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

By Matthew

Published: 2023-11-22 · Archived: 2026-04-05 17:03:56 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

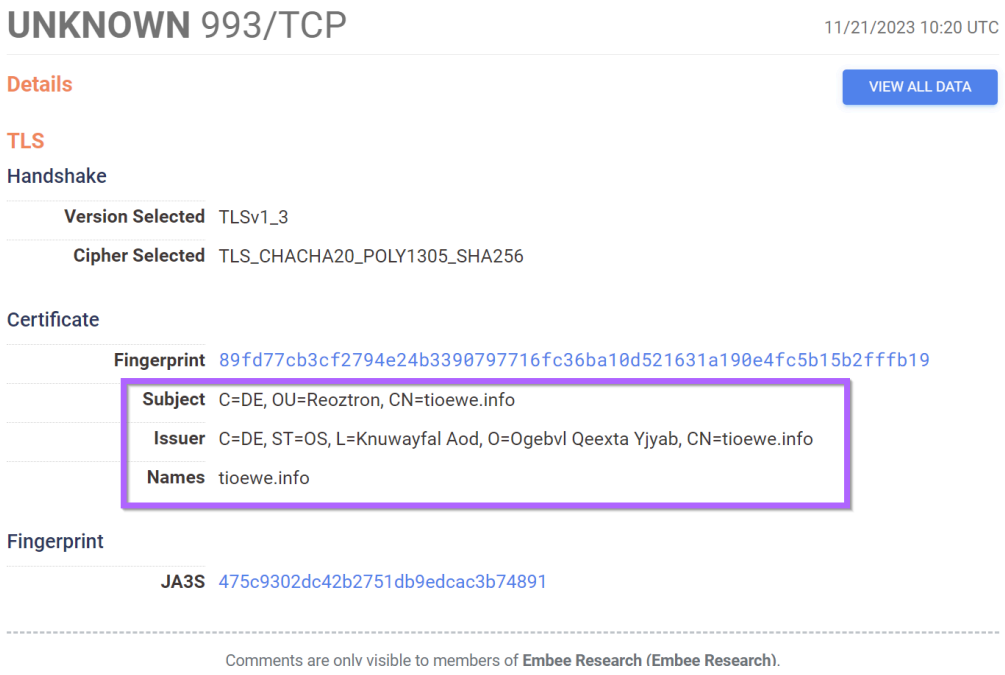
## Qakbot Command and Control Servers

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

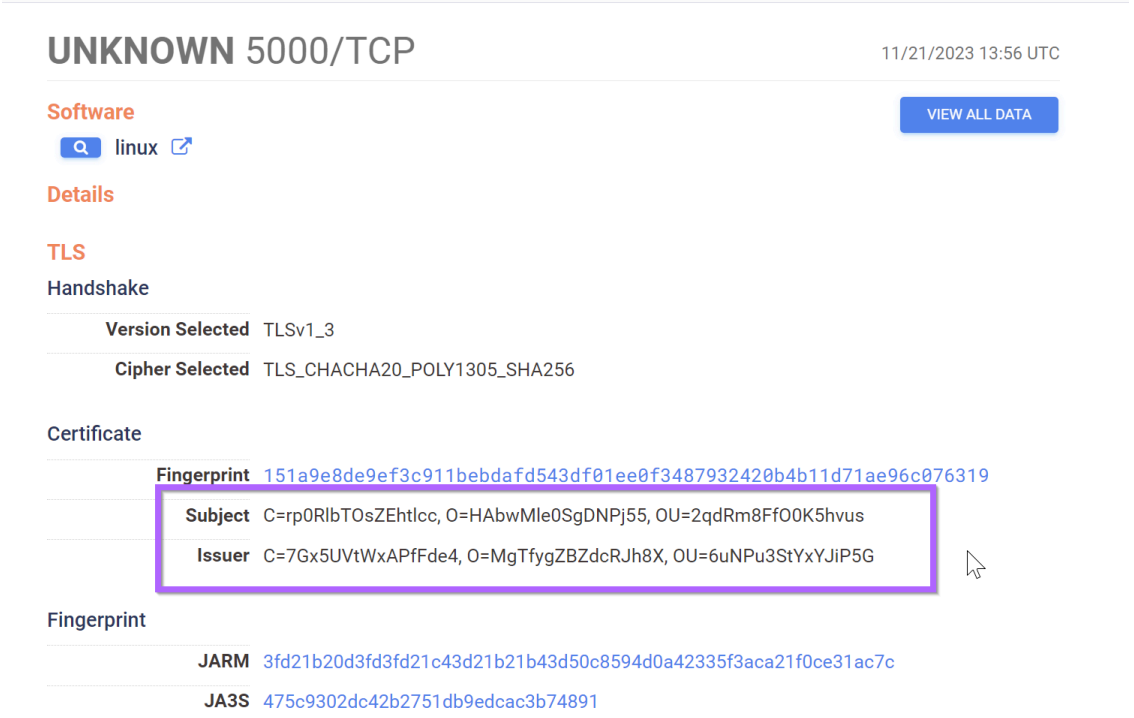



## BianLian GO Trojan

[Censys Link]

- Empty Banner on Main Service
- Very particular structure to certificate names (both Issuer and Subject) eg `C=zHNWYSaBumxjPKPY, O=KcUnN1CdTgEOxr6h, OU=FtVXN2EyNbwlXUP8`
- Service always unidentifed, presumably due to lack of headers.

> services: (banner_hashes="sha256:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855" 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)

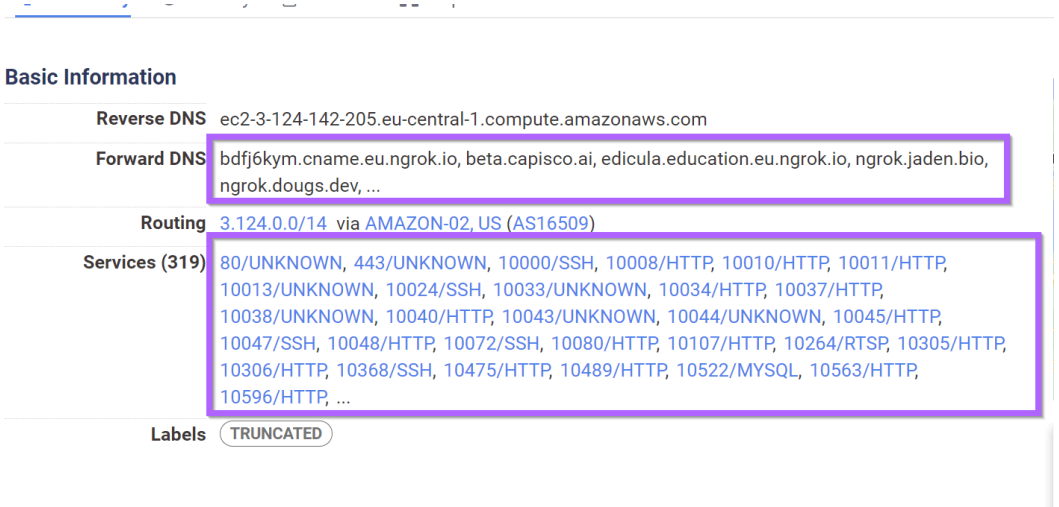



## NJRat/Xworm Botnet Servers

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




## 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.

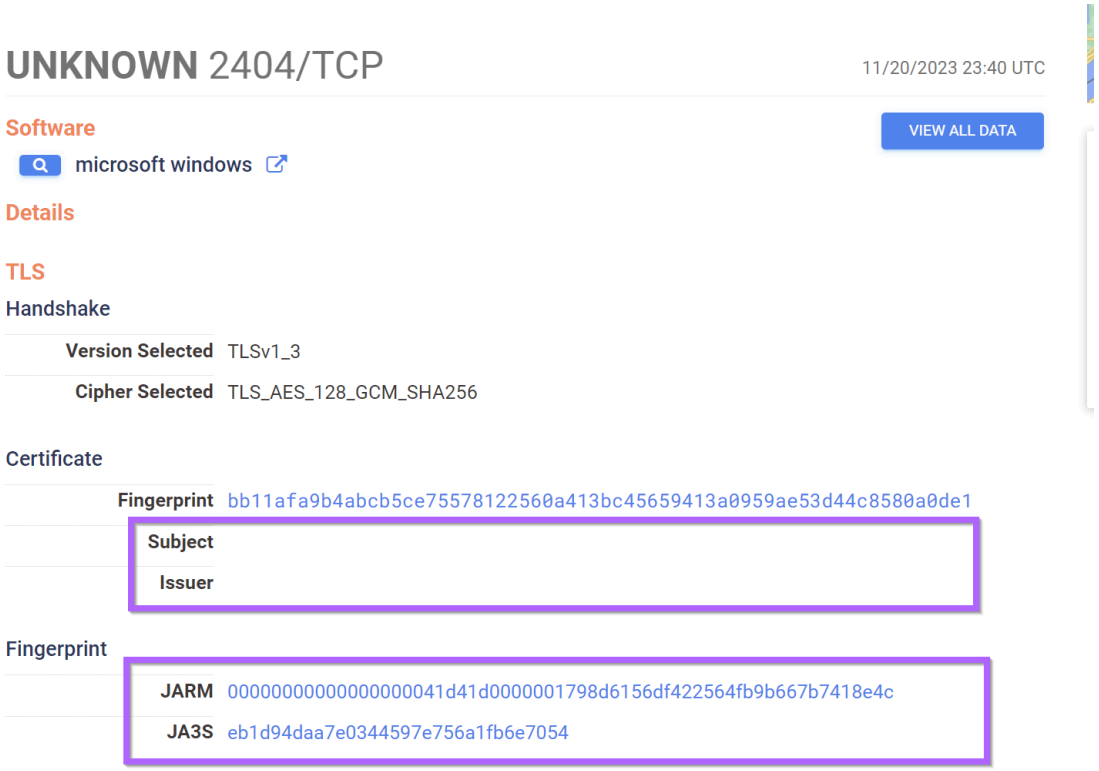
> services.dns.server_type="FORWARDING" and dns.reverse_dns.names:*.ru and services.extended_service_name="VALVE" and service_count:3

## 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:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855" and jarm.fingerprint="00000000000000000041d41d0000001798d6156df422564fb9b667b7418e4c" and port:2404 and tls.ja3s: eb1d94daa7e0344597e756a1fb6e7054)

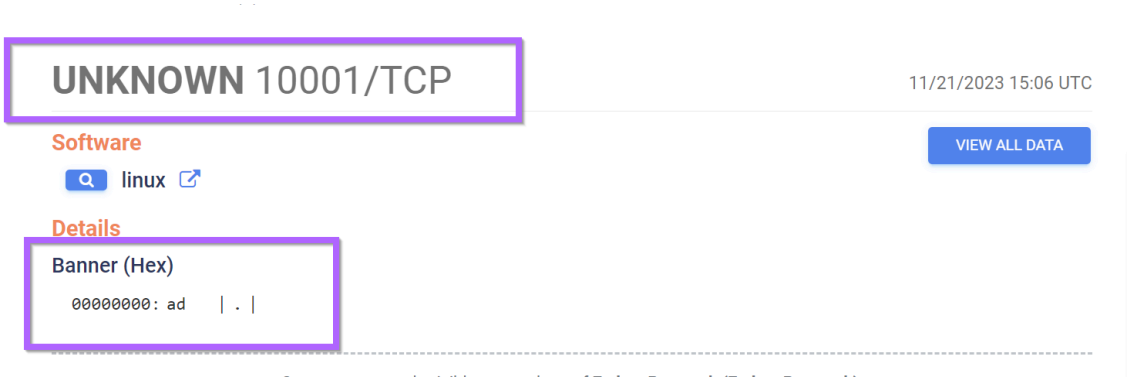



## XTreme RAT

Censys Link

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

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

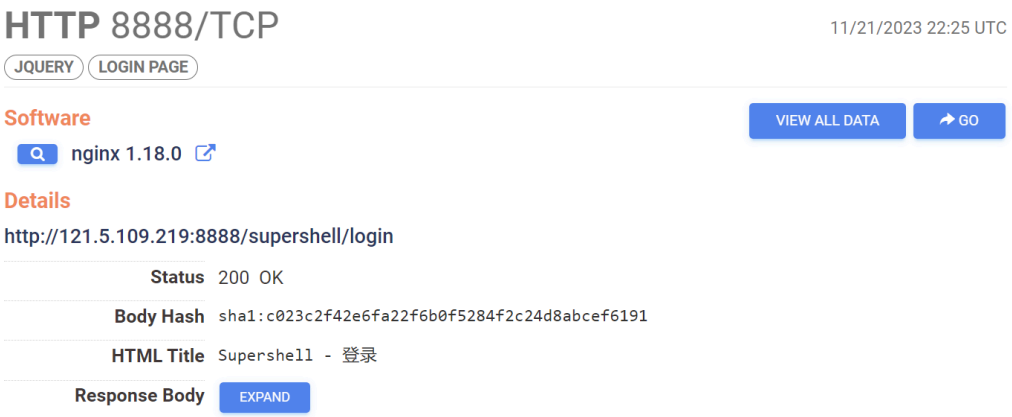



## SuperShell BotNet

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"




## Sign up for Embee Research

Malware Analysis, Detection and Threat Intelligence

No spam. Unsubscribe anytime.

---