

# Ransomware Reality Check

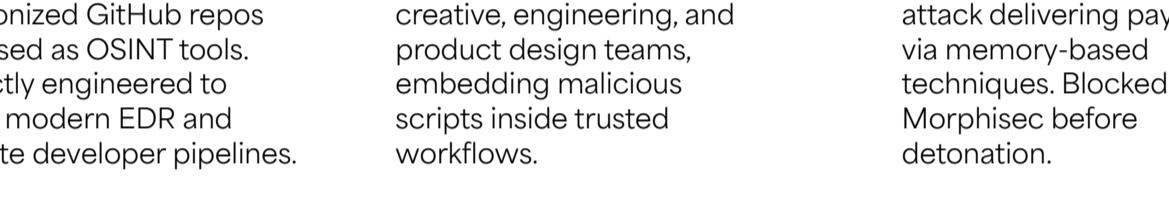
RANSOMWARE ISN'T SLOWING DOWN...IT'S SCALING.  
HERE'S WHAT SECURITY LEADERS ARE UP AGAINST THIS YEAR:

- 93% of organizations experienced at least one ransomware-ready intrusion in the last 24 months.
- 76% of attacks now include data theft, not just encryption.
- Average **ransom demand jumped 47% YoY**, now exceeding **\$1.5M**.
- Organizations face **23 days of downtime** on average after an attack.
- Fileless and in-memory techniques (favored by today's ransomware crews) rose **30%**, easily bypassing traditional EDR.

2026 requires a prevention-first security posture, not another year of playing catch-up.

## THREAT INTELLIGENCE SNAPSHOT: WHAT MORPHISEC SAW IN 2025

Real attacks. Real organizations. Real prevention.



### PyStoreRAT

A modular, fileless malware delivered through weaponized GitHub repos disguised as OSINT tools. Perfectly engineered to evade modern EDR and infiltrate developer pipelines.

[Get the Research](#)

### StealC V2 – Blender Supply Chain Attack

Threat actors weaponized Blender.blend files to target creative, engineering, and product design teams, embedding malicious scripts inside trusted workflows.

[Get the Research](#)

### Tuoni C2 Attack on U.S. Real Estate Firm

A highly evasive command- and-control attack delivering payloads via memory-based techniques. Blocked by Morphisec before detonation.

[Get the Research](#)

### Trend Insight:

Attackers are shifting toward AI-assisted, supply-chain, developer-environment, and fileless intrusion methods. Detection tools struggle: prevention is essential.

## WHERE ORGANIZATIONS STILL FALL SHORT

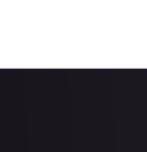
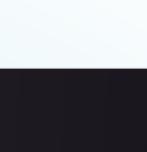
Even mature teams still struggle with:

-  **Unpatched legacy systems** – present in 57% of companies.
-  **Backups exposed to attackers** – compromised in 39% of incidents.
-  **Identity misuse**, involved in over 80% of ransomware operations.
-  **Developer environments lacking controls** – a major entry vector in cases like PyStoreRAT.

### Risk Insight:

Most ransomware campaigns succeed because attackers exploit predictable, unchanging systems. AMTD eliminates that predictability.

## WHY PREVENTION MATTERS MORE THAN DETECTION IN 2026



### Detection-Only Tools (EDR/XDR)

- Generate alerts after malicious behavior begins
- Often miss fileless and in-memory attacks
- Increase SOC workload
- Allow attackers visibility into system memory

### Preemptive Defense with AMTD (Morphisec)

- Blocks attacks before execution
- Neutralizes fileless and zero-day techniques
- Stops exploitation without needing signatures
- Reduces dwell time and attack surface exposure

### Outcome:

Lower blast radius. Lower workload. Higher resilience.