InfoSight®
www.infosightinc.com

INFOSIGHT INSIGHTS

January 2026 Issue

Stay Ahead with the Newsletter
for OT & IoT Cyber Risk & Strategy.

Cyber Intelligence Briefing: Advanced Threat Actors, Supply Chain Risks & Emerging OT Gaps

January 2026, Vol. I, Issue XII

This month's headlines converge on one reality: attackers are winning with operational leverage, not novelty. Nation-state operators are turning simple misconfigurations and exposed management planes into durable footholds, while malware like BRICKSTORM and emerging macOS strains show how quietly adversaries can persist once inside. At the same time, breach impact continues to escalate as data-rich industries outside "traditional" targets—real estate and healthcare included—absorb regulatory, legal, and reputational fallout. Layer in zero-days on edge devices, malicious packages in developer ecosystems, and high-permission browser extensions, and the trust boundary keeps expanding across vendors, endpoints, and productivity tooling. The practical takeaway is straightforward: reduce exposure at the perimeter, harden identity and admin surfaces, continuously validate remediation, and maintain always-on detection and response that can keep pace with AI-accelerated tradecraft.

What's Inside

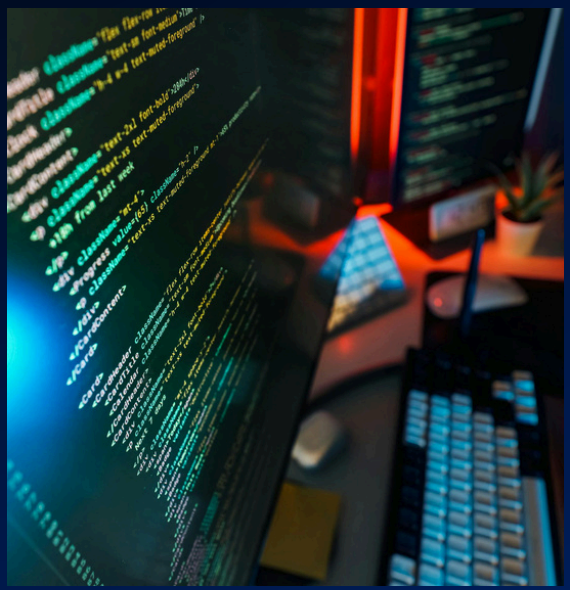
- Nation-State & Advanced Threat Activity
- Major Breaches & Data Compromises
- Vulnerabilities & Zero-Day Exploits
- Software Supply Chain & Open Source Risks
- Malware, Crimeware & Endpoint Threats
- OT, ICS & Emerging Technology Risks

Nation-State & Advanced Threat

State-Linked Intrusions Expand Through Misconfigurations

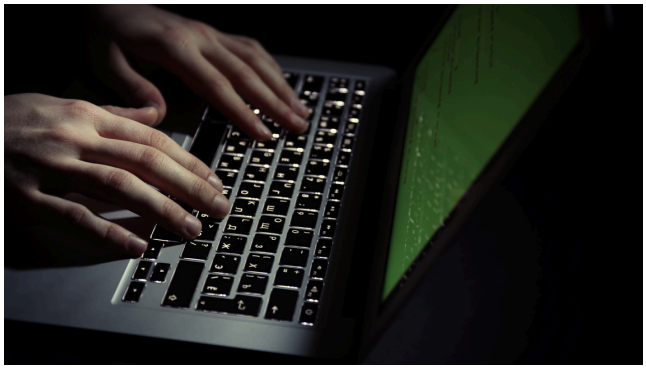
China-nexus operators exploited insecure configurations in Cisco AsyncOS appliances used for email and web security management. By abusing exposed interfaces, they deployed custom backdoors and executed arbitrary commands, enabling long-term persistence within targeted environments. This campaign reinforces how operational misconfigurations—not just unpatched vulnerabilities—are increasingly leveraged by well-resourced threat groups.

Read more.



Persistent Backdoor Activity Intensifies Against U.S. Networks

New reporting from CISA and partners reveals the continued spread of the BRICKSTORM backdoor across VMware and Windows environments. The malware employs stealthy persistence mechanisms and modular components that allow attackers to quietly pivot through compromised systems. Updated detection signatures and IOCs underscore the need for continuous monitoring, threat hunting, and rapid response as activity remains ongoing. Read more.



Major Breaches & Data Compromises

Real Estate Firm Faces Major Data Exposure Affecting Thousands

Rockrose Development confirmed a significant breach exposing sensitive data—including Social Security numbers, financial details, and medical information—for nearly 47,000 people. The company is coordinating with forensic investigators, regulators, and legal counsel to manage fallout and notify impacted individuals. This incident reflects the growing trend of real estate and property management firms becoming attractive targets due to the volume of personal data they store. Read more

Healthcare Breach Settlement Underscores Regulatory Pressure

Dakota Eye Institute agreed to a $1 million settlement resolving claims tied to its 2023 data breach, which compromised sensitive patient information. Although the organization denies wrongdoing, plaintiffs argued the institute failed to implement adequate safeguards under HIPAA. The settlement signals increasing legal and financial risk for healthcare entities that lack strong cybersecurity controls. Read more.

Vulnerabilities & Zero-Day Exploits

Zero-Day Attacks Target Widely Deployed Edge Devices

SonicWall appliances are being actively exploited via zero-day vulnerabilities that allow attackers to bypass authentication and execute remote commands on edge infrastructure. Security researchers warn that threat actors are rapidly weaponizing device-level flaws, especially those in perimeter systems that provide direct access to internal networks. Organizations relying on these devices should apply mitigations immediately while monitoring for anomalous traffic or compromise indicators. Read more.

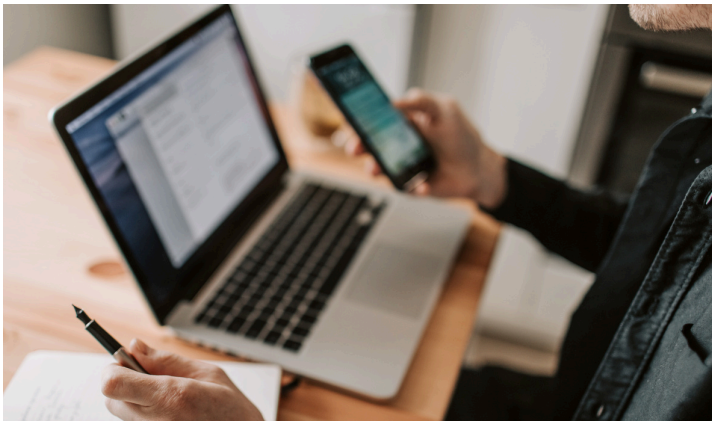
Software Supply Chain & Open-Source Risks

Federal Leaders Renew Focus on Open-Source Security Gaps

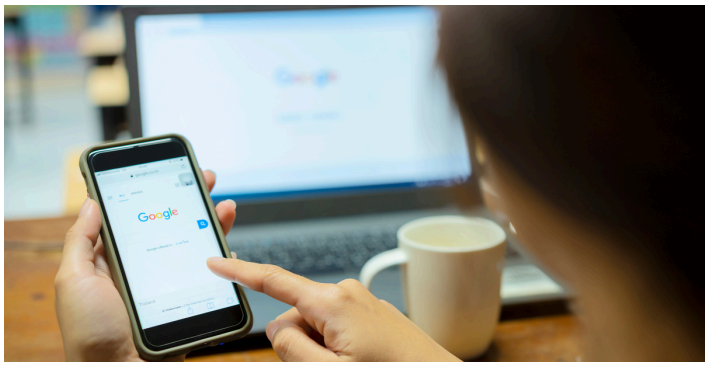
Senator Tom Cotton urged the White House to strengthen national defenses against risks stemming from open-source software, including foreign code tampering and insufficient project oversight. The letter highlights long-standing concerns about relying on community-maintained software without dedicated security resources. Policymakers increasingly view supply chain stability as a national security imperative, signaling potential future regulation or funding initiatives. Read more.

Malicious npm Package Mimics API Tool to Steal Credentials

A fraudulent WhatsApp API package uploaded to npm was discovered stealing credentials from developers who unknowingly installed it. The attacker masqueraded as a legitimate library, enabling dependency hijacking within the open-source ecosystem. This incident underscores how easily malicious actors can infiltrate developer workflows and why organizations must implement strict dependency auditing and package verification practices. Read more.



Malware, Crimeware & Endpoint Threats



Rogue Browser Extension Harvests User Data at Scale

Researchers identified a malicious Chrome extension that secretly harvested user data—including browsing activity and authentication tokens—and transmitted it to attacker-controlled infrastructure. Because browser extensions operate with extensive permissions, they remain a high-value target for threat actors seeking silent access to user accounts. This discovery reinforces the need for extension governance and continuous monitoring across enterprise endpoints. Read more.

Global Crime Ring Exposed in ATM Jackpotting Crackdown

The U.S. Department of Justice charged 54 individuals connected to a large-scale ATM jackpotting operation that used malware and hardware manipulation to force machines to dispense unauthorized cash. The scheme spanned multiple countries and leveraged coordinated financial fraud techniques. The takedown demonstrates the increasing organization and sophistication of financially motivated threat groups. Read more.

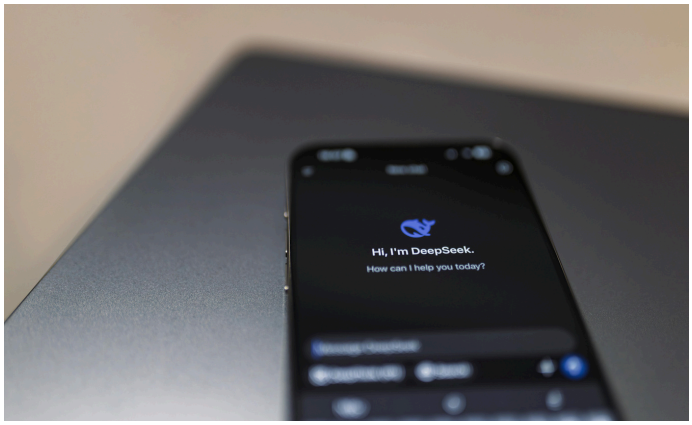
Signed macOS App Used to Deliver New Malware Variant

A new macOS malware strain known as MacSync was distributed through a legitimately signed Swift application, allowing it to bypass macOS trust controls and security warnings. The malware includes capabilities for data exfiltration, persistence, and remote command execution. The attack showcases how macOS is becoming a more attractive target—and how adversaries are evolving their methods to exploit platform trust mechanisms. Read more.

OT, ICS & Emerging Tech Risks

AI and OT Interoperability Gaps Create New Security Challenges

Industry researchers warn that AI-enabled tools are still difficult to safely integrate with legacy OT systems due to architectural incompatibilities, unreliable data pipelines, and unpredictable model behavior. These gaps create new attack surfaces where manipulated inputs or misaligned automation could disrupt operations. As organizations pursue digital transformation, securing the intersection of AI and industrial environments is becoming an urgent challenge. Read more.



How InfoSight Helps

The throughline this month is speed and scale: AI-assisted espionage and AI-in-the-loop malware are pushing beyond human-paced defense models, while vendor exposure and insider risk are widening the trust boundary. Meanwhile, overlooked vectors like calendar invites and collaboration platforms continue to mature into high-impact attack surfaces. The operational priority is to treat AI governance, third-party oversight, and productivity-tool security as core controls, not supporting initiatives.

InfoSight reduces these risks with a layered, evidence-driven approach:

- 24/7 SOCaaS/MDR to detect AI-accelerated tradecraft, suspicious identity activity, and stealthy loader behavior through behavioral monitoring and rapid response.
- CTEM-aligned VMaaS to continuously prioritize and validate remediation across internet-facing and internal attack paths.
- Third-party risk support to expand monitoring coverage, validate vendor control maturity, and close the visibility gap that drives financial-sector exposure.
- Identity and M365-focused assessments to harden the access layer that agentic attacks increasingly target.
- vCISO governance to operationalize AI-use policy, incident readiness, and board-level reporting with defensible documentation.