

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, April 20, 2026 (Reported on Tuesday, April 21, 2026)

Government

ZionSiphon Malware Targets Water Infrastructure Systems

Read more at [InfoSecurityMagazine](#)

Financial Institutions

North Korea-Linked UNC1069 Uses Fake Zoom and Teams Meetings to Hack Crypto Professionals

Read more at [CyberSecurityNews](#)

KelpDAO suffers \$290 million heist tied to Lazarus hackers

Read more at [Bleeping Computer](#)

Healthcare

Arizona & Texas Clinics Notify Patients About Ransomware Incidents

Read more at [HIPAAJournal](#)

Other

A Token Flaw Turned Azure's AI Agent Into a Spy

Read more at [BankInfoSecurity](#)

Half of the 6 Million Internet-Facing FTP Servers Lack Encryption

Read more at [SecurityWeek](#)

Gh0st RAT and CloverPlus Adware Delivered Together in New Dual-Payload Malware Campaign

Read more at [CyberSecurityNews](#)

Handling the CVE Flood With EPSS, (Mon, Apr 20th)

Read more at [SANS](#)

Formbook Malware Campaign Uses Multiple Obfuscation Techniques to Avoid Detection

Read more at [InfoSecurityMagazine](#)

Microsoft: Teams increasingly abused in helpdesk impersonation attacks

Read more at [Bleeping Computer](#)



**News from Monday, April 20, 2026
(Reported on Tuesday, April 21, 2026)**

Anthropic MCP Design Vulnerability Enables RCE, Threatening AI Supply Chain

Read more at [TheHackerNews](#)

The Gentlemen ransomware now uses SystemBC for bot-powered attacks

Read more at [Bleeping Computer](#)

Mastodon says its flagship server was hit by a DDoS attack

Read more at [TechCrunch](#)

The backup myth that is putting businesses at risk

Read more at [Bleeping Computer](#)

