Weekly Threat Report

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

This week's threat landscape highlights two converging trends that are reshaping the security priorities of organizations across every sector: nation-state actors are escalating attacks against operational technology and critical infrastructure, while autonomous AI systems are generating new categories of risk that sit entirely outside the traditional threat model.

Here's what you need to know:

See what you've missed

CISA and FBI Warn: Gunra Ransomware Actively Exploiting Fortinet Appliances

CISA and the FBI issued a joint advisory confirming that Gunra ransomware actors are exploiting vulnerabilities in Fortinet FortiOS and FortiProxy to gain network access, exfiltrate data, and deploy ransomware, with critical infrastructure organizations.

Identity-Based Attacks Now Outpace Software Vulnerabilities as Ransomware's Entry Point

A Sophos analysis confirmed this week that attackers are more likely to enter through stolen credentials, compromised accounts, and trusted remote-access tools than through unpatched software vulnerabilities.

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

Secure Your Organization Today

Windows Zero-Day Publicly Released Patch Tuesday Addresses 415 Vulnerabilities

A security researcher publicly released a Windows zero-day following a dispute with Microsoft over previous disclosures, while Microsoft's August Patch Tuesday simultaneously addressed 415 vulnerabilities including one actively exploited zero-day and three publicly disclosed zero-days.

China-Linked Actors Weaponize N-able Security Software for Ransomware Delivery

Microsoft and independent researchers confirmed that a China-linked threat actor exploited a vulnerability in N-able's cybersecurity software to deliver ransomware, converting a trusted security tool into an attack vector.

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 trust, attackers are exploiting the infrastructure, identities, and tools organizations trust most. Closing the gaps these stories expose requires vulnerability management, identity governance, asset inventory, and continuous monitoring to operate as an integrated program — not as independent workstreams with separate owners and separate timelines.

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