

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 Tuesday September 22, 2026
(Reported on Wednesday September 23, 2026)

Local Government

ShinyHunters claims FBI hack, data theft in PeopleSoft zero-day breach | Zero-Day/Data Breach | [Bleeping Computer](#)

Extortion group ShinyHunters claims to have exploited an Oracle PeopleSoft zero-day to breach FBI systems and steal employee and applicant data.

Another worry for water systems: infostealer exposure | Infostealer Malware / Credential Exposure | [CyberScoop](#)

SpyCloud research found infostealer malware compromised credentials at nearly 1,800 US water utilities, including one device exposing logins for 167 metering customers.

Financial Institutions

FreeStar Financial Says AI-Driven Campaign Brought In \$1.2M in Deposits | Artificial Intelligence/Marketing | [CU Today](#)

FreeStar Financial Credit Union used Experian consumer data and Psympl's psychographic AI to tailor a high-yield savings campaign that generated \$1.2 million in deposits within 30 days.

Healthcare

Call-on-Doc Notifies Patients About December 2025 Hacking Incident | Data Breach | [HIPAA Journal](#)

Telemedicine provider Call-on-Doc is notifying patients of a data breach following a December 2025 hacking incident affecting patient data.



Other

Unmasking EvilTokens: Getting to the root of device code phishing | Phishing | [Microsoft Security Blog](#)

Microsoft's Digital Crimes Unit helped disrupt EvilTokens, a phishing-as-a-service platform enabling device-code phishing and token theft attacks.

New ClosedQuorum Windows malware uses AI for attack decisions | Malware | [Bleeping Computer](#)

Researchers identify new Windows malware, ClosedQuorum, that queries multiple AI models to autonomously choose post-compromise actions.

New CVSS 10.0 VeloCloud Orchestrator Flaw Actively Exploited in Certificate-Based Setups | Vulnerability | [The Hacker News](#)

Attackers are actively exploiting a maximum-severity flaw in Arista's on-premises VeloCloud SD-WAN Orchestrator affecting certificate-based Edge deployments.

Meta's Muse AI assistant has a zero-day that can turn it into a Mac backdoor | Vulnerability | [Malwarebytes Labs](#)

Researchers found a zero-day flaw letting a terminal command hijack Meta's Muse AI assistant to spy on Mac users and hijack linked accounts.

New Linux Kernel Flaw Gives ARM64 KVM Guests Read-Write Access to Host Memory | Vulnerability | [The Hacker News](#)

Researchers disclosed a Linux ARM64 KVM use-after-free flaw letting nested VM guests read/write host kernel memory and escape to the host.

Rogue external MFA providers can steal passwords during logins | Vulnerability/Identity Attack | [Bleeping Computer](#)

Researchers show how attackers with privileged access can register a fake external MFA provider to harvest user passwords during normal sign-ins.

