

Akira Ransomware Group | ThreatMon End-to-End Intelligence

 [linkedin.com/posts/threatmon_akira-ransomware-group-ugcPost-7277859919427440640-M6lZ](https://www.linkedin.com/posts/threatmon_akira-ransomware-group-ugcPost-7277859919427440640-M6lZ)








Posted on LinkedIn

 [View organization page for ThreatMon End-to-End Intelligence](#)


[ThreatMon End-to-End Intelligence](#)

8,834 followers

3mo

 **New Report Alert: Akira Ransomware – A Rising Threat in 2024**   Emerging in March 2023, the Akira ransomware group has quickly established itself as a formidable adversary in the cybercrime landscape. From targeting critical sectors such as healthcare, finance, education, and manufacturing to employing advanced double-extortion techniques, Akira's operations are a growing global concern.  Our latest report delves into their evolution, including their transition to Rust-based architecture and their alarming expansion into VMware ESXi environments. With over 250 organizations impacted worldwide and ransom demands reaching up to \$4 million, Akira's campaigns underscore the importance of proactive cybersecurity measures.  Don't miss our detailed analysis! Learn about Akira's tactics, targets, and the implications for organizations in critical sectors.

[#CyberThreatIntelligence](#) [#Ransomware](#) [#AkiraRansomware](#) [#ThreatAnalysis](#)
[#CriticalInfrastructure](#) [#CyberSecurityInsights](#)

 138 1 Comment

 [Sarwar Alam](#), [graphic](#)

To view or add a comment, [sign in](#)