Cybercriminals Are Abandoning Traditional Ransomware in Favour of Data Theft

EDINBURGH, SCOTLAND, July 30, 2026 /EINPresswire.com/ -- Cybercriminals are increasingly abandoning traditional tactics in favour of stealing sensitive data to extort organisations. This marks a fundamental shift in how cyber attacks are conducted, according to new threat intelligence analysis from Quorum Cyber.

> Increasingly, cybercriminals don't need to encrypt systems to achieve their objectives. If they can steal an organisation's most valuable data, they already have the leverage they need."
>
> *Jack Alexander, Global Intelligence Lead at Quorum Cyber*

Drawing on intelligence gathered during the first half of 2026, Quorum Cyber has identified a growing move away from attacks centred solely on encrypting systems towards operations focused on data theft, identity compromise, and extortion. The shift reflects changing economics within cybercrime, with attackers increasingly able to generate revenue without deploying ransomware at all.

The new report, titled “2026 Global Cyber Risk Mid-Year Review,” finds that once attackers gain trusted access through stolen credentials, phishing, compromised cloud identities or insider manipulation, their primary objective is increasingly to extract valuable information over simply disrupting operations. Stolen customer data, intellectual property, source code, cloud credentials, and SaaS identities are being monetised through extortion, resale or subsequent attacks.

Quorum Cyber's team of analysts found that organisations remain heavily focused on preventing encryption-based ransomware attacks, meaning that many are less prepared to detect or prevent large-scale data exfiltration.

Jack Alexander, Global Intelligence Lead at Quorum Cyber, commented: "In the last 10-12 years ransomware has become synonymous with cybercrime but we're seeing a significant change in attacker behaviour. Increasingly, cybercriminals don't need to encrypt systems to achieve their objectives. If they can steal an organisation's most valuable data, they already have the leverage they need."

He continued: "Data has become the more valued currency of cybercrime. Once attackers gain trusted access through compromised credentials, phishing or social engineering, their priority is

increasingly to identify what information they can take before they're detected. That data can then be used for extortion, sold to other threat actors or exploited in follow-on attacks." Rather than relying solely on malware deployment, attackers are increasingly exploiting trusted identities and legitimate access. Quorum Cyber's intelligence highlights a growing trend of cybercriminals purchasing compromised credentials, recruiting insiders, abusing help desk processes, stealing authentication tokens and targeting cloud environments to gain access before quietly extracting sensitive information.

The report findings also suggest ransomware groups are becoming more commercially sophisticated. Some are moving towards extortion-only operations, recognising that many organisations fear regulatory investigations, customer notification requirements and reputational damage more than temporary operational disruption. Others are adopting increasingly structured negotiation tactics designed to maximise the likelihood of payment. Jack Alexander concluded: “The findings reflect a significant change across the threat landscape and identity, trust and data are now the primary targets for financially motivated cybercriminals. As organisations continue to adopt cloud services, SaaS platforms and AI-powered tools, protecting sensitive information and detecting abnormal access is becoming increasingly important alongside traditional cyber defences.”

Quorum Cyber will host a webinar on Aug. 18, 2026 to discuss the findings in greater detail. Visit AI, Identity and Trust: Secure the Foundations of Cyber Resilience in 2026 to register.

About Quorum Cyber
Founded in Edinburgh in 2016, Quorum Cyber is a proactive, threat-led cyber security company helping organisations defend against an increasingly complex digital landscape, including the opportunities and risks created by AI. With customers across North America, the UK, and beyond, Quorum Cyber is a Microsoft Solutions Partner for Security, a member of the Microsoft Intelligent Security Association (MISA), and the 2025 Microsoft Security MSSP of the Year. Its mission is to help good people win by providing clarity and confidence in moments of cyber risk. For more information, visit www.quorumcyber.com.

April Burghardt
PR Consultant
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/930316055

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.