Weekly Threat Report

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

This week's threat landscape exposes a structural challenge that extends beyond any individual vulnerability or threat group: attackers are chaining AI capability, identity compromise, rapid vulnerability exploitation, and trusted-service abuse into interconnected attack paths. Compliance controls mapped to individual frameworks, vulnerability management here, identity governance there, third-party risk somewhere else — are not built to detect or contain threats that move across all of those categories in a single campaign.

Here's what you need to know:

See what you've missed

U.S. Agencies Confirm AI-Generated Exploit Scripts Targeting Industrial Control Systems

CISA, NSA, FBI, DOE, and EPA issued a joint advisory confirming that threat actors are using AI-generated exploit scripts to target Siemens S7 industrial controllers and PLCs across critical infrastructure sectors.

Microsoft Entra ID CVSS 10.0 Vulnerability Confirmed Exploited

CVE-2026-69836, a maximum-severity remote code execution vulnerability in Microsoft Entra ID, was confirmed as actively exploited this week. Simultaneously, Palo Alto Networks' Unit 42 documented a large-scale campaign targeting Entra tenants through stolen credentials

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

Secure Your Organization Today

Medusa Ransomware Hits Hundreds of Organizations

CISA and the FBI updated their Medusa ransomware advisory this week confirming activity across hundreds of organizations, while actively exploited vulnerabilities spanned GitLab, VMware vCenter, Microsoft SharePoint, and macOS

Compromised Rust Maintainer and TWINLOOT Malware Expose Supply Chain

A compromised Rust package maintainer account pushed malicious crates containing code that executes during compilation, exposing developer machines through standard build processes without any separately suspicious download or execution.

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 ransomware and how your organization can stay ahead of emerging threats before they happen.

Start Working On Your Checklist

What to focus on this week ...

Cyber risk is expanding across technology, operations, and human behavior. This week's headlines share a single structural thread: the attack surface is interconnected in ways that siloed security controls and framework-mapped compliance programs were not built to cover. OT exposure, identity compromise, rapid exploitation, and trusted-platform abuse are not separate risk categories this week.

They are overlapping attack paths in active use. Integrated security governance, continuous monitoring, and evidence-based control validation are what close those gaps.

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