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 becoming more scalable. One vulnerable product reaches hundreds of organizations. One exploitable perimeter device opens the path to full network compromise. One AI agent can execute what previously required a coordinated human team. The organizations best positioned to respond are those whose security programs are built around detection speed, remediation validation, and integrated controls — not policy documentation alone.

Here's what you need to know:

See what you've missed

CISA Confirms SharePoint Vulnerabilities Driving Active Ransomware Campaigns

CISA confirmed that ransomware actors are actively exploiting CVE-2026-45659, a high-severity remote code execution flaw in Microsoft SharePoint Server, with a Rapid7 proof-of-concept incorporated into live attack campaigns almost immediately after publication.

Cl0p Claims Data Theft From Nearly 50 Organizations via Shared Enterprise Software

Cl0p ransomware operators claim to have stolen data from nearly 50 organizations — including Shell, Philips, GE, and Fiserv, through vulnerabilities in PTC Windchill and FlexPLM enterprise software.

Gunra Ransomware Targets Critical Infrastructure Through Perimeter Vulnerabilities

CISA, the FBI, and partner agencies warned of Gunra ransomware activity targeting government and critical infrastructure through known vulnerabilities in internet-facing perimeter technologies including Fortinet products.

Autonomous AI Agents Are Executing Cyberattack Stages Without Human Direction

Researchers reported on a near-autonomous cyberattack in which multiple AI agents operated in parallel to map systems, identify vulnerabilities, adapt strategies, and extract data without human direction at each step — though attribution and specific details remain subject to ongoing investigation.

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 Checklsit

What to focus on this week ...

Cyber risk is expanding across technology, operations, and human behavior. The common thread across this week's stories is scalability — attackers are finding leverage points that multiply impact across many organizations at once, while AI is beginning to eliminate the human bottlenecks that security programs were designed to detect. Closing these gaps requires vulnerability management, third-party risk governance, and AI oversight to operate as integrated, evidence-based programs — not independent workstreams measured by policy existence alone.

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