FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 24 November 2025 | Issue 310

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 Impersonation

System Vulnerabilities

Amazon, Apple, Ashlar-Vellum Cobalt, Atlassian, Check Point, Cygwin, Debian, Dell, AEZA, F5 (Big IP), Festo, Firefox, FluentBit, Fortinet, Grafana, HP, Hitachi, IBM, Lenovo, Microsoft, Mitsubishi, Opto22, Oracle, Red Hat, Rockwell Automation, RSA, SiRcom, SUSE, Ubuntu, VMware, Wireshark, WordPress, and Zenitel.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: Adult Dating, Black Friday Sales, Employee Handbook, Fake Invoice, Insurance Request, RETAINER Invoice INV18561 - Final Payment Request.

Threats, Malware, Cyber Campaigns, and Adversaries

- AdaptixC2 Beacon
- Amatera Stealer
- Amadey
- Astaroth
- Amadey
- AsyncRAT
- BeaverTail
- BianLian
- DarkCrystal
- EdgeStepper
- Eternidade Stealer
- Formbook
- GlassWorm
- GULoader
- HoldingHands RAT
- JsOUTProx
- LandUpdate808
- Latrodectus
- Lokibot
- PoisonPlug
- PureHVNC
- PureLogs
- Rhadamanthys Stealer
- Qakbot
- Remcos
- SectopRAT
- Shadowpad
- ShadowRay
- ShriveledPeach Malware
- sLoad
- Snakeloader
- SocksShell
- TamperedChef
- VenomRAT
- Vidar
- Xloader
- XRed
- Xworm

- Metamorfo
- ModiLoader
- Oyster
- yty
- Zapcat
- ZgRAT

NEWS AND RISK INFORMATION

Breaking down S3 Ransomware: Variants, attack paths, and Trend Vision One defenses. “Recent ransomware developments have shifted focus toward exploiting cloud-native environments, particularly Amazon S3, through misconfigurations and advanced misuse of AWS encryption and access mechanisms.” (Trend Micro)

Hackers steal sensitive data from major banking industry vendor. “One of the banking industry’s biggest vendors is responding to a cyber attack that has compromised some of its clients’ sensitive data. SitusAMC, which major banks use to manage their real-estate loans and mortgages, announced on Saturday that hackers broke into its systems on Nov. 12 and stole data that included banks’ “accounting records and legal agreements,” as well as information belonging to some of those banks’ customers.” (Cybersecurity Dive)

Flaws expose risks in Fluent Bit logging agent. “A set of critical vulnerabilities affecting Fluent Bit, a widely used telemetry agent deployed more than 15 billion times, has been uncovered by cybersecurity researchers. The issues highlight weaknesses in components that organizations depend on to move logs, metrics, and traces across banking, cloud, and software-as-a-service (SaaS) platforms. According to a new advisory published today by Oligo Security, a series of flaws in input handling, tag processing, and output processing reveal that Fluent Bit’s flexibility can become a liability when sanitization fails.” (Infosecurity Magazine)

Multi-threat Android malware Sturnus steals messages from Signal and WhatsApp. “A new Android banking trojan named Sturnus can capture communication from end-to-end encrypted messaging platforms like Signal, WhatsApp, and Telegram, as well as take complete control of the device. Although still under development, the malware is fully functional and has been configured to target accounts at multiple financial organizations in Europe.” (Bleeping Computer)

ShadowPad malware abuses WSUS flaw. “A recently discovered vulnerability in Microsoft Windows Server Update Services (WSUS), identified as CVE-2025-59287, has been actively exploited by threat actors to distribute ShadowPad malware. This modular backdoor, associated with Chinese state-sponsored hacking groups, allows attackers to gain full system access by executing remote code with system privileges.” (Cyware)

The Tsundere botnet uses the Ethereum blockchain to infect its targets. “A newly emerged malware campaign, dubbed Tsundere Botnet, is actively targeting Windows systems through various sophisticated infection mechanisms. This Node.js-based botnet utilizes Ethereum blockchain smart contracts.” (Securelist)

Who Is Dark Storm? The threat actor European security teams can’t ignore. “The threat actor Dark Storm … has emerged as one of the most active pro-Russian hacktivist groups this year, escalating disruptive cyber attacks against several government agencies across Europe and Russia. Known primarily for aggressive Distributed Denial-of-Service (DDoS) operations, the group is widening its targets, deepening alliances, and promoting DDoS-as-a-Service offerings to other threat actors across the underground ecosystem.” (Cyber Express)

THREAT OF THE WEEK

Cyber Monday threats and ShinyHunters top the risks this week.

Holiday Deals Lower Costs of Phishing Campaigns

Summary

Every year, Black Friday and Cyber Monday bring deep discounts across the tech industry, including web hosting providers and domain registrars. Although intended for legitimate consumers, they provide malicious actors with crucial resources at minimal cost.

Indeed, combined with bulk website registration tools like NameCheap's "Beast Mode," threat actors can purchase hundreds of domain names for under $50 in seconds and use typosquatting tactics to bypass traditional filters. Cheap "disposable domains" enable attackers to frequently rotate victim landing pages, making it harder for cyber defenders to detect and track malicious infrastructure. And if threat actors typically use a typosquatted pattern in domain names, discounted registrations make it easier to buy additional blocks of domains with varied patterns, increasing flexibility and evasion capabilities.

Website Registration Discounts | As of 19 November 2025

Registrar	TLD	Black Friday Price	Reduced From	Comments
Hostinger	.COM	$0.99	$19.99	Standard phishing top-level domain (TLD); low cost.
Hostinger	.ONLINE	$0.99	$34.99	Low cost.
Namecheap	.COM	$9.98	$14.98	Standard phishing TLD; low cost.
Namecheap	.SHOP	$0.48	$39.99	Commonly seen typosquat TLD, also low cost.
Namecheap	.ORG	$6.48	$12.98	Highly valuable for "official"-looking scams.
Namecheap	.XYZ	$1.98	$19.48	Abundant domain name availability.
Dynadot	.BIZ	$1.50	$5.50	Professional/business theme.
Cloudflare	.WORK	$7.20	N/A	Professional/business theme.
GNAME	.TOP	$4.58	$8.40	Novelty TLD; less efficient for mass fraud.
GNAME	.CC	$6.99	$11.68	Generic and tech oriented.

An added challenge for cybersecurity teams is the surge in phishing emails during the holidays, which heightens the risk of successful attacks amid increased online activity and reduced user vigilance. Artificial intelligence enables threat actors to generate phishing emails – as well as clone retailer websites and push fake social media ads – that are almost indistinguishable from the real thing. While retail brands remain the primary targets in 2025, financial institutions can still be exploited as gateways for payments, payment processing, or account access.

Prevention Practices

Help consumers protect themselves by reminding them to be aware of scams before, during, and after they shop.

Before You Shop

- **Use secure, private networks:** Never shop on public Wi-Fi. Use your home network or your mobile phone's cellular data.
- **Secure your accounts:** Use unique, strong passwords for every account and enable two-factor authentication where possible.
- **Be skeptical of deals:** If an offer seems too good to be true, it probably is. Research prices on comparison sites and verify deals on official retailer websites.
- **Check retailer legitimacy:** Stick to well-known retailers. Check reviews and look for a BBB Business Profile on BBB.org for unfamiliar brands.

While You Shop

- **Type URLs directly:** Go directly to the store's official website instead of clicking ads or links in emails.
- **Check for "https://":** Confirm the site is secure by checking for URLs that start with "https://" and feature a padlock icon.
- **Use credit cards for protection:** Credit cards offer more fraud protection than debit cards. Avoid using wire transfers or gift cards to pay for online purchases from unknown sellers.
- **Guard your personal information:** Be cautious about any site that asks for an excessive number of personal details.
- **Avoid saving card information:** Don't save your credit card details on unfamiliar websites. It's safer to re-enter it each time.

After You Shop

- **Monitor your accounts:** Regularly check your bank and credit card statements for any unauthorized transactions.
- **Report suspicious activity:** If you see anything suspicious, report it to your bank or credit card company immediately.
- **Watch for phishing attempts:** Be wary of unsolicited emails or texts about order confirmations, shipping issues, or fake delivery notifications. Do not click links or provide information.

Threat Actors Compromise Third-Party OAuth Tokens

Summary

Google’s Threat Intelligence Group (GTIG) observed threat actors, tied to ShinyHunters (UNC6040), compromising third-party OAuth tokens to potentially gain unauthorized access to Salesforce customer instances. Members should know that Salesforce has already taken action to revoke the affected tokens and has removed the applications from the AppExchange.

Salesforce and Mandiant have notified potentially affected organizations.

Adversaries are increasingly targeting the OAuth tokens of trusted third-party Software-as-a-Service (SaaS) integrations. Google notes that they recently observed this issue with the campaign targeting Salesloft Drift.

Action to be Taken

If your institution uses Gainsight integrations, continue to monitor for official communications from Gainsight and Salesforce.

- All institutions should view and audit their SaaS environments:
    - Audit connected apps: Regularly review all third-party applications connected to your Salesforce instance.
    - Review OAuth tokens: Investigate and revoke tokens for unused or suspicious applications.
    - Assume compromise: If you detect anomalous activity from integration, rotate the credentials immediately.

- Read the Salesforce Security Advisory for the latest status: https://lnkd.in/gh4gFK7i

Spyware Allows Cyber Threat Actors to Target Users of Messaging Applications

Summary

The Cybersecurity Infrastructure and Security Agency (CISA) is aware of multiple cyber threat actors actively leveraging commercial spyware to target users of mobile messaging applications (apps). These threat actors use sophisticated targeting and social engineering techniques to deliver spyware and gain unauthorized access to a victim's messaging app, facilitating the deployment of additional malicious payloads that can further compromise the victim's mobile device.

These cyber actors use tactics such as:

- Phishing and malicious device-linking QR codes to compromise victim accounts and link them to actor-controlled devices.
- Zero-click exploits, which require no direct action from the device user.
- Impersonation of messaging app platforms, such as Signal and WhatsApp.

While current targeting remains opportunistic, evidence suggests these cyber actors focus on current and former high-ranking government, military, and political officials, as well as civil society organizations and individuals across the United States, the Middle East, and Europe.

CISA strongly encourages messaging app users to review the updated Mobile Communications Best Practice Guidance and Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society for steps to protect mobile communications and messaging apps, as well as mitigations against spyware.

Mitigating Risks From Bulletproof Hosting Providers

Summary

On 19 CISA, in collaboration with the US National Security Agency, US Department of Defense Cyber Crime Center, US Federal Bureau of Investigation, and international partners, released the guide Bulletproof Defense: Mitigating Risks from Bulletproof Hosting Providers to help internet service providers (ISPs) and network defenders mitigate cybercriminal activity enabled by bulletproof hosting (BPH) providers.

Institutions with unprotected or misconfigured systems remain at high risk of compromise, as malicious actors leverage BPH infrastructure for activities such as ransomware, phishing, malware delivery, and denial-of-service (DoS) attacks. BPH providers pose a significant threat to the resilience and security of critical systems and services.

The resource guide urges ISPs and network defenders to implement recommendations to mitigate risks posed by BPH providers. By reducing the effectiveness of BPH infrastructure, defenders can force cybercriminals to rely on legitimate providers that comply with legal processes.

Read the entire resource guide.

GOVERNMENT AND REGULATORY NEWS

Sector Financial Institution Letter and Other Announcements

CISA

- Hidden Functionality Vulnerability in Festo MSE6-C2M/D2M/E2M Devices Allows Remote Compromise, 24 November

FDIC

- FIL-55-2025, Notice of Proposed Rulemaking on Revisions to the Community Bank Leverage Ratio (CBLR) Framework, 25 November
- FIL-54-2025, Final Rule Adjusting and Indexing Certain Regulatory Thresholds, 25 November
- FIL-53-2025, Compliance Date Extension: Sections 328.4 and 328.5 Amendments to FDIC Official Signs and Advertising Requirements, False Advertising, Misrepresentation of Insured Status, and Misuse of the FDIC's Name or Logo Rule, 25 November

OCC

- OCC 2025-39, Bank Activities: Request for Information on Community Banks' Engagement with Core Service Providers and Other Essential Third-Party Service Providers, 24 November
- OCC 2025-38, Bank Secrecy Act/Anti-Money Laundering: Discontinuation of Annual Money Laundering Risk System Data Collection, 24 November
- OCC 2025-37, Bank Secrecy Act/Anti-Money Laundering: Community Bank Minimum Bank Secrecy Act/Anti-Money Laundering Examination Procedures, 24 November

---

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- Tactical Malware Analysis XWORM
- Technical Analysis of Calendaromatic and CrystalPDF
- 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
- Navigating Cyber 2025
- Define the Role, Limit the Risk: The Roles and Responsibilities of AI Usage in Financial Services
- Cross-Sector Mitigations: Scattered Spider | Guidance for Proactive Defense
- From Nuisance to Strategic Threat: DDoS Attacks Against the Financial Sector
- 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 Season 2
- FinCyber Today Podcast Season 1

UPCOMING EVENTS

Americas

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

- 5 December | Member Success Call
- 15 December | Monthly CIAC Webinar
- 17 December | CIAC and COFFE Open Forum
- 1-4 March | 2026 Americas Spring Summit

View all Americas events.

TLP GREEN

12120 Sunset Hills Rd, Reston
VA 20190