FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 5 January 2026 | Issue 314

This report highlights this week's top risks to support community institution information security and technology teams in proactively protecting their financial institutions from threats that can impair their ability to operate and avoid compliance, economic, legal, regulatory, and reputational impacts.

This Week's Threats

Fraud Campaigns

- Account takeover
- CEO Executive Impersonation
- Fraudulent withdrawals
- Payroll Diversion

System Vulnerabilities

Amazon, Apache, Cisco, Columbia Weather Systems, Cygwin, D-Link, Debian, Dell, GitLab, Google, Hitachi, HPE, IBM, Linux, Microsoft, Mitsubishi, Nessus Agent, Open WebUI, Oracle, Red Hat, Samsung, Ubuntu, and Veam.

Themed Phishing and Smishing Campaigns

Please see the Phishing Daily Digest for all activities. Use keywords for AV blacklists.

Subject Keywords: Adult Dating, Android, Apple ID, Confirmation of Preferred Contact Details, DD DEPOSIT, Expense Reimbursement, Fake Invoice, Gift Card, Pay, PDF, Personal Phone Contact, Request for Updated Contact Information, Time-Sensitive Task, Visa, WhatsApp.

Threats, Malware, Cyber Campaigns, and Adversaries

- AdaptixC2 Beacon
- Aisuru botnet
- Amatera Stealer
- Amadey
- Albiriox
- Astaroth
- Amadey
- AsyncRAT
- BeaverTail
- BianLian
- CastleLoader
- DarkCrystal
- DroidLock
- EdgeStepper
- Eternidade Stealer
- Formbook
- FvncBot
- GlassWorm
- ModiLoader
- Oyster
- PoisonPlug
- Predator Spyware
- PureHVNC
- PureLogs
- PyStoreRAT
- Rhadamanthys Stealer
- Qakbot
- Remcos
- Rust
- SectopRAT
- Shadowpad
- ShadowRay
- ShriveledPeach Malware
- sLoad
- Snakeloader
- SocksShell

- GULoader
- HoldingHands RAT
- JsOUTProx
- LandUpdate808
- Latrodectus
- Lokibot
- Makop ransomware
- Metamorfo
- TamperedChef
- VenomRAT
- Vidar
- Xloader
- XRed
- Xworm
- Zapcat
- ZgRAT

NEWS AND RISK INFORMATION

Cloud file-sharing sites targeted for corporate data theft attacks. “A threat actor known as Zestix is actively selling corporate data stolen from cloud file-sharing services such as ShareFile, Nextcloud, and OwnCloud. The data theft is facilitated by info-stealing malware like RedLine, Lumma, and Vidar.” (Bleeping Computer)

Cybercriminals abuse Google Cloud email feature in multi-stage phishing campaign. “The fact that these emails can be configured to be sent to any arbitrary email addresses demonstrates the threat actor's ability to misuse a legitimate automation capability to their advantage and send emails from Google-owned domains, effectively bypassing DMARC and SPF checks.” (Hacker News)

Cyber threat intelligence report: Top 4 malware targeting finance. “According to Bitsight Threat Intelligence, malware activity impacted approximately 34 percent of organizations observed, accounting for 36 percent of total attacks over the past year. Financial services organizations remain particularly exposed due to the direct monetization potential of stolen credentials, sensitive customer data, and authenticated system access. The top four malware include 1. banking trojans, 2. Android banking malware, 3. information-stealing malware, and 4. Malware-as-a-Service (MaaS) ecosystems.” (Bitsight)

Missing MFA strikes again: Hacker hits collaboration tools. “Dozens of organizations that use real-time content collaboration platforms appear to have lost not only credentials but also terabytes of hosted data to information-stealing malware being wielded by an initial access broker with a sideline in auctioning large volumes of stolen data.” (Data Breach Today)

VVS Stealer uses advanced obfuscation to target Discord users. “VVS Stealer is a Python-based malware targeting Discord users, employing advanced obfuscation techniques to extract sensitive data. It primarily focuses on stealing Discord tokens and browser information.” (Information Security)

THREAT OF THE WEEK

ClickFix and Black Cat highlight the risks this week.

ClickFix Attack Uses Fake BSOD Screens

Summary

Cyware reports that a new ClickFix social engineering campaign is targeting the hospitality sector in Europe, leveraging a typical response to a fake Blue Screen of Death (BSOD) screen to install malware.

The attack begins with a phishing email purporting to be from Booking[.]com, telling victims that their hotel reservation is cancelled and they are due a significant refund via Booking[.]com. The site is a counterfeit and displays a fake error message.

Victims who click the refresh button are met with a full-screen fake BSOD and are prompted to fix the problem with a malicious PowerShell command that downloads and compiles DCRAT. According to Cyware, the malware can “steal data, spread throughout networks, and deploy additional payloads, such as cryptocurrency miners, further compromising the target's security.”

Black Cat Hackers Use Fake Notepad++ Sites

Summary

The Black Cat hacker group is behind another advanced cyber attack campaign, according to GBHackers. This campaign uses fake Notepad++ download websites to distribute malware and steal sensitive data.

The malware employs advanced tactics, including a multi-layered execution chain and DLL sideloading, which establish persistence and evade detection capabilities. Once the malware is installed, shortcuts are created, leading to backdoor mechanisms that enable the theft of browser credentials, keylogging, and the exfiltration of sensitive data.

Remediation

- Download software exclusively from official websites or verified repositories, verifying file integrity through hash validation and antivirus scanning.
- Deploy endpoint protection solutions that include regular system scanning. Be suspicious of unsolicited download links and unknown software sources.
- Initiate incident response procedures upon detecting botnet infections, including forensic analysis of compromise vectors and thorough system remediation.

DATA PRIVACY WEEK

Are You a Champion?

Summary

The National Cybersecurity Alliance announced that 26–30 January is Data Privacy Week, an "international effort to empower individuals and businesses to respect privacy, safeguard data and enable trust." This year's theme is "Take Control of Your Data."

As part of the effort, the Alliance is encouraging people and businesses to become Data Privacy Champions and promote respect for consumer privacy. The Alliance will provide a customizable toolkit to Champions to further this aim.

Action Items

Champions – and everyone else – are urged to help consumers manage their data and regain control over its dissemination. The Alliance provides these links:

- Managing Privacy Settings
- Controlling Data
- Respecting Privacy

Learn how you can participate. (here)

JUST FOR COMMUNITY INSTITUTIONS

Do You Have Recourse When it Comes to Your ATMs?

Summary

Recent ATM attacks have been a topic of discussion among members of FS-ISAC. A recent survey provides some interesting feedback from community institutions.

Highlights

- 66% have a 24-hour Duty Officer to respond to physical ATM security threats.
- 46% have a first and second maintenance provider who responds to alarm issues.
- 63% alarm the top and bottom of their ATM. Some said they alarm only the top or the bottom.
- 41% have at least two surveillance cameras, and 26% have three cameras.
- 93% have 24-hour access to surveillance cameras.
- 76% include ATM inspections as a part of their opening procedures.

Table 1

		Yes	No	Yes	No	Yes	None	Top	Bottom	Both	One	Two	Three +	Yes	No	Yes	No
1	Does your institution have a 24-hour Duty Officer to respond to physical security threats?	17	27														
2	If the answer to the above question is no, do you have a first and second maintenance provider who responds to alarm issues?			19	20												
3	Do you have alarms (which also provide access logs) for your ATMs to alert you about security incidents?					2	7										
	Top ATM																
	Bottom								7								
	Both									26							
4	Do you have multiple camera coverage for your ATMs to document security incidents? If so, how many cameras are installed per ATM?										5	17	11				
5	Do you have access to surveillance cameras outside of normal business hours?													38	20		
6	Do your opening and closing procedures include ATM															31	12

Workbook last saved: Just now

The Survey Says

ATM security is determined by the firm's size, risk appetite, and complexity. These questions will help you draft a security approach that suits your institution:

- What is your leadership's position towards financial loss?
- Does your institution have a dedicated Bank Security Officer?
- Do you perform an annual threat assessment of branches with ATM(s) and know the local rate of burglaries and theft?
- In the event of an incident, do you have visual evidence that law enforcement can use to identify suspects?

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- 2025 Year in Review
- Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks
- Deepfake Threats, Controls, and Mitigations: A Practitioner's Guide
- FS-ISAC Deepfake Threat Taxonomy: Threats and Controls for Detection Models and Watermarks
- Security Advisory: Software Supply Chain Risk: Protecting Against NPM Software Dependencies
- The Timeline for Post Quantum Cryptographic Migration
- Security Advisory: Protecting CRM and SaaS Platforms
- The Business Information Security Officer: Actionable Advice from Practitioners in Four Industries
- Define the Role, Limit the Risk: The Roles and Responsibilities of AI Usage in Financial Services
- Leveling Up: A Cyber Fraud Prevention Framework for Financial Services

See the complete list of Knowledge resources

INSIGHTS FROM TOP LEADERS IN OUR COMMUNITY

Recent Episodes

- FinCyber Today Podcast

UPCOMING EVENTS

Americas

Members can enroll in the Member Services app to attend events.

- 15 January | Executive Protection Meeting
- 26 January | Monthly CIAC Webinar
- 28 January | CIAC and COFFE Open Forum
- 30 January | Member Success Session

View all Americas events.

TLP GREEN

12120 Sunset Hills Rd, Reston
VA 20190