March 20, 2026

RANSOMWARE GROUP PROFILE

Akira

Entity type:
Ransomware-as-a-Service (Raas)

Year established:
April 2023

Volume:
USD 150 million in 2025; USD 244 million total as of late September 2025

Founder:
Unknown

Base of operations:
Possibly Russia/post-Soviet region

Sanctions details:
Not sanctioned

Background

Akira is one of the most consequential ransomware groups operating globally, and the most prolific by total ransom proceeds in 2025. Active since April 2023, the group operates as a closed RaaS enterprise using double extortion — combining encryption with the threat to publicly release stolen data — to pressure victims into payment. Akira has demonstrated a consistent capacity to adapt its targeting, tooling, and on-chain laundering infrastructure in response to law enforcement pressure, making it one of the more technically and operationally sophisticated threats in the current ransomware landscape.

Victim profile

Akira has impacted organizations across multiple sectors and geographies, with a concentration of victims in the United States, Canada, Brazil, Australia, and several European countries. Its targeting spans manufacturing, professional services, technology, education, finance, and critical infrastructure. Public reporting has tied Akira to several high-profile incidents, including attacks on Stanford University, Nissan Australia, and Finnish IT provider Tietoevry. The group posted approximately 980 victims on its leak site between January 1 and December 11, 2025, alternating with Agenda/Qilin for the top position by victim count — while significantly

outpacing Agenda/Qilin in ransom proceeds, taking in over USD 150 million in 2025 alone, nearly twice that of the second most active strain.

Actor lineage and technical notes

Security researchers have identified code and operational similarities between Akira and the Conti ransomware ecosystem, suggesting possible overlaps in developer tooling or shared affiliates. TRM assesses that Akira is likely linked to Russia, with evidence pointing to developers based in Russia or the broader post-Soviet region. Multiple non-VPN IP observations tied to Russia reinforce this assessment, as do observations of the group communicating in Russian on dark web cybercrime forums.

Notably, Akira's malware does not include the typical safeguard used by many Russian-linked groups that halts execution when a Russian keyboard layout is detected — a deliberate omission that may be intended to obscure attribution or reflect an operational choice to maximize targeting flexibility.

Connected threat actors

TRM's on-chain analysis has identified links between Akira and at least two other ransomware groups. The Fog ransomware group employed the same Defiway laundering infrastructure as Akira during Phase III, reinforcing indications of cooperation or shared operational resources. TRM further assesses that the Frag ransomware group may represent an extension of Akira: both actors utilize a shared two-address wallet cluster and the same bridge and payment service that Akira used exclusively between late 2024 and June 2025. Frag also demonstrates on-chain overlaps with Fog, suggesting a network of operationally linked groups sharing tooling and infrastructure.

On-chain laundering TTPs

Akira has undergone at least four distinct evolutions in its post-payment laundering tactics since 2023. This pattern of continuous TTP rotation is one of Akira's defining characteristics, and reflects a deliberate effort to stay ahead of monitoring and enforcement.

Phase I (2023)

Early Akira payment flows can be grouped by likely affiliate based on consistent on-chain behaviors, including the reuse of intermediary addresses, wallet clusters receiving funds from

multiple victim payments, shared cash-out points, and other observable transactional patterns. This phase provides the clearest on-chain visibility into Akira's affiliate structure.

Phase II (early to mid-2024)

Akira shifted to a more standardized laundering process using WanChain, with most victim payments funneled through a single WanChain address before being dispersed across multiple global VASPs for cash-out. This transition marked a move away from affiliate-visible clustering toward centralized laundering infrastructure.

Phase III (late 2024)

The group transitioned again, routing all victim proceeds through the Defiway bridge. During this period, Fog ransomware employed the same laundering approach, reinforcing TRM's assessment of overlap or operational cooperation between the two groups.

Phase IV (August 2025 – present)

Akira altered its laundering workflow once more. Each victim payment now passes through a unique intermediary address, followed by aggregation across two consolidation addresses, before being off-ramped at a single global virtual asset service provider (VASP). TRM identified HTX as the primary cash-out destination during this phase. Despite operating as a RaaS, Akira's laundering patterns during this phase remain highly standardized — the admin-affiliate revenue split appears to occur only after funds are deposited into the shared VASP cash-out address, keeping the split opaque on-chain. Akira and other groups including Anubis, Lumos, and INC have been cashing out within the same day or up to 36 hours after payment receipt.

TRM has also observed isolated deviations from Akira's Phase IV pattern, with some victim funds routed through Chainflip cross-chain swaps before being deposited in full into Tornado Cash. This behavior may reflect affiliate-level divergence from standardized procedures or the early indicators of a fifth laundering phase.

Law enforcement and regulatory response

The FBI and CISA issued a joint advisory on Akira in November 2025, sharing indicators of compromise and noting USD 244 million in total victim payments as of late September 2025.

As of the time of this profile, Akira has not been subject to OFAC sanctions, criminal indictments, or a law enforcement disruption operation.