FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 3 February 2025 | Issue 268

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.

SPECIAL ANNOUNCEMENT

National Consumer Protection Week 2025

Summary

March is right around the corner — which means **National Consumer Protection Week** (NCPW) isn't far behind. This year, NCPW is 2-8 March 2025. Now's the time to start planning.

During NCPW, local, state, and national organizations — along with people like you — work together to share information about consumer issues and help people learn to spot, report, and avoid scams. Here are some ways to join in:

- **Give out FTC materials**. Order and share free resources on avoiding frauds and scams at Bulkorder.ftc.gov. Order by 3 February to ensure delivery in time for NCPW.
- **Encourage your friends and family to report scams and identity theft to the FTC.** Their reports can help the FTC and its law enforcement partners build cases that stop scams and alert others in their community about current fraud trends.
- **Share FTC resources for every community.** Find consumer protection basics for college students, a dedicated website for the military community, a campaign for older adults, and more.

Let's get involved!

This Week's Threats

Fraud Campaigns

- ACH Fraud
- Account Takeover (phone)
- Business Email Compromise
- Smishing Transaction Alert
- Unauthorized Withdrawals
- Wire Fraud Diversion

System Vulnerabilities

Adobe, Android, Amazon, Apache, Azure, CA Database Mgmt., Chrome, Cisco, CyberArk, Cygwin, Debian, Dell, F5, Google, HPE, IBM, Lenovo, Linux, Microsoft, Mozilla, nginx, Oracle, Red Hat, SUSE, Ubuntu, WatchGuard, and Xerox.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: Amazon, Bank, Exodus Wallet, Gift Card, Global Management Partners, Human Resources, New Year's gif/luck, PayPal, Paypay, Payroll, Time Sensitive, Unpaid Invoice, Your account has been flagged, You've sent a money request, and WOULD THIS WORK AS A GOOD TIME???

Threats, Malware, Cyber Campaigns, and Adversaries

- Astaroth
- AsyncRAT
- BeaverTail (InvisibleFerret)
- Black Basta
- BLACKWIDOW (aka Lotus)
- ClickFix/ClearFake
- Conduent ransomware
- Credential Pharming
- Grandoreiro
- Latrodectus
- LandUpdate808
- LummaStealer
- MetaStealer
- Malicious SSLVPN web authentication Attempts
- Mispadu
- Nitrogen
- SocGholish
- SparkRAT
- Umbral Stealer
- Xloader
- Xworm
- Zloader

NEWS AND RISK INFORMATION

Akamai warns of active attacks from new Mirai variant. “Known as Aquabotv3, the malware exploits a vulnerability in a series of Mitel internet-connected phones. The aim of the threat actors is to create a platform for denial-of-service attacks … Because few organizations actually bother to update the firmware for desk phones it will likely be easy prey for the foreseeable future.” (SC World)

Cybercrime forum seizures. Europol published a press release detailing the seizure of domains and servers belonging to the Cracked and Nulled cybercrime forums that had more than 10 million users in total. Since March 2018, Cracked permitted users to sell stolen login credentials, hacking tools, and servers for hosting malware and stolen data as well as other tools for carrying out cybercrime and fraud. Since 2016, Nulled allowed users to sell stolen login credentials and identification documents, as well as hacking tools and other tools for carrying out cybercrime and fraud. The US Justice Department also unsealed charges against one of Nulled’s administrators, Lucas Sohn. (FS-ISAC)

DeepSeek AI models are vulnerable to jailbreaking. “Research from Palo Alto's Unit 42, Kela, and Enkrypt AI identified susceptibility to jailbreaking and hallucinations in the Chinese company's recently unveiled R1 and V3 models. Cybersecurity firm Wiz disclosed Wednesday that DeepSeek exposed a real-time data processing database to the open internet, allowing security researchers to view chat history and backend data.” (Data Breach Today)

DeepSeek’s popularity sparks a surge in crypto phishing and malware campaigns. “Following the DeepSeek’s rapid popularity, a concerning trend has emerged. Cybercriminals have begun to exploit its growing recognition to launch scams and malware campaigns.” (Cyber Express)

Google fixes Android kernel zero day exploited in attacks. “This high-severity zero day (tracked as CVE-2024-53104) is a privilege escalation security flaw in the Android Kernel's USB Video Class driver that allows authenticated local threat actors to elevate privileges in low-complexity attacks.” (Bleeping Computer)

LockBit ransomware gang teases February 2025 return. “Despite being taken down and humiliated by the National Crime Agency (NCA) coordinated Operation Cronos in February 2024, an unknown individual(s) associated with, or claiming to represent, the LockBit ransomware gang has broken cover to announce the impending release of a new locker malware, LockBit 4.0.” (Computer Weekly)

MediaTek warns critical WLAN vulnerabilities expose millions to remote attacks. “Three particularly concerning vulnerabilities (CVE-2025-20633, CVE-2025-20632, CVE-2025-20631) reside in the WLAN AP driver. An incorrect bounds check could allow remote code execution without needing any additional privileges or user interaction.” (Security Online)

Meta confirms zero-click WhatsApp spyware attack targeting 90 journalists and activists. "The campaign … involved the use of spyware from an Israeli company known as Paragon Solutions. The attackers were neutralized in December 2024." (Hacker News)

THREATS OF THE WEEK

Tax scams, phishing, and system vulnerabilities highlight this week's risks.

'Tis the Season for Tax Phishing

Summary

It's that time of year again and the possibility of phishing scams takes the usual tax-time anxiety to a whole new level as the Internal Revenue Service warns that fraudulent tax professionals are behind tax-related identity theft and financial harm.

These phishing and related scams are designed to trick the recipient into disclosing personal information such as passwords and bank account, credit card, and Social Security numbers, or into sending gift cards or wire transfers to the scammer.

US consumers and companies should be extra vigilant, know the different phishing terms, and be aware of what the scams might look like:

- **Phishing/smishing** – Phishing (emails) and smishing (SMS/texts) attempt to trick the recipient into providing sensitive information or downloading malware — i.e., malicious software — by clicking a link. Phishing emails are often sent to multiple email addresses at an organization to increase the chance someone will fall for the trick.

- **Spear phishing** – This email phishing scam is more specific in that it targets potential victims individually and delivers a more effective email known as a "lure." These types of scams can be harder to identify because they are personalized, which makes the email seem more legitimate.

- **Whaling** – Whaling attacks generally target leaders or other executives with access to large amounts of sensitive information at an organization or business. Whaling attacks can also target human resources or accounting office personnel.

Cloud-based schemes aimed at tax preparers

The IRS and tax preparers continue to see attacks that exploit cloud-based applications.

- These Cloud-related schemes trick their victims with realistic-looking phishing emails that contain links to websites that mimic cloud storage sites that look legitimate but are frauds designed to collect the tax preparer's credentials which the threat actor uses to access the real cloud storage site.

- Tax professionals using cloud-based applications are warned to store information or run tax preparation software using multi-factor authentication to help safeguard data. Multi-factor authentication requires at least two forms of identity, such as a password and a fingerprint, providing an extra layer of security.

Red flags when choosing a tax professional

"Ghost" preparers - The IRS requires that paid tax preparers sign returns. Unscrupulous "ghost" preparers, however, have the taxpayer sign and send the IRS their tax returns. These scammers often promise large refunds or charge low fees based on the refund amount. These red flags of unethical behavior can indicate fraud.

Valid ID for tax preparers - Taxpayers should always choose a tax preparer with a valid Preparer Tax Identification Number (PTIN). By law, anyone who is paid to prepare or assists in preparing federal tax

returns must have a valid PTIN. Paid preparers must sign and include their PTIN on any tax return they prepare.

Safe tax preparers for employers

Employers need to understand their payroll and employment tax responsibilities and choose a trustworthy tax prep service. Here are a couple of options:

- **A certified professional employer organization.** Typically, these organizations are solely liable for paying the customer's employment taxes, filing returns, and making deposits and payments for the taxes reported related to wages and other compensation. They file employment tax returns and deposits and pay the combined tax liabilities of their customers using the CPEO's Employer Identification number. An employer enters into a service contract with a CPEO and then the CPEO submits Form 8973, Certified Professional Employer Organization/Customer Reporting Agreement to the IRS. Employers can find a CPEO on the Public Listings page of IRS.gov.

- **Reporting agent**. This is a payroll service provider that informs the IRS of its relationship with a client using Form 8655, Reporting Agent Authorization, which is signed by the client. Reporting agents must deposit a client's taxes using the Electronic Federal Tax Payment System and can exchange information with the IRS on behalf of a client, such as to resolve an issue. They are also required to provide clients with a written statement reminding the employer that it, not the reporting agent, is ultimately responsible for the timely filing of returns and payment of taxes.

Reporting an IRS impersonator

The IRS **doesn't initiate** contact by email, text, phone, or social media to request personal or financial information, and you can verify a suspicious message with the IRS. If you think it's a scam, report it:

- Email
- Letter or notice
- Social media message
- Text message
- Phone call
- Fax

If your Social Security number (SSN) or individual tax identification number (ITIN) was stolen, immediately report it to IdentityTheft.gov.

High-Severity Security Vulnerabilities in SimpleHelp 5.5.7 and Earlier

Summary

Threat actors exploit SimpleHelp Remote Monitoring and Management (RMM) software vulnerabilities to gain initial access to the target network. SimpleHelp remote support software v5.5.7 and before has a vulnerability that allows low-privilege technicians to create API keys with excessive permissions.

Risk

These API keys can escalate privileges to the server admin role.

Remediation

For specific remedial action, please review the recommendations at:

- SimpleHelp
- CVE-2024-57726

- CVE-2024-57727
- CVE-2024-57728

THREAT INTELLIGENCE UPDATE

Breaches That Should Not Have Been

Annual Identity Theft Resource Center's 2024 Annual Data Breach Report highlights.

Summary

The Identity Theft Resource Center (ITRC) released its 2024 report. While the number of incidents did not eclipse the number of breaches in 2023, the number came close. A copy of the report has been provided for CIAC members in Connect.

2024 Statistics

The ITRC says it tracked 3,158 data compromises that resulted in more than 1.7 billion notices sent to individuals, and that the "number of compromises is essentially flat with the previous record-breaking year, but the number of victim notices is up 312%."

The report reveals the following:

- A significant number of data compromises could have been avoided with basic cybersecurity.
- Federal and state disclosure regulations do not have the intended prevention effects, but state privacy laws may — see below.
- The impact of data breaches on individual consumers is masked by the scale of mega-breaches.
- It is hard to quantify the impact of artificial intelligence on data compromises at this point; however, there are red flags.

The report also says, "Despite the disconcerting overall trend lines, there is some good news. Forty percent of states have adopted comprehensive privacy laws, all but one of which includes mandatory cybersecurity standards. As we head into the 2025 state legislative season, expect to see more state privacy laws introduced and passed in the absence of a uniform federal privacy law. There is also an advancement in technology that is rapidly being deployed by companies and adopted by consumers that has the potential to all but eliminate an entire class of cyber-attacks. The technology involves the use of "passkeys" that make stealing or using stolen passwords obsolete."

Download the entire report here.

JUST FOR COMMUNITY INSTITUTIONS

Malicious Use of Generative AI Systems

New reports about AI risks remind all users to do your due diligence!

Summary

Google Threat Intelligence Group published a new report detailing nation-state threat actors' misuse of its AI platform, Gemini. North Korean APT actors used the platform to draft cover letters and research jobs, likely in support of efforts to create and use fake identities to obtain freelance and full-time jobs at foreign companies.

According to Google, one North Korea-backed group used Gemini to draft cover letters and proposals for job descriptions, researched average salaries for specific jobs, and asked about jobs on LinkedIn. Relatedly, cybersecurity researcher David Kuszmar published a ChatGPT jailbreak flaw dubbed "Time Bandit," discovered in November 2024.

Time Bandit allows threat actors to bypass OpenAI's safety guidelines to obtain detailed instructions on sensitive topics — such as the creation of weapons and malware — by exploiting two weaknesses: timeline confusion and procedural ambiguity.

When the two weaknesses are combined, ChatGPT can be manipulated to think it's working in a hypothetical scenario, operating in the past but using information from the future, allowing it to bypass safeguards. These findings highlight how AI systems enable threat actors to create and develop increasingly convincing, effective, and targeted attacks.

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
- Protecting Financial Data with Encryption Controls
- Principles for Financial Institutions' Security and Resilience in Cloud Service Environments
- Business Information Security Officer (BISO) Program and Role
- Resilience in Action - Lessons from the Field
- Navigating Cyber 2024: Annual Threat Review and Predictions
- Digital Operational Resilience Act (DORA) Implementation Guidance
- Financial Services and AI: Leveraging the Advantages, Managing the Risks
- 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
- Phil Venables: AI in Cybersecurity - Threats, Toil, and Talent

UPCOMING EVENTS

Americas

- 24 February | February Monthly CIAC Webinar
- 26 February | Member Success Session for New IntelX Users
- 9-12 March 2025 | Americas Spring Summit
- 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.

12120 Sunset Hills Rd, Reston
VA 20190