

AsyncRAT Family Threat Overview

By Kate Lake

Published: 2026-06-26 · Archived: 2026-07-29 02:00:54 UTC

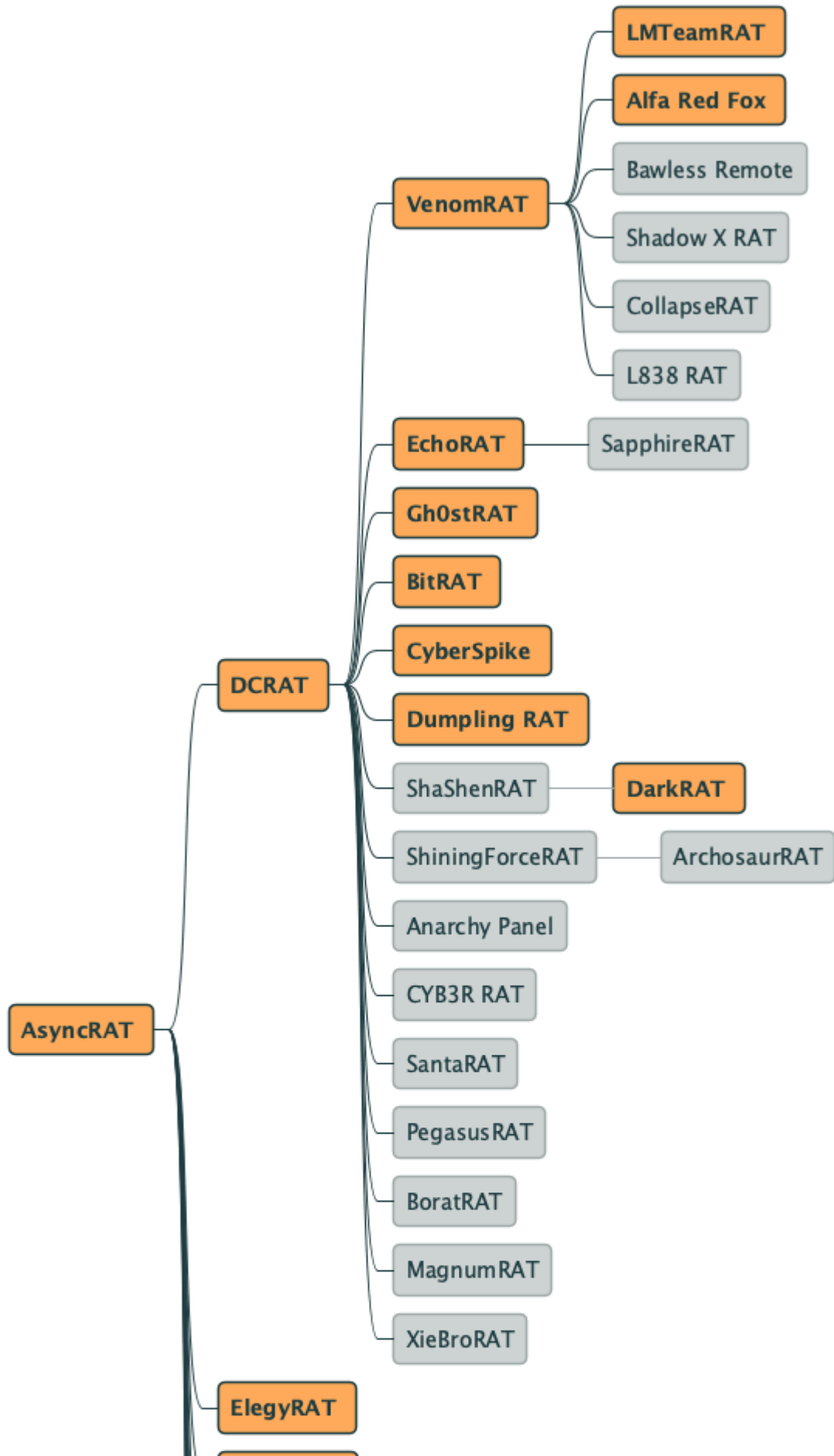
AsyncRAT is a family of open-source Windows remote access trojans (RATs): an original codebase that has been forked repeatedly into dozens of descendant malware families. Its most prolific descendant, DCRAT (also known as DarkCrystal RAT), spawned a second generation of forks of its own. Censys searches on 16 June 2026 confirmed live command-and-control (C2) infrastructure for more than a dozen variants, eight of which are now tracked under their own identifiers (THREAT-245 through THREAT-252).

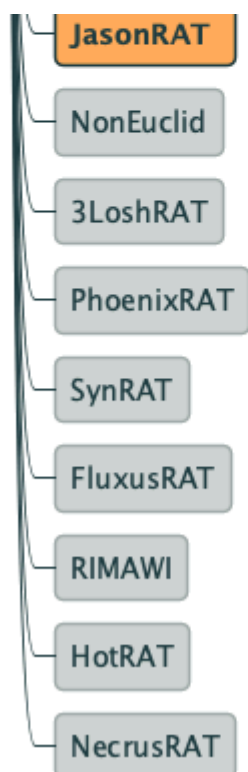
These forks share more than code. Each new fork tends to inherit the parent's TLS certificate structure and rarely changes it, and that inheritance is the family's central weakness for defenders. We assess the certificate pattern `<Name> By <author>, L=SH, C=CN 0=` carried down from DCRAT, is the strongest single signal for identifying this malware across forks, regardless of which variant is deployed.

Key Judgments

- The family has evolved over time through development forks. AsyncRAT, DCRAT, and VenomRAT each spawned multiple downstream RATs, and most forks reuse the parent's certificate fields rather than rebranding them.
- Certificate metadata is the most reliable detection surface. Variant names appear in certificate subject or issuer distinguished names, and the `L=SH, C=CN` plus `0=* By *` combination on non-standard ports flags the family even when a fork is otherwise unbranded.
- Deployment is uneven across the tree. A few variants run dozens of live C2 hosts; many named forks run none that we could confirm.
- Name-based hunting cuts both ways. Distinctive variant names produce clean queries, while generic ones collide with legitimate organizations and self-signed machine certificates.
- Censys has mapped the AsyncRAT lineage across roughly 40 named variants, 13 of them confirmed with live infrastructure.

The Family and Its Lineage





Pictured left is the AsyncRAT family tree, showing AsyncRAT at the root with its DCRAT and VenomRAT descendant branches. Orange nodes are variants with confirmed Censys infrastructure; gray nodes are forks we have not yet observed live. Confirmed variants are ordered first within each branch.

AsyncRAT was first published on GitHub in January 2019 by a developer using the handle NYAN-x-CAT. It built on the groundwork of Quasar RAT ([THREAT-0164](#)), an earlier open-source C# RAT published at `https://github.com/quasar/Quasar` and available since 2015. Analysts assess AsyncRAT was less a fork of Quasar than a major rewrite, though the two still share the custom cryptography classes used to decrypt malware configuration. That open-source release is what seeded the family described here.

AsyncRAT sits at the root, with DCRAT as its most prolific descendant. DCRAT in turn produced VenomRAT, which produced its own cluster of forks including LMTeamRAT and Alfa Red Fox. Other DCRAT children include EchoRAT, Gh0stRAT, BitRAT, CyberSpike, Dumpling RAT, and DarkRAT (by way of ShaShenRAT). The full tree spans roughly 40 named variants across three tiers of descent.

Two builder handles surface in the family's certificates, in the same organization and organizational-unit fields that the `O=<Name> By <author>` structure reserves for the author. `qwqdanchun` appears across several variants, including Gh0stRAT and LMTeamRAT. That handle also owns the public DCRat source repository (`https://github.com/qwqdanchun/DcRat`), which corroborates that certificates carrying it trace to DcRat-lineage builds. A second handle, `alexeikun`, appears in a VenomRAT fork whose certificate reads `CN=Venom Server, OU=alexeikun, O=Venom By alexeikun, L=SH, C=CN` — the same naming scheme with a different name in the author slot, which suggests alexeikun compiled that build. The handles tie otherwise separate forks back to shared builders, and the author slot is itself a useful pivot: it names who produced a given build, not just which fork it is.

Infrastructure Findings

Censys host-index searches on 16 June 2026 confirmed live C2 for the high-volume variants and surfaced single hosts for much of the long tail.

Variant	Confirmed Censys Hits	Identifier
AsyncRAT	~49	THREAT-0169
DCRAT	~36	THREAT-0165
Gh0stRAT	~21	THREAT-0165 (folded into DCRAT)
VenomRAT	~18	THREAT-0167
BitRAT	~1	THREAT-0162
ElegyRAT	1	THREAT-245
LMTeamRAT	1	THREAT-246
EchoRAT	few live hosts	THREAT-247
JasonRAT	1	THREAT-248
Dumpling RAT	1	THREAT-249
CyberSpike	1	THREAT-250
DarkRAT	no live hosts at time of writing	THREAT-251
Alfa Red Fox	no live hosts at time of writing	THREAT-252

The single-host variants matter because their certificates carry impossible-to-spoof combinations. LMTeamRAT, for example, surfaces on one host but with an issuer that names both its parent and its builder, which leaves no doubt about the family.

Variant Profiles

High-volume variants

- **AsyncRAT** — root of the tree and its largest live footprint at roughly 49 confirmed hosts. Published as open source by NYAN-x-CAT (<https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp>), the codebase the rest of the family forks from.
- **DCRAT** — AsyncRAT's most prolific descendant and the source of the inherited `O=<Name> By <author>, L=SH, C=CN` certificate structure that the rest of the family carries. Roughly 36 hosts. Its source is published by [qwqdanchun](https://github.com/qwqdanchun/DcRat) (<https://github.com/qwqdanchun/DcRat>), the same handle seen in the certificate author slot.

- **Gh0stRAT** — DCRAT fork, roughly 21 hosts. Despite the shared name, it is unrelated to the original Gh0st RAT, a Chinese remote access tool whose source leaked around 2008 and which carries its own distinct lineage; this variant reuses the name on a DCRAT codebase. The certificate index distinguishes two `qwqdanchun` builds: a common one with subject `CN=DcRat` and issuer `CN=Gh0st Rat Server`, `OU=qwqdanchun, O=DcRat By qwqdanchun, L=SH, C=CN` (25 certs), and a rarer full rebrand with subject `CN=Gh0st RAT` and issuer `CN=Gh0st Server`, ... (one cert, first seen 23 December 2022).
- **VenomRAT** — DCRAT fork that spawned six downstream RATs of its own, roughly 18 hosts. Its certificate signature (`CN=VenomRAT` , or the `O=VenomRAT By` issuer) also catches forks that never rebranded, such as Alfa Red Fox.
- **BitRAT** — DCRAT fork with a minimal live footprint, around one host.

Tracked low-volume variants

Each of these carries a distinct certificate or host and is tracked under its own identifier. Several run a single live host or none at all, but the certificate evidence is unambiguous.

- **ElegyRAT** ([THREAT-245](#)) — AsyncRAT fork. One live host at `192.229.116.23:8808` , issuer `CN=ElegyRAT Server` .
- **LMTeamRAT** ([THREAT-246](#)) — VenomRAT fork. One host, issuer `CN=LMTEAM Server, OU=qwqdanchun, O=VenomRAT By qwqdanchun, L=SH, C=CN` . Both the `qwqdanchun` handle and the VenomRAT parent are visible in a single certificate.
- **EchoRAT** ([THREAT-247](#)) — DCRAT fork, separated out from the AsyncRAT cluster. Representative host `192.238.134.73:56005` .
- **JasonRAT** ([THREAT-248](#)) — AsyncRAT fork. One host at `107.175.159.134:7777` .
- **Dumpling RAT** ([THREAT-249](#)) — DCRAT fork. One host at `47.98.129.153:8848` .
- **CyberSpike** ([THREAT-250](#)) — DCRAT fork. One host at `121.199.75.205:443` .
- **DarkRAT** ([THREAT-251](#)) — ShaShenRAT fork of DCRAT. No live hosts at time of writing, tracked by the issuer organization `O=DarkRat By ShaShen` .
- **Alfa Red Fox** ([THREAT-252](#)) — VenomRAT fork. No live hosts at time of writing, and also caught under VenomRAT's `O=VenomRAT By` signature.

The Family-Wide Signal

The certificate structure DCRAT introduced is inherited rather than regenerated. Most VenomRAT-tier forks keep `CN=VenomRAT` or the `O=VenomRAT By` issuer pattern, so they stay identifiable under the VenomRAT certificate signature even when they are not separately branded. More broadly, any certificate combining `L=SH, C=CN` with an `O=* By *` organization field, served on a non-standard port, is a strong indicator for the family no matter which fork generated it. That pattern is the basis for tracking the whole lineage under a single signature rather than chasing each fork by name.

Detection Posture

Variant names split cleanly into hunt-worthy and noisy. Distinctive names produce zero-false-positive queries and are worth periodic re-checking as new infrastructure appears: NonEuclid (also documented by the Cybersecurity

and Infrastructure Security Agency, CISA), ArchosaurRAT, ShiningForceRAT, CYB3R RAT, and SantaRAT all fall here.

Other names are unusable for certificate-based hunting because they collide with legitimate entities. PhoenixRAT searches return Phoenix Contact GmbH industrial hardware; PegasusRAT returns NSO Group brand noise; MagnumRAT matches several unrelated businesses; and L838 RAT sits too close to Windows auto-generated hostnames (WIN-L838...). Detection for these variants will need panel content or a confirmed certificate sample rather than a name match.

Outlook

The family will keep forking, and new forks will likely keep inheriting the DCRAT certificate structure, so a lineage-wide certificate signature should hold up better over time than per-variant name searches. Several named variants currently show no live infrastructure; they may deploy later, which is why the investigation re-runs these searches periodically. One near-term lead remains open: the certificate index already distinguishes two `qwqdanchun` Gh0stRAT variants worth tracking separately.

Prior Censys research on this family and the techniques used to deliver it:

- [AsyncRAT C2 Activity at Internet Scale](#)
- [Unmasking the Infrastructure of a Spearphishing Campaign](#)
- [A Technique-Based Approach to Hunting Web-Delivered Malware](#)

External: [AsyncRAT's Open-Source Code Sparks Surge in Dangerous Malware Variants](#) (The Hacker News, July 2025).



AUTHOR

Aidan Holland

Senior Security Researcher

Aidan Holland is a Senior Security Researcher with Censys ARC, where he specializes in threat intelligence and internet-wide security research. His work focuses on identifying and analyzing malicious infrastructure, tracking threat actors, and developing tools for security analysis at scale. Aidan is an active contributor to the open source security community, building and maintaining tools for threat hunting, data analysis, and security automation.

Source: <https://censys.com/blog/asynrat-family-threat-overview/>