

2026 State of Malware

Executive Summary

**8%****increase**

in ransomware attacks year-over-year

86%**of ransomware attacks**

are conducted remotely

135**countries**

experienced ransomware attacks in 2025

\$2.5B**estimated**

economic impact of the Jaguar Land Rover attack

The threat landscape is shifting rapidly from human-driven intrusions to AI-orchestrated attacks. In 2025, attacks on businesses were dominated by stealthy, hands-on-keyboard operations that relied on legitimate tools, stolen credentials, and human decision making, with little or no traditional malware. Attackers blended into normal administrative activity, moved quickly—often at night or on weekends—and exploited blind spots such as unmanaged systems to deploy ransomware remotely. By prioritizing speed, stealth, and the disruption of security and recovery mechanisms, they left defenders with shrinking windows to detect, contain, and respond.

By the end of the year, speculation about AI in cybercrime gave way to reality. AI systems outperformed human vulnerability researchers, exploit pipelines compressed patch-to-exploit timelines to minutes, and the first confirmed cases emerged of AI agents executing complex, multi-stage compromises with minimal human oversight. Cybercrime has entered its machine-scale era. Organizations that invest in visibility, resilience, and automation now will be best positioned to keep pace with a threat landscape evolving faster than ever before.

Five operating patterns every business should know:

1. Faster attacks

Compressed dwell times leave businesses little time to respond.

2. Working at night

Threat actors time their operations for periods of low visibility and reduced staffing.

3. Living off the land

Legitimate tools and credentials are used to blend into normal activity.

4. Staging from blind spots

Unmanaged and unmonitored systems are used to stage remote attacks.

5. Attacking security and backup software

Security controls and recovery mechanisms are deliberately targeted.

For more information on how to defend your organization in 2026, read the 2026 State of Malware.

[Download now](#)

0101000111101