

Daily Threat Intelligence Briefing

Today's threat briefing contains live links that connect you to the original source articles. You can see the real URL by hovering your mouse over the links and checking that they match the source articles. These links were taken straight from the website of the source article. Tyler Technologies has not checked these sites or links for security.

**News from Wednesday September 23, 2026
(Reported on Thursday September 24, 2026)**

Local Government

Watchdog finds most agencies failed to meet CISA cloud security orders, heightening risk of attack | Vulnerability | [CyberScoop](#)

DHS inspector general finds most federal agencies still haven't implemented CISA's binding cloud security directives, raising breach risk.

Financial Institutions

Malicious AI agents steal 600K credit cards, infect 100+ sites with skimmers | Web Skimming / Malware | [Bleeping Computer](#)

Threat actor leveraged open-source AI agent frameworks to automate attacks on 100+ e-commerce sites, harvesting over 600,000 payment card records via skimmers.

Healthcare

Medical Imaging Archive Flaws Put Patient Scans at Risk | Vulnerability | [BankInfoSecurity](#)

Security researcher discloses flaws in open-source DCM4CHE medical imaging archive that could allow attackers to delete, forge, or reassign patient scan data.

77% of Ransomware Groups Are Targeting the Healthcare Sector | Ransomware | [HIPAA Journal](#)

Report finds most active ransomware groups continue to prioritize US healthcare organizations among their targets.



Other

F5 patches BIG-IP APM zero-day flaw exploited in RCE attacks | Zero-Day/Vulnerability | [Bleeping Computer](#)

F5 released emergency patches for a critical BIG-IP APM vulnerability that attackers were actively exploiting for remote code execution.

Check Point hacked: The security software protecting your network has become a prime attack target | Vulnerability | [CSO Online](#)

Check Point warns attackers are actively exploiting two vulnerabilities, including an RCE flaw, in its Security Gateway and Spark firewall products.

Attackers Use Malicious Terraform Providers to Deliver Go Malware via HashiCorp Registry | Supply Chain | [The Hacker News](#)

Researchers found malicious Go modules and Terraform providers on HashiCorp's registry used to distribute Go-based malware to developers.

MikroTik Chain Let Attackers Take Over MikroTik Routers Without a Password or SSH Key | Vulnerability | [The Hacker News](#)

Researchers detail a chained pair of MikroTik RouterOS SSH flaws allowing full unauthenticated remote takeover of exposed routers.

Attackers Manipulate AI Chatbots in Mass Disinformation, Phishing Campaign | Social Engineering | [Dark Reading](#)

Researchers find attackers seeding malicious links and false content across the web to manipulate ChatGPT, Gemini, and Google AI Overview into surfacing phishing and disinformation.

Compromised MemTensor Packages Deliver sckit Credential Stealer via npm and PyPI | Supply Chain | [The Hacker News](#)

Attackers compromised npm and PyPI packages from MemTensor to distribute a cross-platform Go-based credential-stealing malware called sckit.

