Ransomware Moves up the Org Chart: Managers Are Prime Targets

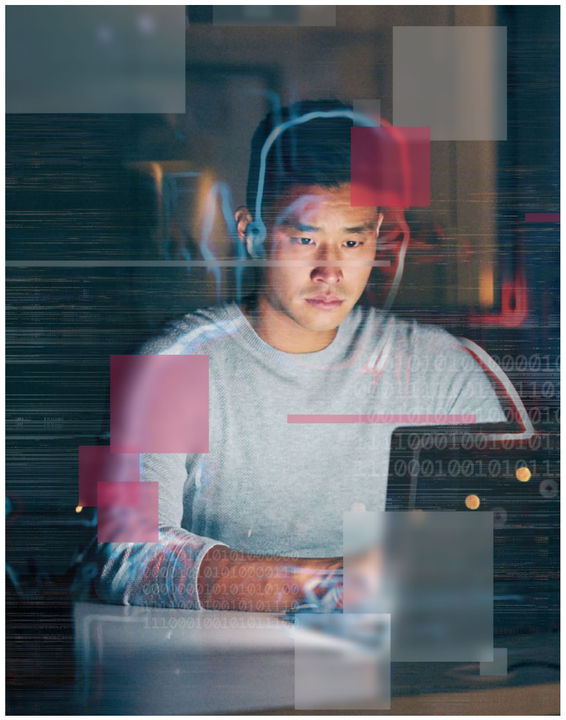
zscaler™

THREATLABZ RESEARCH

Ransomware attack reporting often focuses on companies that are breached, the stolen data, the malware tooling, and the ransom payments. However, there is minimal data about who threat actors target inside organizations. New ThreatLabz research bridges this gap and examines the human side of ransomware attacks, including the roles and business functions that are most represented among targeted victims. The findings revealed that ransomware threat actors are not just targeting individuals randomly at organizations; they are targeting specific employees with privileged roles and business-critical functions to increase their chances of gaining a foothold, moving through the network, exfiltrating sensitive information, and monetizing their access.

Methodology

Over one month, ThreatLabz identified 351 compromised victims across 334 organizations linked to a threat actor that specializes in gaining initial access to steal large amounts of corporate data and selectively encrypt critical systems.

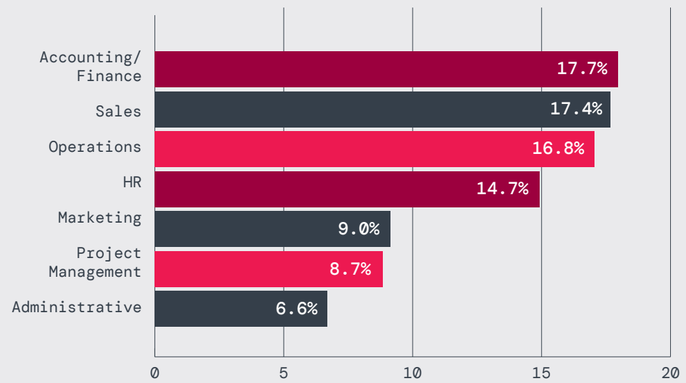


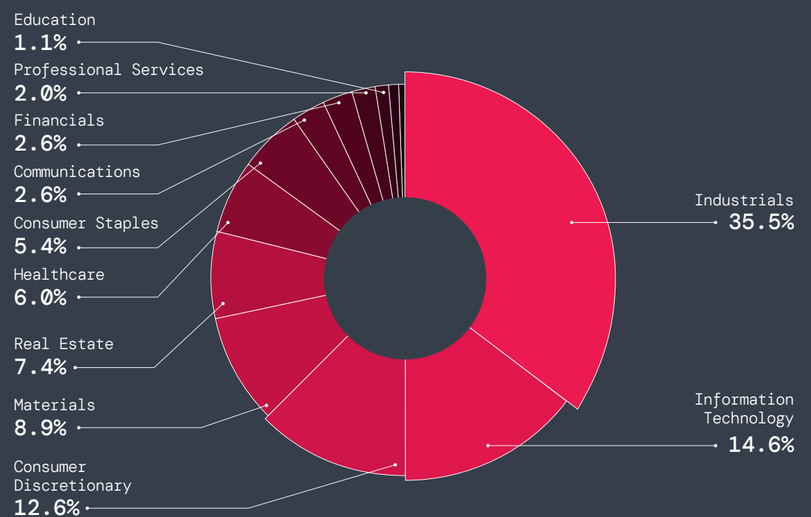
Key Findings

62% of victims held the title of manager or higher

50% of victims worked at **industrial and IT** companies

BUSINESS-CRITICAL ROLES WERE TARGETED





Gen X made up the **largest percentage of victims:**

44%

Average age: 46
Millennials: **33%**
Gen Z: **14%**
Baby Boomers: **9%**

4.6% of companies had more than one employee compromised

Ransomware Victimology Snapshot

- Ransomware victims compromised by this threat actor **largely held managerial titles or above.** This suggests attackers are targeting employees who have privileged access to customer data, financial records, contracts, and operational systems.
- Individuals from **five departments accounted for more than 75% of the victims:** accounting/finance, sales, operations, HR, and marketing, respectively.
- Victims spanned a wide age range, from 23 to 70 years old, but **concentrated around the mid-to-late 40s with Gen X** accounting for 43.9% of victims.
- At the organization level, **50% of victim companies came from just two sectors:** the industrials (35.5%) and information technology (14.6%).
- More than a dozen companies had **multiple employees that were compromised**.

Example Victim Profiles

These profiles provide real-world examples of ransomware victims and why they may be targeted.

Regional Sales Manager

Industry: Industrials

Why they're targeted: Access to customer accounts, active deals, contracts, pricing, and revenue information

Accounts Payable Manager

Industry: Information Technology

Why they're targeted: Access to payment details, invoices, financial approvals, and vendor records

Property Manager

Industry: Real Estate

Why they're targeted: Access to lease agreements, vendor invoices, contracts, client data, and financial information

Senior Project Manager

Industry: Consumer Discretionary

Why they're targeted: Access to project budgets, vendor contracts, and sensitive files or documents

Enterprise Lesson: Secure High-Risk Business Users

This campaign reinforces a critical ransomware defense priority: strengthen controls around the users and workflows closest to sensitive business data. When attackers target employees in sales, finance, accounting, or operations, a single compromised account can create corporate-wide risk.

The attackers use urgency, IT impersonation, and familiar tools like Microsoft Teams and Quick Assist to gain trust. From there, the risk escalates quickly into credential theft, remote access, lateral movement, data theft, potential file encryption, and ultimately extortion.

Ransomware prevention cannot stop at malware detection. It also needs to account for the employees whose access creates the most business risk if compromised.

To reduce that risk, enterprises should:

- Implement segmentation via a Zero Trust architecture to prevent lateral movement and reduce the attack surface.
- Train employees to verify requests from "IT personnel" using information provided in the company directory.
- Block external instant messages and calls on collaboration platforms such as Microsoft Teams and Slack.
- Enforce least-privilege access to limit exposure to sensitive systems and data as much as possible.
- Deploy AI-powered inline threat protection and endpoint security to detect and stop attacks.
- Continuously monitor user, device, and application activity for signs of compromise.

X @ThreatLabz | ThreatLabz security research blog

zscaler™ | Act Fast. Stay Secure.