FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 24 February 2025 | Issue 271

This report elevates this week's top risks to assist community institution information security and technology teams in proactively protecting their financial institution from dangers that can impair their ability to operate and avoid compliance, economic, legal, regulatory, and reputational impact.

This Week's Threats

Fraud Campaigns

- Account takeover (web)
- Business Email Compromise
- Unauthorized withdrawals
- Unauthorized wire transfer requests

System Vulnerabilities

Amazon, Apple, Avaya, Cisco, Citrix, Confluence, Cygwin, Debian, Dell, F5, Gitlab, Google, Hitachi, IBM, Linux, Microsoft, OpenSSH, Oracle, Red Hat, RFQ/Invoice, SUSE, Ubuntu, and Zimbra.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: ACTION Required, Amazon, AOL, Bonus Dec 2024 - Q4 2024 Earnings, COMPLETED: Agreement Transcripted Ready for Review, Compromised Website, e-Mail Access Request Updated #6444053110, Gift Cards, Important Request, Meeting Request, Office 365 Renewal, Overdue Invoice, QR, Resume, See attached CSV file, Treat Urgently, and Urgent Request.

Threats, Malware, Cyber Campaigns, and Adversaries

- Astaroth
- AsyncRAT
- BeaverTail (InvisibleFerret)
- BitB
- BLACKWIDOW (aka Lotus)
- Bumblebee (aka ShellSting, Shindig)
- CellikRAT V4.0 Malware
- ClickFix/ClearFake
- ConnectWise RAT
- Credential Pharming
- EvilGinx
- Fake Captcha
- Grandoreiro
- Latrodectus
- LandUpdate808
- LummaStealer
- MetaStealer
- Mispadu
- Nitrogen
- RootDoS
- Safeplay Ransomware
- SocGholish
- SparkRAT
- Typosquatting
- Umbral Stealer
- Xloader
- Xworm
- Zloader

NEWS AND RISK INFORMATION

Critical vulnerability in Pentaho business analytics server. “Hitachi Vantara has issued a security advisory addressing a vulnerability, designated as CVE-2024-37361, in its Pentaho Business Analytics Server. This vulnerability carries a CVSS score of 9.9, indicating a critical severity and potential for significant impact.” (Cybersecurity News)

GhostSocks - Lumma's partner in proxy. “GhostSocks, a Golang-based SOCKS5 backconnect proxy malware, was first identified in October 2023 when it was advertised on a Russian-language criminal forum and supports Microsoft Windows alongside Linux.” (infrawatch)

LockBit ransomware strikes exploiting a Confluence vulnerability. “In a swift and highly coordinated attack, LockBit ransomware operators exploited a critical remote code execution vulnerability (CVE-2023-22527) in Atlassian Confluence servers, targeting an exposed Windows server. This vulnerability, rated CVSS 10.0, enabled unauthenticated attackers to execute arbitrary commands by injecting malicious Object-Graph Navigation Language (OGNL) expressions into improperly sanitized template files.” (GBHackers)

New North Korean macOS cyber espionage tools leverage social engineering tactics. “Among the malicious apps uncovered is DriverEasy.app, an application written in Swift/Objective-C that masquerades as a Google Chrome-related tool. This malware uses social engineering to steal credentials by displaying fake authentication prompts.” (SecurityOnline)

New York amends its Data Breach Notification Law. “New York has amended its data breach notification law twice in the last 60 days to (1) add a 30-day deadline for notifying affected residents, (2) clarify that covered financial entities must still notify the New York Department of Financial Services (NYDFS) in accordance with existing NYDFS cybersecurity regulations, and (3) expand the prior definition of “private information” to include medical and health insurance information.” (JD Supra)

OCC reports security incident involving email system. On 26 February, the Office of the Comptroller of the Currency (OCC) reported an isolated and resolved a security incident involving an administrative account in the OCC email system. The OCC’s investigation analyzed all email logs since 2022 for due diligence. The OCC identified a limited number of affected email accounts that have since been disabled. The OCC reported the incident to the Cybersecurity and Infrastructure Security Agency, as required. There is no indication of any impact to the financial sector at this time. (OCC)

PayPal's "new address" feature abused to send phishing emails. “An ongoing PayPal phishing scam exploits the platform's address settings to send fake purchase notifications, tricking users into granting remote access to online scammers.” (Bleeping Computer)

Salt Typhoon exploited the 2018 Cisco bug to infiltrate US telecoms. “Cisco Talos confirmed that a Cisco vulnerability from seven years ago was used by the China-based Salt Typhoon threat group to infiltrate the networks of major US telecom companies. In abusing the flaw — CVE-2018-0171 — Cisco Talos said the advanced persistent threat group (APT) used valid, stolen credentials to maintain access for long periods, in one case up to three years.” (SC Media)

Two actively exploited security flaws in Adobe and Oracle products flagged by CISA. “The Cybersecurity Infrastructure Security Agency (CISA) has added two security flaws impacting Adobe ColdFusion (CVE-2017-3066) and Oracle Agile Product Lifecycle Management (PLM) (CVE-2024-20953) to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation.” (Hacker News)

THREATS OF THE WEEK

Nation-state APT targeting Signal accounts highlights this week’s risk.

Russian APTs Targeting Signal Accounts

Summary

On 19 February, the Google Threat Intelligence Group (GTIG) reported on multiple Russian APTs' increasing efforts to compromise Signal Messenger accounts. Recently, these groups have targeted Ukrainian military and government accounts for ongoing intelligence gathering.

The most novel and widely used technique in the Russian APTs' attempts to compromise Signal accounts is abusing the app's legitimate "linked devices" feature. This feature allows one Signal account to be used concurrently on multiple devices. Linking devices typically requires scanning quick-response (QR) codes, so threat actors craft malicious QR codes that, when scanned, will link a victim's account to an actor-controlled Signal instance. If the link succeeds, future messages will be delivered synchronously to both the victim and the threat actor in real time, providing an effective means to eavesdrop on the victim's secure conversations without requiring a full-device compromise.

GTIG anticipates the tactics and methods used to target Signal will grow in prevalence in the near term and proliferate to additional threat actors and regions. Researchers also warn that the tactics and methods used for Signal can be used with other messaging platforms, including WhatsApp and Telegram.

THREAT INTELLIGENCE UPDATE

Black Basta Ransomware Gang's Internal Chat Logs Expose Inner Workings

Analysis of millions of leaked messages will help protect the sector's environment.

Introduction and Analyst Insights

Recent access to and analysis of the chat logs used by the well-known and proficient Russia-linked ransomware group Black Basta provide valuable insight into the particular vulnerabilities, vendors, products, tools, and targeting approaches the gang has used in its planning and attacks.

The logs span from 18 September 2023 to 28 September 2024, and provide the tactics (what, who, and how) the group focused on and actionable intelligence from a list of vulnerabilities that can be used to scan for and remediate potential exploitation points and help ensure environments are better protected.

While Black Basta has been mostly inactive since the start of the year, it is believed to be a result of recent internal conflicts that caused several key members to leave the gang — the details the chats provide are considered a goldmine and potential blueprint of the mindset that other groups could also be using.

One cybersecurity firm fed over a million messages into ChatGPT, the firm says, that can summarize the chatbot log data in seconds and help companies dive deeper into the treasure trove of Black Basta's inner workings.

Summary

Late last week, internal chat logs from Black Basta became available. Their analysis provides rare insight into the operations of one of the world's most infamous ransomware groups.

- By sifting through the exposed communications, researchers found exhaustive details about the group's preferred tools and techniques, including custom malware loaders, indicators of compromise, cryptocurrency wallets, and email addresses associated with the syndicate's affiliates.
- The chat logs offer unprecedented insights into the group's operations, with details on victims and exploits, copies of phishing templates used in their cyber-attacks, cryptocurrency addresses associated with ransom payments, and information about ransom demands and victims' negotiations with hacked organizations.
- The logs showed that Black Basta exploited weak credentials, exposed RDP servers, unpatched ESXi vulnerabilities, misconfigured VPNs, and social engineering (vishing and phishing) to gain initial access, often rotating the infrastructure to evade detection and testing new payloads against defenses.
- The chat logs appear to show the gang's efforts in exploiting security bugs in enterprise network devices, such as routers and firewalls that sit on the perimeter of a company's network

and act as digital gatekeepers. The hackers boasted about their ability to exploit vulnerabilities in Citrix remote access products to break into at least two company networks as well as exploit vulnerabilities in Ivanti, Palo Alto Networks, and Fortinet software to carry out cyber-attacks.

- The leaked chats are said to contain 380 unique links related to company information hosted on ZoomInfo, a data broker that collects and sells access to businesses and their employees. The chat logs show the hackers used those links to research the companies they targeted, giving some indication of the number of organizations targeted by the gang over 12 months.
- The chat logs are said to have been shared by a leaker amid “internal conflict.” The conflict appears to relate to members failing to provide victims (who paid the ransom) with functional decryption tools, the group’s targeting of Russian banks — some of the group worried Russian authorities would investigate them in response to geopolitical pressures — and concern about the potential for US government legal action.
- The tone of the chat messages has been described as blunt and even aggressive — sometimes frustrated or exhausted — with the members stating high expectations for deadlines and not sugarcoating failures.
- The logs named several organizations as targets — including automotive company Fisker, health tech provider Cerner Corp., and UK-based travel firm Hotelplan — that had not been publicized as targets previously.
- Cybersecurity firm Hudson Rock fed over a million Black Basta chat messages into ChatGPT, the company says, and launched “BlackBastaGPT,” which can summarize the data in seconds. The program is open to the public, allowing threat intelligence researchers to dive into the group’s internal chats to unpack their ops, tactics, cash flow, and humor.

Key Findings

While there were some discussions about discovering new vulnerabilities it was evident that Black Basta prioritized known weaknesses, often leveraging available tools and proof-of-concept exploits. According to analysis conducted by VulnCheck:

- 62 unique CVEs were mentioned in the Black Basta chat logs, with 53 (85.5%) known to have been exploited and 44 (70.9%) appearing in CISA’s Known Exploited Vulnerabilities (KEV) catalog.
- Black Basta showed a clear preference for targets with known weaknesses, focusing on vulnerabilities that already have available exploits.
- The group seemed to favor widely adopted enterprise technologies, including products like Citrix NetScaler, Confluence Atlassian, Fortinet, Cisco, Palo Alto, CheckPoint, and Microsoft Windows.
- Several older vulnerabilities also appeared in the chats, often as part of a “Top 10 of 2022” list that highlighted widely exploited issues, with one CVE described as “Old but not forgotten.”
- It was found that a mention of a CVE in the chat did not necessarily mean that it was subsequently used in an attack.

Analyzing the timeline between the publication of CVEs and their first mention in the chats provided insight into Black Basta’s targeting speed. Often, discussions (sic) could occur within days of the release of a new security advisory. In a few cases, discussion occurred even before an official publication was posted.

Beyond the CVEs identified in the chats, there was evidence that Black Basta employed a broader arsenal of exploits while targeting vulnerabilities, using:

- **Opportunistic exploitation.** Black Basta appears to have favored existing vulnerabilities and readily available proof of concept exploits for initial access, particularly targeting email services. This reinforces the importance of promptly fixing vulnerabilities known to be weaponized in any exploit framework or security tool.
- **Tooling and techniques.** Discussion frequently referenced tools and platforms such as ZoomInfo, ChatGPT, GitHub, Shodan, Fofa, Metasploit, Core Impact, Cobalt Strike, and Nuclei, a mix of offensive and defensive security tools that underscored the group’s flexible, opportunistic approach.
- **Exploit development and acquisition.** In addition to using known exploits, Black Basta likely also has the resources to develop new exploits and considered purchasing exploits from external groups hesitated to purchase exploits.
-

An analysis found that Black Basta selected its targets based on several key factors:

- **Financial viability and ransom payment potential**: The group tends to prioritize high-revenue companies over a large number of random targets, with discussions suggesting that fewer high-profile targets generate more revenue than mass-targeting lower-value entities. There was a clear emphasis on targeting organizations that are more likely to pay ransoms.
- **Vulnerability-based targeting**: The group discussed specific exploits for initial access and email services, indicating a preference for targets with known weaknesses, with pre-attack reconnaissance that included checking domain and infrastructure vulnerabilities.
- **Industry-specific selection**: Sectors that handle sensitive data — such as financial, legal, and healthcare — are frequently targeted due to their higher likelihood of paying to protect client confidentiality.
- **Access to initial compromise**: Decisions often hinge on whether initial access is available, including leveraging exposed RDP, Citrix, VPN, or email credentials. Some attacks begin with methods like credential stuffing or brute-force attempts.
- **Geographical considerations**: Although Black Basta claims to be apolitical, discussions imply that they may selectively target companies in regions with specific financial or regulatory environments.
- **Use of stolen data for secondary extortion**: In certain cases, the group discussed selling stolen data to competitors or foreign entities, highlighting the attractiveness of targets with valuable intellectual property or business secrets.

Possible Targets Mentioned: Vendors and Products *(compiled by VulnCheck)*

Initial access devices and Microsoft technologies:

- Fortinet: CVE-2024-23109, CVE-2024-23108, CVE-2024-21762, CVE-2024-23113
- Citrix Netscaler: CVE-2023-3519, CVE-2023-3467, CVE-2023-3466, CVE-2023-4966
- Palo Alto Networks Pan-OS: CVE-2024-3400
- Checkpoint: CVE-2024-24919
- F5 Big-IP: CVE-2022-1388
- Juniper OS: CVE-2023-36845, CVE-2023-36844
- ConnectWise: CVE-2024-1709, CVE-2024-1708
- Zyxel: CVE-2022-30525
- Atlassian Confluence CVE-2021-44228, CVE-2024-21683, CVE-2023-22515, CVE-2022-26134
- Intel: cve-2017-5754, cve-2017-5753
- JetBrains CVE-2024-27198
- Microsoft Windows: CVE-2020-1472, CVE-2021-40444, CVE-2021-42287, CVE-2021-42278, CVE-2022-30190, CVE-2022-37969, CVE-2023-36874, CVE-2023-36884, CVE-2024-21338, CVE-2024-26169, CVE-2023-36394, CVE-2023-35628
- Brick Builders Wordpress Theme CVE-2024-25600
- Cisco: CVE-2023-20198
- Gitlab: CVE-2023-7028
- Google Chrome: CVE-2022-0609
- Jenkins CVE-2024-23897
- Linux CVE-2024-1086
- JetBrains CVE-2023-42793
- RARLAB CVE-2023-38831
- VMware Spring CVE-2022-22965
- Microsoft SharePoint CVE-2023-29357
- Microsoft Office CVE-2023-23397, CVE-2023-21716, CVE-2017-11882

Email and communication services (offering a safe vector for phishing campaigns and providing initial access to networks):

- Microsoft Exchange: CVE-2021-26855, CVE-2021-28482, CVE-2021-42321, CVE-2022-41040, CVE-2022-41082, CVE-2023-36745
- Microsoft Outlook: CVE-2024-21378, CVE-2024-21413
- Exim: CVE-2023-42115
- Zimbra: CVE-2022-27925, CVE-2022-37042, CVE-2022-41352
- WordPress SMTP plugins: CVE-2023-6875, CVE-2023-7027

References

- https://techcrunch.com/2025/02/21/a-huge-trove-of-leaked-black-basta-chat-logs-expose-the-ransomware-gangs-key-members-and-victims/

- https://cyberscoop.com/black-basta-internal-chat-leak/
- https://www.bleepingcomputer.com/news/security/black-basta-ransomware-gang-s-internal-chat-logs-leak-online/
- https://cybernews.com/security/black-basta-ransomware-dissected/
- https://vulncheck.com/blog/black-basta-chats
- http://www.hudsonrock.com/blackbastagpt

JUST FOR COMMUNITY INSTITUTIONS

Member Success Session for Tier 7 – 8 Introduced

Summary

FS-ISAC's Member Success team rolled out a new feature on 21 February for tier 7 and 8 members called the "Everything FS-ISAC Q&A Session." The call enabled members to interact with FS-ISAC staff members and ask any membership-related question.

If you missed the call, visit the Member Success Session Recap Connection channel and listen to the recording.

FRAUD UPDATE

Zelle Payments Under Scrutiny

Summary

Observations from cybersecurity firm BioCatch suggest a significant increase in digital scams as financial institutions improve detection and threat actors adjust their tactics. Indeed, one large financial institution told FS-ISAC that nearly 50% of all reported scams between June and December 2024 originated from social media (the firm will begin delaying, declining, or blocking Zelle payments to accounts if they are identified as originating from social media contact starting 23 March).

GOVERNMENT AND REGULATORY NEWS

Home Mortgage Disclosure Act (HMDA)

Summary

As a reminder, credit unions subject to HMDA data collection requirements in calendar year 2024 must submit their loan/application register data using the HMDA Platform by 3 March 2025. Starting 1 January 2025, HMDA reporters must log in with a Login.gov account to access the HMDA Platform.

According to the National Credit Union Association (NCUA), credit unions that meet the following four criteria are subject to HMDA data collection requirements in the 2025 calendar year:

- The credit union's total assets as of 31 December 2024 exceeded $58.
- The credit union had a home or branch office in a Metropolitan Statistical Area on 31 December.
- The credit union originated at least one home purchase loan (other than temporary financing such as a construction loan) or refinanced a home purchase loan, secured by a first lien on a one-to-four-unit dwelling during 2024.
- The credit union originated at least 25 covered closed-end mortgage loans in each of the two preceding calendar years (2023 and 2024) or at least 200 covered open-end lines of credit in each of the two preceding calendar years (2023 and 2024).

If your credit union does not meet all four criteria, you are exempt from filing HMDA data for mortgage loan applications processed in the 2025 calendar year. Submissions for 2025 data are due by 2 March 2026.

Insurance Fund Report Highlights

Summary

The National Credit Union Administration Board held its second open meeting of 2025 and received a briefing by the Chief Financial Officer on the performance of the National Credit Union Share Insurance Fund for the quarter ending on 31 December 2024.

The Share Insurance Fund reported a net income of $78.6 million, $22.3 billion in assets, and $145.9 million in total income for the fourth quarter of 2024. As of the fourth quarter of 2024, the equity ratio was 1.30 percent.

View the entire press release

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- More Opportunity, Less Risk: 8 Steps to Protect Financial Services Data with GenAI
- FS-ISAC 2024 Year-in-Review Report
- Stop the Scams: A Phishing Prevention Framework for Financial Services
- Ransomware Essentials: A Guide for Financial Services Firm Defense
- Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks
- Building Cryptographic Agility in the Financial Sector
- LockBit: Access, Encryption, Exfiltration, and Mitigation

See the full list of Knowledge Resources

INSIGHTS FROM TOP LEADERS IN OUR COMMUNITY

Recent Episodes

- Carsten Fischer: The Need for Speed in Threat Mitigation
- Stephen Sparkes: The Evolution of the CISO Role
- Lindsey Bateman: Keep Your Eyes On The Horizon For Emerging Threats – And New Solutions
- Burim Bivolaku: Financial Sector Collaboration Is Key To Third-Party Risk Management
- Beate Zwijnenberg: Can Cyber Risk be Quantified?
- Josh Magri: The CRI Profile – A Simplified Approach To Better Assessment

UPCOMING EVENTS

Americas

- 9-12 March 2025 | Americas Spring Summit
- 17 March | March CIAC webinar meeting
- 26 March | Member Success Session for New IntelX Users
- 30 April | CIAC Open Forum for Everyone
- 14 May | Member Community Connection, Los Angeles FBI

- 3 June 2025 | FinCyber Today Canada

View all Americas events.

TLP GREEN

12120 Sunset Hills Rd, Reston
VA 20190