

AKIRA

Ransomware-as-a-service operation active since March 2023, now the world's second most active group behind Qilin. Extorted an estimated \$244 million from over 600 victims in 2025 alone, with code and wallet overlaps pointing back to the defunct Conti operation.

Howling Scorpion (CrowdStrike)

Megazord / Akira_v2 (variants)

Windows/Linux/ESXi

RISK RATING

Critical

ACTIVE SINCE

2023

BUSINESS MODEL

RaaS, mature affiliate model

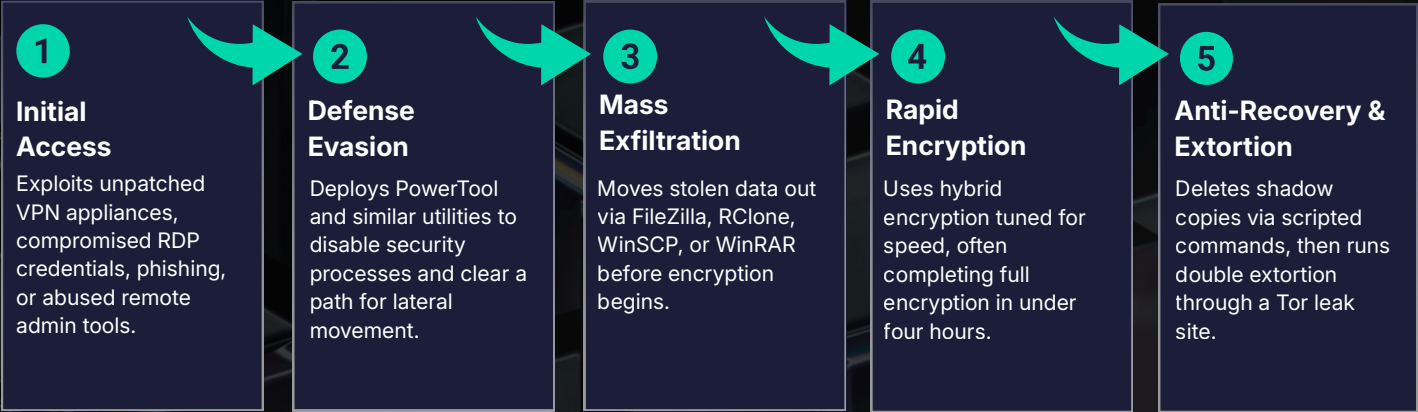
PRIMARY VECTOR

VPN exploitation, compromised RDP

2026 STANDING

\$244M from 600+ victims

ATTACK CHAIN



MITRE ATT&CK MAPPING

ID	TECHNIQUE
T1190	Exploit public-facing application (VPN appliances)
T1078	Valid accounts (compromised RDP credentials)
T1562.001	Impair defenses (PowerTool, security process termination)
T1567.002	Exfiltration to cloud storage (FileZilla, RClone, WinSCP)
T1486	Data encrypted for impact (hybrid encryption, ESXi-targeted)
T1490	Inhibit system recovery (scripted shadow copy deletion)

SECTOR BY SECTOR Summary



Manufacturing
Its most consistent target, alongside business services and construction, across every major tracker.



Professional & Business Services
A close second, chosen for the downstream client access these firms typically hold.



Technology & Finance
Rounds out its top targets, reflecting a broad, opportunistic reach rather than a narrow specialism.

ORIGIN & EVOLUTION

Emerged in March 2023 with code and wallet overlaps pointing back to the defunct Conti operation, though no organizational link has been confirmed. Distributed by an operator group CrowdStrike tracks as Howling Scorpius, Akira has extorted an estimated \$244M from over 600 victims without a single indictment, sanction, or law enforcement disruption naming the group as of August 2026.

THREAT LANDSCAPE CONTEXT

Code and cryptocurrency wallet overlaps tie Akira back to the defunct Conti operation, though no confirmed organizational link exists. Deliberately omits the Russian-keyboard kill switch most Russian-linked ransomware includes to avoid domestic prosecution, an unusual attribution wrinkle that may be intentional obfuscation.

SIGNATURE TRADecraft

Exploits unpatched VPN appliances or compromised RDP credentials, then deploys PowerTool to disable security processes and clear a path for lateral movement. Moves stolen data out via FileZilla, RClone, WinSCP, or WinRAR before encrypting with a hybrid method tuned for speed, often completing full encryption in under four hours.

ANALYST OUTLOOK

No law enforcement action has ever named Akira, unlike LockBit, Scattered Spider, or Qilin's near-misses, which may explain its consistency at #2 globally for over two years. Expect it to remain a top-tier threat as long as its Conti-era tooling and operational discipline hold up.

NOTABLE INCIDENTS

Global data storage and infrastructure company

November 2025

A 42-day compromise began when an employee clicked a fake CAPTCHA check (ClickFix) on a compromised website; two separate EDR tools logged the malicious activity but generated too few alerts to trigger a response before three networks were encrypted.

Los Angeles law firm

January 2026

Compromised roughly 10GB of sensitive legal data, consistent with the group's focus on professional services firms holding confidential client information.

Toppan Next Tech, Singapore

Breached the MSP and printing company, exposing client statements and showing Akira's willingness to hit supply-chain providers for downstream access.