CYBER EXTORTION

CRIMINALS USE YOUR DATA TO FINE-TUNE DEMANDS

CYBER CRIMINALS are increasingly stealing companies' data to bolster their ransomware extortion demands, according to a new report by cyber insurer Resilience.

As part of these tactics, hackers are infiltrating company databases before launching attacks to better understand their defenses and the value of their data and maximize ransom demands. They are also searching for companies' cyber insurance policies to tailor demands to coverage and maximize payouts.

The results emphasize the importance of employers adapting their defenses to evolving cyberattacks that, if large enough, can cripple an organization's ability to recover.

This shift toward a focus on data has been rapid. Data theft-only attacks rose from 49% of extortion claims in the first half of 2025 to 65% in the second half, according to the "Resilience 2025 Cyber Risk Report."

Criminals now infiltrate networks, quietly move through databases and assess which data has the highest regulatory, legal or competitive value — then structure ransom demands accordingly.

In some cases, threat groups have gone further by searching stolen files for cyber insurance policies. Groups such as Interlock have reviewed policy details to calibrate ransom demands within coverage limits and increase the odds of payment.

Extortion has also become layered. Attackers may:

- Demand payment to decrypt systems.
- Demand additional payment to suppress stolen data.
- Threaten customers or business partners directly.

Points of failure: Where attackers are getting in

The report emphasizes that hackers are primarily focused on gaining access by stealing or abusing employees' login credentials.

According to the Resilience report, key points of failure include:

Phishing: The resurgence of phishing in 2025 suggests AI is making campaigns more believable and scalable. AI-generated phishing campaigns are achieving success rates as high as 54% compared with 12% for traditional methods.

New tools allow attackers to craft highly personalized messages, impersonate executives and bypass language barriers. Deepfake audio and video are expected to raise the risk of executive impersonation and fraudulent wire transfers next year.

Vendor compromise: When critical vendors are breached, losses can cascade across entire industries.

Ways vendors are compromised

- Vendor ransomware that spreads business interruption to clients
- Vendor data breaches that expose customer information
- Non-malicious vendor outages that disrupt operations

Credential theft via infostealers: More than 2 billion credentials were harvested in 2025, often serving as an early warning sign of a larger ransomware attack.

How to protect your firm

As threats evolve and cyber attackers use new tactics, employers will need to react accordingly. Organizations may consider:

- Investing in data loss prevention and zero-trust software.
- Deploying multifactor authentication and e-mail authentication protocols.
- Monitoring for stolen credentials on the dark web and rotating session tokens immediately when a compromise is detected. This will often require contracting with vendors that specialize in this area.
- Developing vendor incident contingency plans that address supply chain failures.
- Conducting tabletop exercises to rehearse coordinated legal, technical and communications responses.
- Reviewing cyber insurance policy limits to ensure coverage reflects current severity levels rather than historical averages.

If you have concerns about potential cyber risks, give us a call to discuss your cyber insurance options.