Executive Summary

5 active campaigns are currently targeting healthcare and technology sectors across Americas, Europe, and Asia-Pacific regions. **High priority:** CVE-2025-55182 RCE (GLOBAL.25.008). Total IOC count: **280 indicators** tracked this week.

.

Active Threat Campaigns

Campaign	Type	Targets	Key Technique	Priority Action
CVE-2025-55182 RCE (GLOBAL.25.008)	Espionage / Financial	Tech, Finance, Healthcare, Retail - US, CA, AU, EU	Exploits Node.js RCE vulnerability to deploy SNOWLIGHT malware and cryptominers via LOTL techniques	Patch immediately - CISA KEV deadline Dec 26
Shai-Hulud NPM Worm (CAMP.25.079)	Financial	Tech, Healthcare, Finance - US, CA, CH, FR	UNC6566 supply chain attack via trojanized NPM packages to steal developer credentials and secrets	Audit NPM dependencies, rotate exposed credentials
Microsoft Account Phishing (CAMP.25.086)	Espionage	Healthcare, Govt, Finance - US, NZ, DK, IN	UNC6293 compromises websites to social engineer victims into granting Microsoft account access	Review OAuth grants, train users on social engineering
Salesforce OAuth Compromise (CAMP.25.078)	Financial	Healthcare, Media, Tech - US, EU, AU	ShinyHunters-linked actor compromised Gainsight OAuth tokens to access 230 Salesforce instances	Revoke Gainsight tokens, review Salesforce OAuth apps
Oracle EBS Zero-Day (CAMP.25.075)	Financial	Healthcare, Energy, Retail, Tech - US	FIN11-linked actor exploits Oracle EBS XDO Template Manager for GOLDVEIN malware and CL0P extortion	Monitor Oracle EBS, apply patches when available

Top 3 Actions This Week

1. **1. Patch CVE-2025-55182 (Node.js):** Immediately update all Node.js runtime environments to patched versions. This vulnerability is on CISA's KEV list with a December 26, 2025 remediation deadline.
2. **2. Review Third-Party OAuth Integrations:** Audit all OAuth applications connected to Salesforce and Microsoft 365. Revoke suspicious tokens and implement token rotation policies.
3. **3. Secure Software Supply Chain:** Implement NPM package verification and audit processes. Rotate GitHub tokens, AWS credentials, and other developer secrets.

.

Threat Metrics

Activity Trends

▲ 45% CVE exploitation campaigns
▲ 32% Supply chain attacks
▼ 12% Ransomware incidents
▲ 28% OAuth/credential theft

Indicators of Compromise: 280

- File hashes: 62
- IP addresses: 113
- Domains: 18
- URLs: 87

Resources: Google Threat Intelligence | MITRE ATT&CK (attack.mitre.org) | CISA Alerts (cisa.gov)

Report suspicious calls or emails to your IT security team immediately.