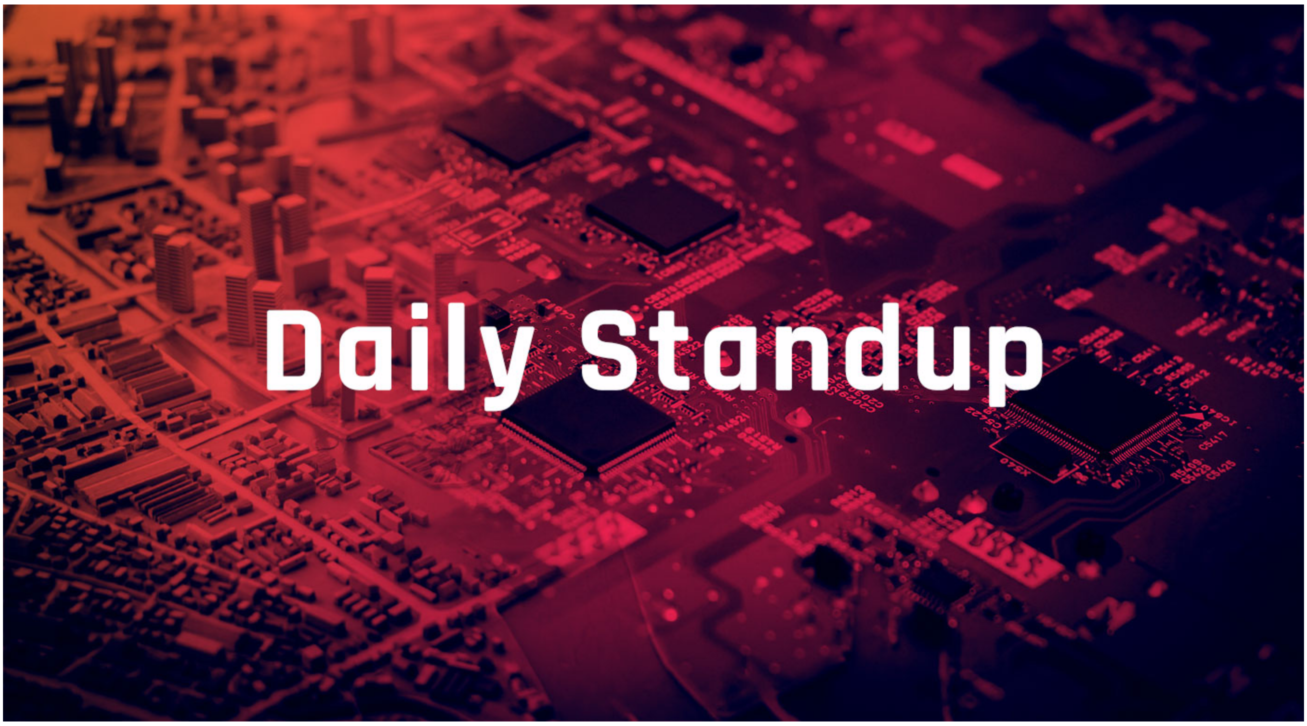
Intelligence Report

Daily Standup

November 13, 2023



LockBit Ransomware Leaks Gigabytes of Boeing Data (BleepingComputer)

Target audience: CISO, CIO, Incident Response, Security Ops, Threat Intel/CTI

Summary: *The LockBit ransomware gang published data stolen from Boeing, one of the largest aerospace companies that services commercial airplanes and defense systems. Before the leak, LockBit hackers said that Boeing ignored warnings that data would become publicly available and threatened to publish a sample of about 4GB of the most recent files. LockBit ransomware has leaked more than 43GB of files from Boeing after the company refused to pay a ransom. Most of the data listed on the hacker group's leak site are backups for various systems, the most recent of them with an October 22 timestamp. The ransomware actor posted Boeing on their site on October 27 and gave the company a November 2nd deadline to contact them and engage in negotiations. The hackers said at the time they had stolen "a tremendous amount of sensitive data" and were ready to publish it.*

Analyst comment: The "LockBit" ransomware group leaked over 43 GB of data from Boeing after the company refused to meet their ransom demands. This incident highlights the increasing audacity of ransomware groups in targeting large, high-profile organizations and their willingness to follow through on threats to leak sensitive data. To mitigate such threats, companies must prioritize robust cybersecurity measures, regularly back up critical data, and prepare contingency plans to respond effectively to ransomware attacks, reducing the likelihood of data compromise and leakage.

See also:

Boeing.Com (LockBit Ransomware Blog) (Flashpoint Collections)

"'LockBit' Ransomware" (Flashpoint)

Ransomware Attack on China's Biggest Bank Disrupts Treasury Market Trades, Reports Say (SecurityWeek)

Target audience: CISO, CIO, Incident Response, Security Ops, Threat Intel/CTI

Summary: *A financial services business of China's biggest bank says it was [h]it by a ransomware attack that reportedly disrupted trading in the U.S. Treasury market. Industrial and Commercial Bank of China Financial Services handles trades and other services for financial institutions. A statement on its website seen Friday said the ransomware attack this week disrupted some of its systems but that it had disconnected parts of the affected systems to limit the impact from the attack. The company, which is based in New York, said it was investigating and had reported the problem to law enforcement. All Treasury trades executed Wednesday and repo financing trades on Thursday were cleared, it said. It said ICBC's banking, email and other systems were not affected. The company gave no further details but reports said the attack was by LockBit, a Russian-speaking ransomware syndicate that does not target former Soviet countries.*

Analyst comment: A ransomware attack on the Industrial and Commercial Bank of China Financial Services disrupted US Treasury market trades. This incident, attributed to the LockBit ransomware syndicate, underscores the increasing threat ransomware poses to global financial markets and critical financial services. It highlights the urgent need for financial institutions to enhance their cybersecurity measures, regularly update their systems, and collaborate with law enforcement and cybersecurity firms to better anticipate and mitigate the risks of such sophisticated cyberattacks.

See also:

"FLASH: LockBit Source Confirms Attack on ICBC" (Flashpoint)

Microsoft Warns of Fake Skills Assessment Portals Targeting IT Job Seekers (Hacker News)

Target audience: Authentication Teams, Fraud Teams, Incident Response, Security Ops, Threat Intel/CTI

Summary: *A sub-cluster within the infamous Lazarus Group has established new infrastructure that impersonates skills assessment portals as part of its social engineering campaigns. Microsoft attributed the activity to a threat actor it calls Sapphire Sleet, describing it as a "shift in the persistent actor's tactics."*

Sapphire Sleet, also called APT38, BlueNoroff, CageyChameleon, and CryptoCore, has a track record of orchestrating cryptocurrency theft via social engineering. "Sapphire Sleet typically finds targets on platforms like LinkedIn and uses lures related to skills assessment," the Microsoft Threat Intelligence team said in a series of posts on X (formerly Twitter). "The threat actor then moves successful communications with targets to other platforms." The tech giant said past campaigns mounted by the hacking crew involved sending malicious attachments directly or embedding links to pages hosted on legitimate websites like GitHub.

Analyst comment: This shift in tactics by "Sapphire Sleet," known for orchestrating cryptocurrency thefts, demonstrates the evolving sophistication of cybercriminal groups in exploiting professional networking platforms such as LinkedIn to ensnare victims. To mitigate these risks, individuals and organizations should exercise heightened caution when engaging with unsolicited job-related communications, verify the legitimacy of online portals, and maintain robust cybersecurity practices to protect against such social engineering attacks.

See also:

"BlueNoroff Strikes Again with New macOS Malware" (Jamf Blog)

Microsoft Threat Intelligence ("Sapphire Sleet," X)

Additional stories are included below, as they are of interest to threat intelligence teams:

"Medical Company Fined $450,000 by New York AG Over Data Breach" (SecurityWeek)

"Iranian Hackers Launch Malware Attacks on Israel's Tech Sector" (BleepingComputer)

"France, UK Seek Greater Regulation of Commercial Spyware" (SecurityWeek)

"Police Takes Down BulletProftLink Large-Scale Phishing Provider" (BleepingComputer)

"US Government Issues Guidance on SBOM Consumption" (SecurityWeek)

"Mortgage Giant Mr. Cooper Says Customer Data Exposed in Breach" (BleepingComputer)

"Microsoft: BlueNoroff Hackers Plan New Crypto-Theft Attacks" (BleepingComputer)

"Intel Sued Over 'Downfall' CPU Vulnerability" (SecurityWeek)

"McLaren Health Care Says Data Breach Impacted 2.2 Million People" (BleepingComputer)

"Maine Govt Notifies 1.3 Million People of MOVEit Data Breach" (BleepingComputer)

"Hackers Breach Healthcare Orgs via ScreenConnect Remote Access" (BleepingComputer)

Please find past standups at https://fp.tools/home/intelligence/standup.