BLACK KITE

THE RANSOMWARE SHAKE-UP: What 6,000 Attacks Tell Us

From syndicate takedowns to SMB pressures, see what our year-long analysis of **150+ ransomware groups, dark web activity, and 6,000+ victims** reveals about today's fractured threat landscape.

No Kingpins. Just Chaos.

The fall of LockBit and AlphV didn't end ransomware—it fractured the ecosystem. Smaller, erratic groups now dominate, launching more attacks with less discipline.

24% YoY
increase in number of victims

96 ACTIVE
ransomware groups (including 52 new)

123%
increase in victims over two years

The groups got smaller. **The problem got BIGGER.**

Ransomware Is Now a Supply Chain Crisis

Ransomware groups now deliberately target vendors embedded deep in supply chains, knowing the ripple effects can pressure victims to pay quickly.

67%
of third-party breaches are ransomware-related

3,000+
auto dealers affected by CDK Global breach

400
victims linked to single Cleo software exploit

One vulnerable vendor = **mass disruptions.**

SMBs: The New Sweet Spot

Attackers favor **many hits** over a few big logos.

11%
of victims had revenue >$100M

$4M-$8M
most targeted revenue tier

Big companies are harder to breach. Small and mid-sized businesses (SMBs) are easier to ransom and less likely to report. With hardened defenses at the top, attackers have shifted their focus downmarket.

Second Strikes are Surging

Victims listed on leak sites become magnets for follow-up attacks. Affiliates jump between groups, recycling access, and revisiting targets.

100+
organizations were attacked twice

14
saw a second breach within 7 days

60+
were re-attacked after 6 months

Being a victim once doesn't buy you immunity – **it paints a target.**

Less Ransom, More Damage

$553K
average ransom payment

35%
decrease in average ransom payment

After the collapse of major syndicates, smaller groups without the infrastructure for complex extortion took over. They skip negotiation, make a single demand, take what they can get, and move on.

25%
of victims paid a ransom

Quick hits are replacing drawn-out negotiations.

Spot the Risk Before It Hits

46%
of companies with RSI™ >0.8 were hit

61%
showed RSI spikes within 6 months of an attack

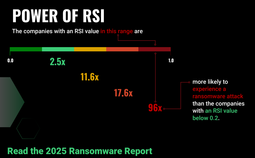
.5%
of companies with RSI <0.2 were victimized

Black Kite's Ransomware Susceptibility Index® (RSI™) helps you stop guessing and start anticipating. Scored from 0.0 to 1.0, the higher the score, the more likely you are to be a target.

When RSI™ spikes, it's not a warning—it's a countdown.

POWER OF RSI

The companies with an RSI value in this range are



Read the 2025 Ransomware Report

Ransomware has fractured into a chaotic web of new groups, hitting harder and spreading faster through supply chains and small vendors.

Dive deeper into how the threat is evolving—and what it means for your organization—in the "2025 Ransomware Report: How Ransomware Wars Threaten Third-Party Cyber Ecosystems."

ACCESS THE REPORT

No downloads—just click and explore!

BLACK KITE