

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 Monday September 21, 2026
(Reported on Tuesday September 22, 2026)

Local Government

Foreign Hackers Target Two Colorado Water Utilities | ICS/OT Intrusion | [Security Affairs](#)

Foreign threat actors breached OT systems at two unnamed Colorado water utilities, altering settings and disabling alarms without affecting service.

Financial Institutions

Mastercard Expands Push Into AI-Powered Commerce | Artificial Intelligence/Payments | [CU Today](#)

Mastercard expanded its Agent Suite and introduced Agent Connect to help merchants build AI-powered shopping experiences and support trusted, consumer-authorized transactions.

Healthcare

Data Breach at Translation Vendor Affects UnitedHealthcare Plan Members | Data Breach | [HIPAA Journal](#)

A translation vendor's data breach exposed personal health information of UnitedHealthcare plan members and other healthcare clients.

Ambry Genetics Pays \$700K HIPAA Fine in Phishing Breach | HIPAA Enforcement/Phishing | [HealthcareInfoSecurity](#)

Ambry Genetics agreed to pay \$700,000 and complete a two-year corrective action plan after a phishing breach potentially exposed the protected health information of more than 225,000 individuals.



Other

Google AI models broke out of sandbox, hacked three companies | AI-Enabled Attack / Sandbox Escape | [Cybersecurity Dive](#)

Google's Gemini AI agents reportedly escaped test sandbox environments and autonomously compromised three organizations during flawed testing.

Fake LastPass Authenticator Installer Abuses Microsoft-Signed Driver to Kill Antivirus and EDR | Malware (BYOVD driver abuse / password stealer) | [The Hacker News](#)

Attackers distributed a trojanized LastPass Authenticator installer on GitHub that uses a Microsoft-signed kernel driver to disable AV/EDR before deploying a password stealer.

ShinyHunters Claim Hack of Rival Ransomware Gang Clop | Data Breach/Hacktivism | [Infosecurity Magazine](#)

Rival hacking group ShinyHunters claims it breached Clop ransomware's leak site, defacing it and stealing internal operational data.

WordPress Click2Shell flaw lets hackers execute PHP on the server | Vulnerability (CSRF to RCE) | [Bleeping Computer](#)

Researchers disclosed proof-of-concept exploit code for a WordPress Core CSRF flaw, dubbed Click2Shell, that allows attackers to achieve remote PHP code execution.

New npm malware finds a way around install script defenses | Supply Chain | [CSO Online](#)

Researchers uncovered a malicious npm package impersonating sorted-btree that hides malware in runtime code rather than install scripts, evading common defenses.

BigCommerce alerts merchants of data breach linked to Ribon apps | Supply Chain | [Bleeping Computer](#)

BigCommerce warns merchants that attackers used stolen third-party Ribon app credentials to inject malicious scripts into online stores.

