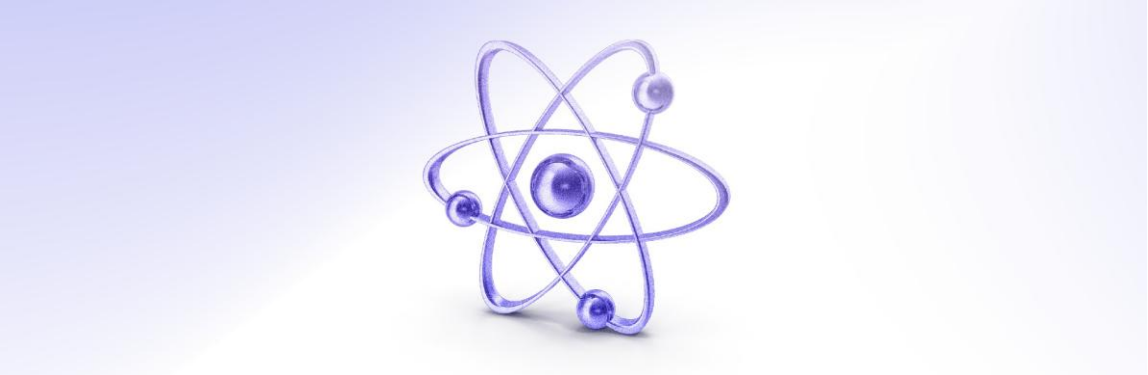
FS-ISAC | Executive Brief

Global Cyber Threat Level | **Americas:** **EMEA:** **APAC:** **July 2025**

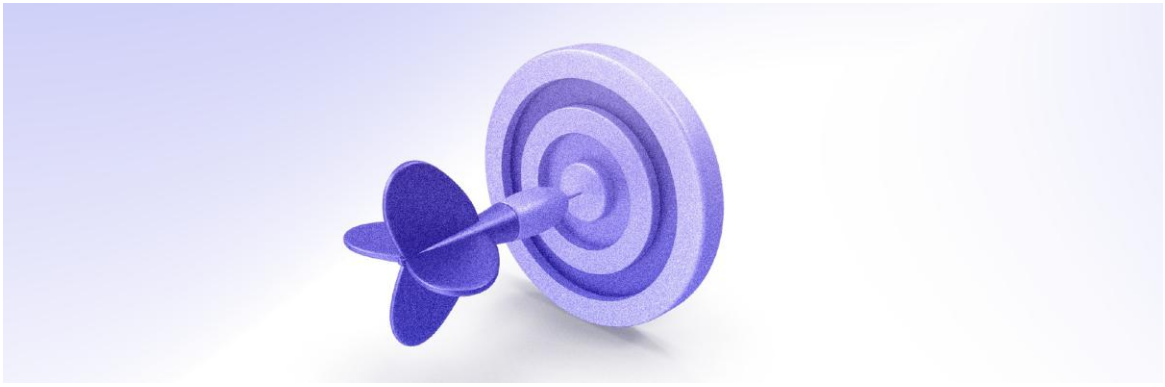
We encourage you to share this brief with other senior executives of your organization or to incorporate this information in your regular reporting processes.



THREAT INTELLIGENCE UPDATE

The 13 June Israeli air strikes on Iranian military, nuclear, and government facilities touched off a series of retaliatory strikes between Israel, Iran, and the United States. In response, the North American Threat Intelligence Committee and EMEA Threat Intelligence Committee raised the Cyber Threat Level to ELEVATED. However, since Iran's missile attack on a US base in Qatar on 23 June, there have been no significant cyber attacks against the US or Europe by Iran-aligned threat actors. The EMEA Cyber Threat Level was downgraded to Guarded on 30 June; the AMER threat level was downgraded on 10 July. The day after the attack on Qatar, Israel and Iran agreed to a ceasefire.

On 4 July, FS-ISAC published an updated Iranian Cyber Threat Assessment regarding developments in the region, assessing that while Iranian cyber activities still present a moderate cyber threat to the financial sector outside of the Middle East, the direct cyber threat is unlikely to have significantly risen. Impacts on the financial sector — outside of Israel — will probably result from attacks on Israeli companies that provide services or otherwise participate in the supply chain, rather than direct attacks. While the situation remains stable, FS-ISAC will continue to monitor and report on new developments.



WHAT'S NEW AT FS-ISAC

FS-ISAC Publishes Annual DDoS Threat Report: From Nuisance to Strategic Threat: DDoS Attacks Against the Financial Sector

The financial services sector was the world's main target in 2023 and 2024 for volumetric DDoS attacks, those designed to overwhelm the target with traffic. Application-layer DDoS attacks against the financial sector increased 23% between 2023 and 2024. These trends indicate that sophisticated threat actors are launching precision-targeted, multi-dimensional assault strategies to exploit complex vulnerabilities in financial services' cybersecurity.

We explored these trends in From Nuisance to Strategic Threat: DDoS Attacks Against the Financial Sector, our annual joint report written with Akamai, the founding partner in our Critical Providers Program. The report includes:

- An analysis of the current DDoS threat landscape, including dominant attack types and threat actors
- Our new DDoS Maturity Model — a structured framework to help firms evaluate their capabilities and map them to current DDoS threats
- Fundamental cyber practices for managing DDoS threats, applicable to firms at all levels of maturity, and a guide to selecting DDoS mitigation providers

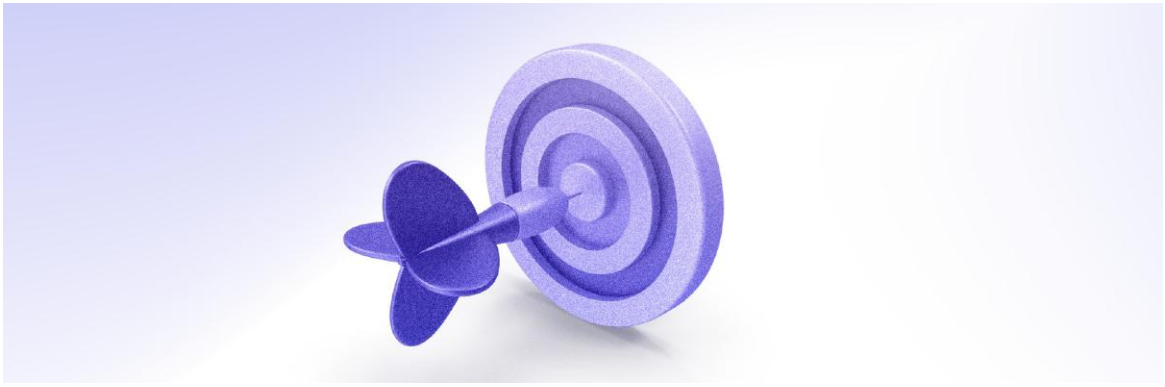
Google and FS-ISAC Launch Financial Services Priority Flagger Program

Google and FS-ISAC announced a new joint effort, the Financial Services branch of Google's Priority Flagger Program (PFP). The initiative will combine Google's advanced threat detection capabilities with FS-ISAC's extensive network and intelligence sharing capabilities to prevent fraud within the financial sector.

Google's Priority Flagger Program streamlines the process of identifying, reporting, and mitigating fraud threats related to Google platforms. As part of this financial services-specific initiative, FS-ISAC now operates a dedicated CONNECT channel for its members to report fraud and other malicious activity leveraging Google Workspace or Google Ads. To join the CONNECT Channel, email GooglePFP@fsisac.com.

The program is part of Google's participation in FS-ISAC's Critical Providers Program, which ensures collaboration and ongoing dialogue between the financial sector and Google.

Read more about leveraging the PFP here, or watch the recording of our Ask the Expert session with Google.



INDUSTRY NEWS

Brazilian Third-Party Social Engineering Scam Nets $100M in a Single Breach

An IT employee at US-based software company C&M was arrested in Sao Paulo in connection with a $100 million theft from a Brazilian financial institution in one night. C&M software connects financial firms to Brazil's Central Bank to enable instant payments on the PIX system, which is used by 76% of Brazilians.

João Roque, one of at least five suspects, said he was recruited by a threat group that bought his workplace credentials to breach the PIX system and make fraudulent transactions. Sao Paulo police stated that their investigation may uncover more financial firm breaches, so total losses could be higher. C&M says social engineering, not software flaws, caused the breach — underscoring the double threat vector of third parties and social engineering.

Read more at AP

Attacks on NVIDIA GPUs Can Degrade AI Accuracy From 80% to Less Than 1%

On 7 July, chipmaker NVIDIA released a security notice warning users of the potential for attacks that could significantly degrade their artificial intelligence (AI) models' outputs.

The attack — a RowHammer variant — permits threat actors to "bypass security boundaries, triggering privilege escalations, data tampering, or even denial-of-service states," says TechRadar. Such exploits could reduce the accuracy of the victim's AI model from 80% to less than 1%, according to The Hacker News, for users of NVIDIA A6000 GPUs (graphics processing units) with GDDR6 memory.

Users are advised to enable Error Correction Codes (ECC) through "nvidia-smi -e 1," use ECC for training nodes or high-risk workloads, and watch for bit-flip attempts by monitoring GPU error logs for ECC-related corrections.

Read more at TechRadar

FS-ISAC | Knowledge

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

AI Risk

- Charting the Course of AI
- More Opportunities, Less Risk: 8 Steps to Protect Financial Services Data with GenAI
- Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks
- Building Cryptographic Agility in the Financial Sector

Post Quantum Cryptography

- The Impact of Quantum Computing on the Payment Card Industry
- Building Cryptographic Agility in the Financial Sector

Fraud

- Leveling Up: A Cyber Fraud Prevention Framework Framework for Financial Services

Phishing/Ransomware/Cloud

- Stop the Scams: A Phishing Prevention Framework for Financial Services
- Ransomware Essentials: A Guide for Financial Services Firm Defense
- Principles for Financial Institutions' Security and Resilience in Cloud Service Environments
- Cyber Fundamentals

Resilience

- Risk and Resilience Report: Subsea Cable Infrastructure
- Resilience in Action - Lessons from the Field

See the full list of Knowledge resources

INSIGHTS FROM TOP LEADERS IN OUR COMMUNITY

Season two of 2025 is here!

- Meg Anderson: Lessons in Cyber Leadership From a Trailblazing CISO
- Jochen Friedemann: The Fun Side of Financial Services Cybersecurity
- Debbie Janeczek: How to Prepare for the Quantum Revolution
- Susan Koski: Managing the Move to the Post-Password Cyber Landscape
- Ariel Weintraub: Ensure Your Supply Chain Continuity – Even Under Pressure

See the full FinCyber Today Podcast catalog

Subscribe

FSISAC
12120 Sunset Hills Rd
Suite 500
Reston, VA 20190

32 Threadneedle Street
London EC2R 8AY
UK

Hong Leong Building
16 Raffles Quay
Singapore 048581