MORPHISEC

Executive Report

# State of Ransomware 2025: Key Findings from the Morphisec CTO Briefing

*What CISOs and Security Leaders Need to Know About the Shifting Ransomware Landscape*

## The Ransomware Business Model Has Evolved—Has Your Defense?

In Q4 2025, ransomware groups are operating more like enterprises than ever before. Affiliate structures, Ransomware-as-a-Service (RaaS), and extortion-only models are reshaping the threat landscape. Morphisec's CTO briefing offers an insider look at these shifts—and the evasive tactics security teams must prepare for in 2026.

## Top 5 Takeaways

1. **Fewer Victims Are Paying—but Payouts Are Rising**
   Only 23-26% of victims now pay ransoms, but average payments continue to climb as attackers focus on high-value targets.
2. **Ransomware-as-a-Service Is Dominating the Market**
   Groups like Keeling, Akira, and DragonForce run professionalized operations with revenue-sharing models and affiliate management systems.
3. **New Entry Points Are Emerging Faster Than Patches**
   Attackers exploit unpatched SonicWall and FortiGate vulnerabilities, leverage Teams-based social engineering, and target misconfigured cloud backups.
4. **Exfiltration Has Replaced Encryption as the Primary Pain Point**
   "Ransomware without encryption" attacks are surging, with data theft alone driving extortion. Attackers now rely on Azure Copy and Bitbucket for stealthy data exfiltration.
5. **Defensive Evasion Is Outpacing Detection**
   Adversaries use safe mode encryption, telemetry tampering, and EDR bypasses to evade even leading endpoint solutions.

# How CISOs Can Adapt to the Next Phase of Ransomware

- **Prioritize Prevention Over Detection**
  Detection-based models can't keep up with evasive techniques. Preemptive defenses and moving target technologies disrupt attackers before payloads execute.
- **Reevaluate Your Backup Strategy**
  Backups are often corrupted, encrypted, or misconfigured. Test recovery plans regularly and isolate backup networks.
- **Expand Visibility Beyond Endpoints**
  Non-agent assets—like gateways, appliances, and file shares—are prime ransomware execution points.
- **Train for Social Engineering Through Collaboration Tools**
  Microsoft Teams and similar platforms are now being weaponized. Harden configurations and enforce external call restrictions.
- **Validate Exfiltration Before Paying**
  Not every extortion claim is legitimate. Demand proof and investigate with forensics teams before responding.

Download the full webinar replay on demand to hear the complete ransomware breakdown from Morphisec's CTO, Michael Gorelik.

**Watch the On-Demand Briefing**

# About Morphisec

Morphisec is the trusted global leader in prevention-first Anti-Ransomware protection, redefining cybersecurity with our industry-leading Automated Moving Target Defense (AMTD) technology. Our solutions are trusted by over 7,000 organizations to protect more than 9 million endpoints worldwide, stopping 100% of ransomware attacks at the endpoint and safeguarding businesses against the most advanced and dangerous threats, including zero-day exploits and ransomware. Shrink your attack surface faster to prevent ransomware entry. Eliminate blind spots across complex environments that attackers exploit for ransomware campaigns.

At Morphisec, we don't just fortify defenses – we proactively prevent attacks before they happen, delivering unmatched protection and peace of mind to our customers. With our Ransomware-Free Guarantee and commitment to Preemptive Cyber Defense, we set the standard for accountability and innovation in the fight against modern cybercrime.

To learn more, visit morphisec.com/demo