Weekly Threat Report

Cyber threats aren't slowing down and neither should your response

This week's threat landscape reveals a defining pattern for the second half of 2026: attackers are using AI to eliminate the time, team size, and expertise requirements that used to make large-scale intrusions difficult. A solo operator now carries the throughput of an organized group. Ransomware operators are blinding defenses before any alert fires. And the developer toolchains organizations trust are becoming primary targets.

Here's what you need to know:

See what you've missed

Solo AI-Assisted Attacker Breaches AWS Environment and Extorts Global Enterprise in 72 Hours

Incident response firm Sygnia documented how a single attacker used agentic AI to compress what would typically take a team of attackers several weeks into approximately 72 hours — chaining weaknesses across application services, cloud resources, CI/CD pipelines, and data stores to extort a global enterprise.

GodDamn Ransomware Deploys Microsoft-Signed PoisonX Kernel Driver to Blind EDR Before Encrypting 10 Hosts

Symantec disclosed that the Hyadina group's GodDamn ransomware used PoisonX — a malicious kernel driver carrying a legitimate Microsoft signature — to terminate endpoint security software across at least 10 machines before deploying ransomware. The driver operates at the kernel level, leaving security tools running but stripping their visibility entirely.

Schedule a meeting with our Solutions Advisors to see where your cyber resilience sits!

Secure Your Organization Today

Injective Labs npm SDK Backdoored to Steal Crypto Wallet Keys from Developer Environments

Attackers compromised a trusted contributor's GitHub account and used Injective Labs' own publishing pipeline to release a malicious SDK version that captured cryptocurrency wallet private keys and seed phrases at the moment of wallet creation. The attack reached 18 packages and 87 downstream dependents before being detected and reversed in under an hour.

Microsoft Discloses GigaWiper — Modular Backdoor Built for Irreversible Destruction

Microsoft disclosed GigaWiper, a modular Windows backdoor that allows operators to choose between full disk wiping, Windows drive overwriting, or fake ransomware that scrambles files without saving a decryption key. The third mode is particularly concerning because it mimics ransomware without offering any recovery path — organizations that encounter it cannot negotiate or pay their way to a resolution. Tested, offline, and isolated backup systems are the only effective mitigation against this class of threat.

Product Recommendation

Cyber Risk Report for Enterprise Security

LEARN MORE

Cyber threats are constantly evolving, putting businesses at risk of data breaches, fraud, and compliance violations. Our Cyber Risk Report provides a thorough evaluation of your digital infrastructure, helping you identify vulnerabilities, assess potential risks, and implement robust security measures.

Resource Highlight

As cyber risks ramp up every week, staying ahead with your organization is the top priority.

Learn more about cyber risks and how a report can help your organization stay ahead of emerging threats before they happen.

Download the Onesheet

What to focus on this week ...

Cyber risk is expanding across technology, operations, and human behavior. The common thread this week is speed — AI-assisted attacks execute faster than human-reviewed alert queues can respond, EDR-killing tooling fires before detection systems see the intrusion, and supply chain compromises scale to hundreds of downstream targets in minutes. Proactive cloud security hygiene, kernel-level visibility, and supply chain monitoring are the controls that close these gaps before they become incidents.

If you'd like guidance tailored to your environment, RSI Security is here to help.

Contact RSI Security today to strengthen your cybersecurity posture.

RSI Security, 1900 W. Kirkwood Blvd., Suite 2500A, Southlake,TX 76092
United States of America,(858) 240-9263