Weekly Threat Report

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

This week's threat landscape highlights a critical inflection point: AI is accelerating attacker capability at every stage of the attack chain — from building malware frameworks to executing fully autonomous ransomware — while simultaneously exposing the limits of automated defense tools. The organizations that fare best are those treating security as an operational discipline, not a technology checkbox.

Here's what you need to know:

See what you've missed

SimpleHelp CVSS 10.0 Zero-Day Actively Exploited — Djinn Stealer Targets AI and Cloud Credentials

Attackers exploited CVE-2026-48558, a maximum-severity authentication bypass in SimpleHelp RMM, to gain trusted technician access to managed environments and deploy Djinn Stealer — a cross-platform credential harvester that specifically targets cloud keys, AI coding assistant tokens, package registries, and CI/CD pipelines. CISA added the flaw to its Known Exploited Vulnerabilities catalog on June 29 with a July 2 federal remediation deadline. Organizations using SimpleHelp should update to version 5.5.16 or 6.0 RC2 immediately, audit technician logs from June 12 onward, and rotate all credentials accessible from the server.

Avalon Framework and CrownX Ransomware: AI-Assisted Development Closes the Expertise Gap

Blackpoint Cyber disclosed Avalon, a new modular malware framework with strong indicators of AI-assisted development that bundles credential theft, lateral movement, backup destruction, and CrownX ransomware into a single memory-resident attack chain. The campaign uses spoofed legal document emails and ISO-embedded payloads to bypass email scanners, then evades major endpoint security tools before targeting backup infrastructure. Organizations should ensure offline backups are tested, validate recovery procedures, and monitor for recovery system tampering as a pre-ransomware signal.

Bad Epoll (CVE-2026-46242): Linux Kernel Zero-Day Achieves Root with 99% Reliability

Researcher Jaeyoung Chung disclosed a race-condition use-after-free in the Linux kernel's epoll subsystem that allows any unprivileged local user to escalate to root on Linux servers, desktops, and Android devices running kernel 6.4 or later. A working public exploit succeeds approximately 99% of the time, and there is no workaround — epoll cannot be disabled. The bug survived an AI code audit by Anthropic's Mythos model, which found a sibling flaw in the same code but missed this one. Organizations should apply available kernel patches immediately and treat this as an emergency patching event, not routine maintenance.

JADEPUFFER: First Fully Autonomous LLM-Driven Ransomware Attack Confirmed

Sysdig documented JADEPUFFER, the first publicly confirmed case of an agentic ransomware campaign executed entirely by a large language model without human operator intervention. The attack used an exposed Langflow instance for initial access, then autonomously pivoted, adapted, and executed a destructive database-extortion playbook against a production server. The significance is speed and scale — LLM-driven attacks can iterate and escalate 24/7 without fatigue, waiting periods, or human coordination.

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. This week's headlines share a common thread: the tools and infrastructure organizations trust most — RMM platforms, backup systems, Linux kernels, and AI development environments — are now primary attack targets. Strong patch discipline, tested recovery procedures, and continuous credential governance are the controls that contain these threats 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