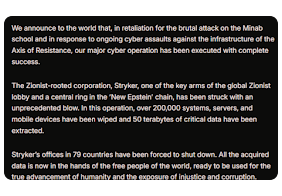
View in browser

Daily Threat Brief

Recent cyber incidents demonstrate escalating threats to financial institutions with Middle East exposure. Iran-backed groups conducted destructive attacks against medical technology firm Stryker, affecting global operations including supply chains [1]. The UAE successfully thwarted ransomware attacks targeting critical infrastructure [6]. Geopolitical tensions amplify cyber risks, with Iranian threat actors targeting US firms across multiple sectors [2]. Financial services face heightened targeting due to valuable data and critical operations. Supply chain attacks using AI-enhanced techniques are emerging [10], while traditional social engineering campaigns continue targeting developers [11].

Issue #1 | March 11, 2026

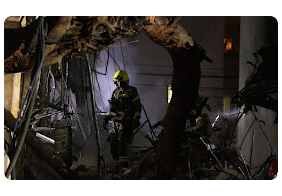
TTPs related to Iran-based APTs



Iran-Backed Hackers Claim Wiper Attack on Medtech Firm Stryker

Krebs on Security / Mar 11, 2026

Summary and significance: Iran-linked hacktivist group Handala conducted a wiper attack against Stryker Corporation, affecting 200,000+ devices across 79 countries. The attack, attributed to Iran's Ministry of Intelligence and Security, exploited Microsoft Intune to remotely wipe systems. Attackers cited retaliation for a U.S. missile strike on an Iranian school. For our organization, this demonstrates Iran-backed threat actors' capability to conduct destructive attacks against critical infrastructure using legitimate administrative tools, relevant given our Middle East operations and potential exposure to similar targeting vectors.



Impacts from the Iran war on insurance and cybersecurity risks

The Latest / Mar 8, 2026

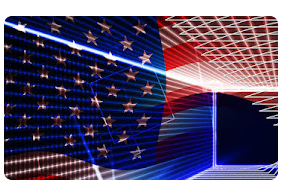
Summary and significance: Iranian cyber threat actors are actively targeting U.S. firms with revenues exceeding $1 billion across multiple sectors. Attacks are expected to be destructive and disruptive rather than financially motivated, including DDoS, data encryption, and phishing campaigns exploiting wartime distraction. Our organization faces elevated risk given our financial sector classification and Middle East operations, particularly regarding data security and infrastructure resilience.

ClickFix Attacks Are Exploiting Windows Terminal to Deliver Malware — And They’re Working

WebProNews / Mar 9, 2026

Summary and significance: ClickFix, a social engineering technique leveraging fake error messages to trick users into executing malicious commands via Windows Terminal, has been adopted by state-sponsored actors including Iranian MuddyWater targeting Middle Eastern organizations. Our organization faces direct risk given our regional operations and financial sector targeting patterns documented in recent campaigns.

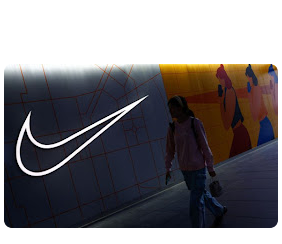
Cyberattacks in the Middle East



FBI is Investigating the ‘Sophisticated’ Hack of Its Surveillance System

Security Boulevard / Mar 6, 2026

Summary and significance: FBI's Digital Collection System Network was compromised via sophisticated techniques exploiting commercial ISP infrastructure. The breach exposed law enforcement sensitive data including pen register/trap and trace surveillance returns and personally identifiable information. Investigation involves FBI, CISA, NSA, and the White House. Significance: Limited direct impact to our organization, though the incident underscores broader US government cybersecurity vulnerabilities that could affect regulatory and operational environments where we conduct business.



Nike: probe into possible data leak after cyberattack claim

Stock Market Listed Companies News - MarketScreener / Jan 27, 2026

Summary and significance: Nike is investigating a potential data breach after cybercriminal group World Leaks claimed to have published 1.4 terabytes of confidential data. The company is assessing the situation; authenticity remains unverified. Limited direct significance for our organization, though the incident underscores evolving ransomware threats affecting major corporations globally.

UAE claims it stopped ‘terrorist’ ransomware attack

The Record from Recorded Future News / Feb 24, 2026

Summary and significance: UAE authorities thwarted a ransomware attack targeting digital infrastructure and vital sectors, attributed to state-sponsored Iranian actors. The incident involved network infiltration attempts, phishing campaigns, and AI-enabled offensive tools. For our organization, this underscores elevated cyber risk to our Middle East operations and reinforces the need for enhanced threat monitoring and incident response protocols in the region.

Cyberattacks Targeting the Financial Sector

PayPal discloses data breach that exposed user info for 6 months

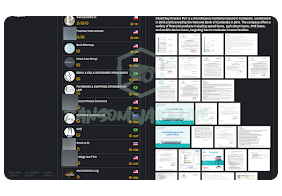
BleepingComputer / Feb 20, 2026

Summary and significance: PayPal disclosed a data breach affecting its Working Capital loan application, exposing customer PII including SSNs from July-December 2025 due to a software error. The company has remediated the issue and offered credit monitoring. Limited direct significance for our organization, though the incident underscores operational security risks inherent in fintech partnerships and third-party integrations we may utilize.

Substack data breach leaks users’ email addresses and phone numbers

Substack data breach leaks users’ email addresses and phone numbers / Feb 5, 2026

Summary and significance: Substack disclosed a data breach occurring in October 2025, exposing user email addresses, phone numbers, and metadata for an unconfirmed number of creators and subscribers. The breach remained undetected for four months. No passwords or financial data were compromised. Limited direct significance for our organization unless we maintain Substack creator accounts or subscriber relationships.

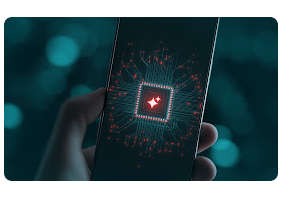


🏴‍☠️ Incransom has just published a new victim : ChokChey Finance

Ransomware.live RSS Feed / Feb 2, 2026

Summary and significance: Incransom ransomware group claimed responsibility for compromising ChokChey Finance, a Cambodian microfinance institution. The attack was discovered February 2, 2026. This incident has minimal direct significance for our organization given the victim's geographic location and business model, though it underscores the persistent threat ransomware poses to financial institutions globally.

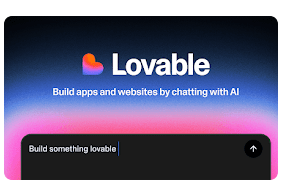
Malware Targeting the Financial Sector



PromptSpy ushers in the era of Android threats using GenAI

ESET Research – security research and expert analysis from ESET Research Labs / Feb 19, 2026

Summary and significance: ESET researchers discovered PromptSpy, the first Android malware using generative AI for UI manipulation. It abuses Google's Gemini to maintain persistence by locking itself in recent apps, deploys a VNC module for remote access, and primarily targets Argentine users. The malware was likely developed in a Chinese-speaking environment.



The DPRK Strikes Again! "Fake Font" Is Latest Threat To Leverage VS Code Tasks

OpenSourceMalware Blog / Jan 24, 2026

Summary and significance: North Korean Lazarus Group targets developers via fake LinkedIn recruiters offering coding assessments. Malicious repos exploit VS Code's task automation to execute JavaScript malware disguised as fonts, deploying InvisibleFerret backdoor that steals cryptocurrency wallets, browser credentials, and establishes persistence.

Malicious NuGet package targets Stripe

RL Blog | ReversingLabs | Threat Research | ReversingLabs / Feb 25, 2026

Summary and significance: Threat actors created a malicious NuGet package called StripeApi[.]Net that mimics the legitimate Stripe[.]net library. The fake package steals API tokens and exfiltrates them to attacker-controlled servers. Though it had 180,000 downloads, most were artificial and the package was removed before real compromise occurred.

Subscribe

Don’t want to receive these emails? Unsubscribe

Made with feedly