

Will the Real Volt Typhoon Please Stand Up?

 censys.com/will-the-real-volt-typhoon-please-stand-up/

One of the more powerful things you can do using Censys is track how a threat actor's infrastructure changes over time or in response to external events.

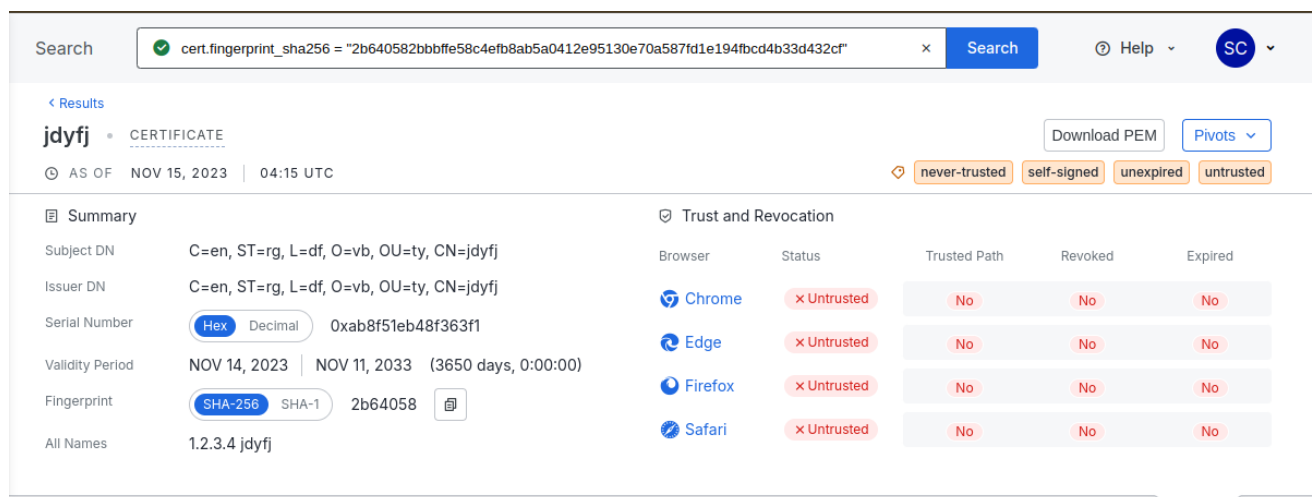
In December 2023, the US Federal Bureau of Investigation (FBI) conducted a court-authorized disruption of the KV Botnet, by running a remote uninstall of infected systems in the United States. The KV Botnet is attributed to Volt Typhoon, a threat group originating from the People's Republic of China (PRC) with a historical focus on critical infrastructure. While this disruption did not impact control infrastructure of the botnet, mass removal of bots is likely a way to spur a reaction from botnet administrators.

Despite both technical exposure by researchers and law enforcement disruption, this infrastructure has remained uncharacteristically consistent, only changing hosting providers. Given the contrasting high level of sophistication between Volt Typhoon's activity within target organizations and their proxy network, it is possible the KV Botnet is operated by a party other than Volt Typhoon.

Based on Censys scanning and indicators publicly reported by Lumen, we were able to map control infrastructure for KV Botnet, specifically the JDY cluster, through 2024.

2024 Activity

The JDY cluster was first detailed by Lumen in 2023 and is believed to target Cisco RV320/RC325 routers for botnet propagation. On 14 November 2023, infected systems from this cluster were seen communicating with new control servers with a different certificate containing "jdyfj", shown below:



Search: Search

Results: **jdyfj** - CERTIFICATE

AS OF: NOV 15, 2023 | 04:15 UTC

never-trusted self-signed unexpired untrusted

Download PEM Pivots

| Summary | | Trust and Revocation | | | | |
|-----------------|--|----------------------|-------------|--------------|---------|---------|
| Field | Value | Browser | Status | Trusted Path | Revoked | Expired |
| Subject DN | C=en, ST=rg, L=df, O=vb, OU=ty, CN=jdyfj | Chrome | ✗ Untrusted | No | No | No |
| Issuer DN | C=en, ST=rg, L=df, O=vb, OU=ty, CN=jdyfj | Edge | ✗ Untrusted | No | No | No |
| Serial Number | Hex: 0xab8f51eb48f363f1 | Firefox | ✗ Untrusted | No | No | No |
| Validity Period | NOV 14, 2023 NOV 11, 2033 (3650 days, 0:00:00) | Safari | ✗ Untrusted | No | No | No |
| Fingerprint | SHA-256: 2b64058 | | | | | |
| All Names | 1.2.3.4 jdyfj | | | | | |

Example JDY C2 Server with a New Certificate Variant

Historical records for this certificate show the following hosts that may have previously been used by this actor:

| IP Address | Certificate First Seen | Certificate Last Seen | ASN |
|-------------------------|------------------------|-----------------------|--------------------------------|
| <u>45.32.174[.]131</u> | 28 December 2023 | 23 April 2024 | AS20473 – CHOOPA, US |
| <u>45.63.60[.]39</u> | 28 December 2023 | 24 April 2024 | AS20473 – CHOOPA, US |
| <u>159.203.113[.]25</u> | 18 November 2023 | 27 December 2023 | AS14061 – DIGITALOCEAN-ASN, US |
| <u>174.138.56[.]21</u> | 17 November 2023 | 2 December 2023 | AS14061 – DIGITALOCEAN-ASN, US |
| <u>108.61.132[.]157</u> | 15 November 2023 | 18 November 2023 | AS20473 – CHOOPA, US |
| <u>144.202.49[.]189</u> | 15 November 2023 | 27 December 2023 | AS20473 – CHOOPA, US |

Censys's scans indicate that, following law enforcement action, 45.32.174[.]13 and 45.63.60[.]39 (highlighted in yellow above) were both likely brought online in response to disruption efforts. In April 2024, these servers were likely migrated to the infrastructure currently hosting this certificate. Notably, the current hosts have used different hosting providers each time servers have moved, shown in the table above, potentially to reduce impact of future disruption efforts.

The Censys research team has identified three hosts currently leveraging this certificate (SHA256 Hash:

2b640582bbbffe58c4efb8ab5a0412e95130e70a587fd1e194fbcd4b33d432cf):

| IP Address | Certificate First seen | Certificate Last Seen | ASN |
|--|------------------------|-----------------------|--|
| <u>2.58.15[.]30</u> | 16 April 2024 | 6 January 2025 | AS199959 – CrownCloud, AU |
| <u>66.85.27[.]190</u> | 16 April 2024 | 7 January 2025 | AS8100 – Quadranet |
| <u>172.233.211[.]226</u> | 25 November 2024 | 7 January 2025 | AS63949 – AKAMAI-LINODE-AP Akamai Connected Cloud, SG |

Thoughts on attribution

[Microsoft's initial public report](#) describes Volt Typhoon as a technically sophisticated threat actor, operating with a minimal toolkit and focus on stealth. However, following both technical exposure by researchers and disruption from law enforcement, operators of the KV Botnet have not taken any meaningful action to conceal their control infrastructure beyond migrating to new hosting providers. This notable difference calls into question the nature of the relationship between Volt Typhoon activity against target networks and the KV Botnet.

[Back to resource hub](#) ➤