



New Zscaler Report Reveals AI-Assisted Attackers Move to Massive Data Theft, Executive Targeting, and Millions in Extortion Payments

September 30, 2026

New Zscaler ThreatLabz 2026 Ransomware Report finds attackers stole nearly 900 terabytes of data, increasingly targeted employees with privileged roles, and used GenAI to accelerate operations

SAN JOSE, Calif., Sept. 30, 2026 (GLOBE NEWSWIRE) -- [Zscaler, Inc.](#) (NASDAQ: ZS), the cybersecurity platform for the AI era, today released new findings from the Zscaler ThreatLabz 2026 Ransomware Report, showing that ransomware is on the rise, and is being aided by AI, increasing by more than 275% since last year, while costing companies more than \$328 million in payments to hacking groups. Zscaler's research revealed that nearly 900 terabytes of data – the equivalent to 90 times the print collection at the Library of Congress – were stolen over the course of a year. The AI-driven increase in ransomware is targeting nearly two-thirds of senior-level executives, and threat actors are increasingly using trusted workplace tools, including Microsoft Teams, to enable data theft and lateral movement within an organization's environment.

Key findings from the ThreatLabz 2026 Ransomware Report reveal:

- Ransomware data theft increased more than 275% year over year, reaching 896.2 terabytes of exfiltrated data
- Blockchain transactions associated with ransomware payments reached \$328 million
- The average ransom payment rose 5.3% year over year to \$431,995
- Manager-level titles and above accounted for 62% of victims in attacks, highlighting a focus on employees with privileged roles and business influence
- Threat actors are increasingly abusing trusted enterprise tools, including Microsoft Teams and Quick Assist, to enable social engineering, lateral movement, data theft, and file encryption

"Successful ransomware extortion is shifting away from file encryption that often causes business disruptions to less visible, but more damaging data theft attacks," said Deepen Desai, Executive Vice President of Cybersecurity at Zscaler. "They are using GenAI to speed up operations, and focusing on stealing more of an organization's intellectual property, customer information, and other sensitive data to drive payment. Security teams need to stop these attacks early by reducing initial access opportunities, limiting lateral movement, and preventing data exfiltration."

Additional findings in the Zscaler ThreatLabz 2026 Ransomware Report include:

- Manufacturing and technology remained the most targeted industries while freight & logistics (+725%), and utilities (+622%) saw the fastest year-over-year growth.
- The United States remained the top ransomware target with U.S. organizations accounting for 50.7% of observed activity, far ahead of Canada (4.8%), Germany (4.3%), and the U.K. (4.1%).
- Script-based tooling is playing a larger role in ransomware as JavaScript, PowerShell, Python, and other scripting languages are helping attackers develop new tooling faster and blend in with legitimate activity.
- Ransomware victim volumes remain persistent amid major ecosystem churn: ThreatLabz tracked 7,366 victims listed on ransomware leak sites, representing only a 3% YoY decline. Qilin, Akira and INC Ransom accounted for 34% of disclosed victims.
- The ransomware landscape is seeing significant expansion, showing nine of the top 15 groups by victim volume were new to the rankings, and ThreatLabz identified 52 newly active groups over the last year.

The Zscaler ThreatLabz 2026 Ransomware Report provides guidance on how to disrupt ransomware across the attack lifecycle and examines the current threat landscape in depth, including exfiltration trends, victim targeting, evolving attacker tradecraft, and extortion economics.

To learn more, read the full report here: <https://www.zscaler.com/campaign/threatlabz-ransomware-report>

Methodology

The report is based on Zscaler telemetry and ThreatLabz analysis and examines ransomware activity from April 2025 through March 2026, with a focus on groups and affiliates, victim targeting, attack techniques, data theft, and payment patterns. Together, the findings show a threat landscape where attackers are increasing leverage through stolen data, targeting business-influential employees, and improving operational efficiency with AI-assisted tooling and abuse of legitimate enterprise platforms.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across 200+ public data centers globally and thousands of private sites at the edge, the SASE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

Media Contact

Nick Gonzalez, Director of Global Public Relations, press@zscaler.com