)

More interesting and practical queries for identifying malware infrastructure.



Nov 22, 2023 - 3 min read

Practical and real-world examples of queries for identifying malware infrastructure. The primary tooling used is [Censys.io](#).

- Redline Stealer
- Qakbot
- NJRat
- Remcos
- BianLian Go Trojan
- XTreme RAT
- SuperShell Botnet

Qakbot Command and Control Servers

Censys [Link](#)

- Empty Banner Produces Unique Hash
- Particular Structure to TLS certificates
- Qakbot server typically on port 443,993 or 995
- Server name all lower case letters with no subdomain
- No identified operating system on servers
- Same ja3s across malicious servers.

services:

```
(banner_hashes="sha256:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"  
and tls.certificates.leaf_data.subject_dn:/C=[^,]+, OU=[^,]+, CN=[^,]+/ and
```

tls.certificates.leaf_data.issuer_dn:/C=[^,]+, ST=[^,]+, L=[^,]+, O=[^,]+, CN=[^,]+/ and (port:443 or port:993 or port:995) and services.tls.certificates.leaf_data.names:/[a-z]{3,15}.[a-z]{2,5}/ and not operating_system.product:* and services.tls.ja3s: 475c9302dc42b2751db9edcac3b74891

UNKNOWN 993/TCP

11/21/2023 10:20 UTC

Details

[VIEW ALL DATA](#)

TLS

Handshake

Version Selected TLSv1_3

Cipher Selected TLS_CHACHA20_POLY1305_SHA256

Certificate

Fingerprint 89fd77cb3cf2794e24b3390797716fc36ba10d521631a190e4fc5b15b2fffb19

Subject C=DE, OU=Reoztron, CN=tioewe.info

Issuer C=DE, ST=OS, L=Knuwayfal Aod, O=Ogebvl Qeexta Yjyab, CN=tioewe.info

Names tioewe.info

Fingerprint

JA3S 475c9302dc42b2751db9edcac3b74891

Comments are only visible to members of **Embee Research (Embee Research)**.

BianLian GO Trojan

[Censys Link](#)

- Empty Banner on Main Service
- Very particular structure to certificate names (both Issuer and Subject) eg C=zHNWYSaBumxjPKPY, O=KcUnN1CdTgE0xr6h, OU=FtVXN2EyNbwLXUP8
- Service always unidentified, presumably due to lack of headers.

services:

(banner_hashes="sha256:e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855" and tls.certificates.leaf_data.subject_dn=/C=[^,]{10,20}, O=[^,]{10,20}, OU=[^,]{10,20}/ and tls.certificates.leaf_data.issuer_dn=/C=[^,]{10,20}, O=[^,]{10,20}, OU=[^,]{10,20}/ and service_name:UNKNOWN)

UNKNOWN 5000/TCP

11/21/2023 13:56 UTC

Software

linux

[VIEW ALL DATA](#)

Details

TLS

Handshake

Version Selected TLSv1_3

Cipher Selected TLS_CHACHA20_POLY1305_SHA256

Certificate

Fingerprint [151a9e8de9ef3c911bebdafd543df01ee0f3487932420b4b11d71ae96c076319](#)

Subject C=rp0RlbtOsZEhtcc, O=HAbwMle0SgDNPj55, OU=2qdRm8Ff00K5hvus

Issuer C=7Gx5UVtWxAPfFde4, O=MgTfygZBZdcRjH8X, OU=6uNpu3StYxYJiP5G

Fingerprint

JARM [3fd21b20d3fd3fd21c43d21b21b43d50c8594d0a42335f3aca21f0ce31ac7c](#)

JA3S [475c9302dc42b2751db9edcac3b74891](#)

NJRat/Xworm Botnet Servers

[Censys Link](#)

- Extremely high number of running services (typically 200-400)
- At least one dns.name pointing to an ngrok address
- Most ports running GStreamer Service

service_count:[200 to 2000] and dns.names:ngrok and services.banner:GStreamer

Basic Information

Reverse DNS ec2-3-124-142-205.eu-central-1.compute.amazonaws.com

Forward DNS [bdfj6kym.cname.eu.ngrok.io](#), [beta.capisco.ai](#), [edricula.education.eu.ngrok.io](#), [ngrok.jaden.bio](#), [ngrok.dougs.dev](#), ...

Routing [3.124.0.0/14](#) via [AMAZON-02, US \(AS16509\)](#)

Services (319) [80/UNKNOWN](#), [443/UNKNOWN](#), [10000/SSH](#), [10008/HTTP](#), [10010/HTTP](#), [10011/HTTP](#), [10013/UNKNOWN](#), [10024/SSH](#), [10033/UNKNOWN](#), [10034/HTTP](#), [10037/HTTP](#), [10038/UNKNOWN](#), [10040/HTTP](#), [10043/UNKNOWN](#), [10044/UNKNOWN](#), [10045/HTTP](#), [10047/SSH](#), [10048/HTTP](#), [10072/SSH](#), [10080/HTTP](#), [10107/HTTP](#), [10264/RTSP](#), [10305/HTTP](#), [10306/HTTP](#), [10368/SSH](#), [10475/HTTP](#), [10489/HTTP](#), [10522/MYSQL](#), [10563/HTTP](#), [10596/HTTP](#), ...

Labels [TRUNCATED](#)

Redline Stealer C2

[Censys Link](#)

- Initial [Redline stealer c2](#) on 77.91.124[.]86:19084
- [Running 3 services](#), DNS and 2 Valve Related services.
- Reverse DNS pointing to a Russian VPN Service
- [Searching](#) on DNS Forwarding + .ru dns + Valve Service + 3 total services results in 18 servers with 3 marked as known malware.
- Other 15 results are "clean", but may be reserved for later malicious use.

services.dns.server_type="FORWARDING" and dns.reverse_dns.names:*.ru and services.extended_service_name="VALVE" and service_count:3

Remcos C2 Servers, Overlap with other RAT Families

[Censys Link](#)

- Empty Banner Produces Unique-ish hash value
- Same Jarm fingerprint across services
- Same Ja3s
- Almost always on port 2404

services:

(banner_hashes="sha256:e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855" and jarm.fingerprint="0000000000000000041d41d0000001798d6156df422564fb9b667b7418e4c" and port:2404 and tls.ja3s: eb1d94daa7e0344597e756a1fb6e7054)

UNKNOWN 2404/TCP

11/20/2023 23:40 UTC

Software

🔍 microsoft windows

[VIEW ALL DATA](#)

Details

TLS

Handshake

Version Selected TLSv1_3

Cipher Selected TLS_AES_128_GCM_SHA256

Certificate

Fingerprint bb11afa9b4abcb5ce75578122560a413bc45659413a0959ae53d44c8580a0de1

Subject

Issuer

Fingerprint

JARM 0000000000000000041d41d0000001798d6156df422564fb9b667b7418e4c

JA3S eb1d94daa7e0344597e756a1fb6e7054

XTreme RAT

[Censys Link](#)

- Banner is a single 0xAD character
- Always running on port 10001

services.banner_hashes="sha256:22adaf058a2cb668b15cb4c1f30e7cc720bbe38c146544169db35fbf630389c4"
and services.port:10001

UNKNOWN 10001/TCP 11/21/2023 15:06 UTC

Software [VIEW ALL DATA](#)

linux

Details

Banner (Hex)
00000000: ad | . |

SuperShell BotNet

[Censys Link](#)

- Presence of "Supershell" in html title
- re-used favicon across panels

services.http.response.html_title:"Supershell" or
services.http.response.favicons.md5_hash="cb183a53ebfc2b61b3968c9d4aa4b14a"

HTTP 8888/TCP 11/21/2023 22:25 UTC

JQUERY LOGIN PAGE

Software [VIEW ALL DATA](#) [GO](#)

nginx 1.18.0

Details

http://121.5.109.219:8888/supershell/login

Status 200 OK

Body Hash sha1:c023c2f42e6fa22f6b0f5284f2c24d8abcef6191

HTML Title Supershell - 登录

Response Body [EXPAND](#)

Sign up for Embee Research

Malware Analysis, Detection and Threat Intelligence

No spam. Unsubscribe anytime.

Source: <https://embeerresearch.io/practical-queries-for-malware-infrastructure-part-3/>