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 November 11, 2026
(Reported on Thursday November 12, 2026)

Local Government

CISA Orders Patch for Cisco Flaw Tied to AI Agent Attack | Vulnerability | BankInfoSecurity

CISA mandates federal agencies patch a Cisco vulnerability within two weeks after Chinese-linked actors used an AI model to exploit it against a European telecom.

OT Incidents Hit a Third of Industrial Organizations, SANS Finds | Survey/Report - ICS/OT Incidents | Infosecurity Magazine

SANS Institute research shows a record annual rise in cyberattacks against industrial control and OT systems, now affecting a third of surveyed organizations.

Healthcare

Monadnock Community Hospital in New Hampshire diverts ambulances amid suspected cyber incident | Unknown/Suspected Cyber Incident | DysruptionHub

A New Hampshire hospital rerouted ambulances after a suspected cyberattack, though its ER and surgeries continued operating.

Insider Data Theft Incident Reported by Premise Health | Insider Threat / Data Theft | HIPAA Journal

Healthcare services provider Premise Health disclosed that a former employee unlawfully copied patient data before departing the company.

Other

Active ScreenConnect attacks breach MSPs, impact dozens of organizations | Supply Chain | Bleeping Computer

Attackers compromised ConnectWise ScreenConnect instances at managed service providers to push rogue remote-access tools to dozens of downstream customer networks.

Microsoft Patches 1,259 Flaws, Including Exploited Outlook Bug That May Expose NTLMv2 Hashes | Vulnerability | The Hacker News

Microsoft's November patch release fixes over 1,200 vulnerabilities, including an actively exploited Outlook flaw that could leak NTLMv2 authentication hashes.

Maersk confirms data breach as WhiteArmor ransomware demands $5 million | Ransomware/Data Breach | Bleeping Computer

Shipping giant Maersk confirmed attackers breached a legacy acquired system, with WhiteArmor ransomware group demanding $5 million for stolen data.

Rewriting less than 10 neurons in an LLM can turn it into a sleeper backdoor | Supply Chain/Model Backdoor | CSO Online

Microsoft researchers reveal a technique dubbed Lazarus that alters under 10 dormant neurons to covertly backdoor open-weight AI models without retraining.

Hackers use AntiFox AI agents in AWS credential-theft attacks | Credential Theft/Malicious Tool Abuse | Bleeping Computer

Threat actors deploy self-hosted instances of the open-source AntiFox AI penetration-testing tool on Alibaba Cloud to steal AWS credentials from targeted web services.

Who Runs the Ransomware Group Qilin? | Ransomware | Krebs on Security

Investigation identifies alleged Russian administrator behind Qilin, now the most active ransomware affiliate program globally.

Lessons from 59 Linux Kernel Bug Reports | Vulnerability | Microsoft Security Blog

Microsoft research team used AI-assisted analysis to uncover 59 Linux kernel vulnerabilities, including eight local root privilege-escalation exploits, now patched upstream.