FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 9 December 2024 | Vol. 260

We encourage you to share this report with other senior executives or incorporate it into your regular reporting processes.

This Week's Threats

Fraud Campaigns

- ACH wire transfer
- Account takeover
- Business Email Compromise
- CEO impersonation
- Employee impersonation
- Online account
- Payroll diversion
- Unauthorized withdrawals

System Vulnerabilities

Apache, Atlassian, Brocade, Cleo VLTrader, Debian, Dell, Drupal, F5, Fortinet, GitLab, Harmony, HP, Huawei, IBM, Ivanti, Lenovo, LexiCom, Linux, Microsoft, Mozilla, Oracle, Palo Alto, Red Hat, RSA, SAP, Tenable, Ubuntu, and Trend Micro.

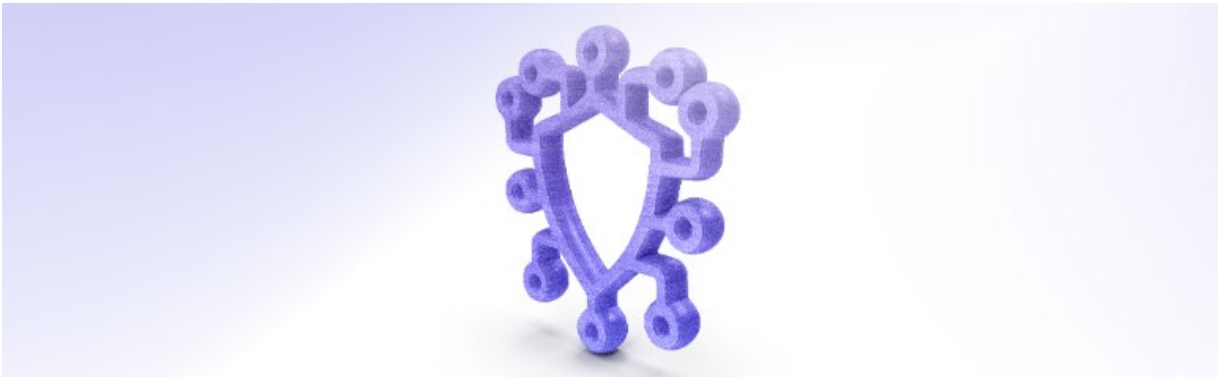
Themed Phishing and Smishing Campaigns

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

Subject Keywords: ACH Details, Changing my ACH, Confirm mobile number, Court Order, Direct Deposit, Do you recognize this transaction, Elite Advisory Services, Financial Advisors, Gift Card, Immediate Task: Step Out to Proceed, Legitimate address, Missing Invoice Payment Report, O365, Overdue Payment, QR, Shared Document, Task, and Invoice, Voided Check, Voided Check, WOULD THIS BE A SUITABLE MOMENT????, and Your credit card has processed.

Threats, Malware, Cyber Campaigns, and Adversaries

- Astaroth
- AsyncRAT
- ClickFix / ClearFake
- Credential Pharming
- Credential Spraying
- Credential Validation
- Domain Spoofing
- Formbook
- Grandoreiro
- JsOutProx RAT
- Latrodectus
- LandUpdate808
- Mispadu
- PortStarter malware
- Snakelogger
- SocGholish
- SPAM Flooding
- Ursa
- VenomRAT
- Xloader



NEWS AND RISK INFORMATION

'AppLite Banker' lures victims with job offers and infects devices with trojan. Attackers posing as job recruiters have launched a mobile-targeted phishing (mishing) campaign that tricks victims into downloading a malicious dropper that installs an updated variant of the Antidot banking trojan on a victim's Android mobile device. The banking trojan variant — dubbed "AppLite Banker" — gives attackers access to corporate credentials, applications, and data when an employee uses the device for remote access by their employer. (SC World)

CVE-2024-12209 (CVSS 9.8): WP Umbrella plugin vulnerability exposes 30,000 websites to compromise. The flaw, identified as CVE-2024-12209 and assigned a CVSS score of 9.8 (indicating a critical severity), could allow unauthenticated attackers to control affected websites completely. (Security Online)

Dell urges immediate update to fix critical power manager vulnerability. A high-severity access control flaw in Dell Power Manager allows privilege escalation. Attackers with local access can execute arbitrary code, bypass security measures, and compromise system confidentiality, integrity, and availability. (Hackread)

DroidBot Android trojan found targeting 77 banks and cryptocurrency exchanges. "DroidBot is a modern RAT that combines hidden VNC and overlay attack techniques with spyware-like capabilities, such as keylogging and user interface monitoring," Cleafy researchers Simone Mattia, Alessandro Strino, and Federico Valentini said. (Hacker News)

Crypto-stealing malware posing as a meeting app targets Web3 professionals. Cybercriminals are targeting people working in Web3 with fake business meetings using a fraudulent video conferencing platform that infects Windows and Macs with crypto-stealing malware. (Bleeping Computer)

Hackers leveraging Cloudflare tunnels, and DNS fast-flux to hide GammaDrop malware. The activity is part of an ongoing spear-phishing campaign targeting Ukrainian entities since at least early 2024 that's designed to drop the Visual Basic Script malware, Recorded Future's Insikt Group said in a new analysis. (Hacker News)

Hundreds of Cisco switches are impacted by bootloader flaws. Cisco released security patches for a vulnerability, tracked as CVE-2024-20397 (CVSS score of 5.2), in the NX-OS software's bootloader that attackers could exploit to bypass image signature verification. (Security Affairs)

NIST issues updated cyber guides focused on assessments and communication. The National Institute of Standards and Technology (NIST) issued two new updates to its existing literature on gauging the efficacy of organizations' cybersecurity protocols, addressing both the selection and maintenance of a proper cybersecurity program depending on organizational needs. (NextGov)

Radiant links $50 Million crypto heist to North Korean hackers. The attribution comes after investigating the incident, assisted by cybersecurity experts at Mandiant, who say the attack was conducted by North Korean state-affiliated hackers known as Citrine Sleet, aka "UNC4736 and "AppleJeus." (Bleeping Computer)

SAP issues critical patch for NetWeaver AS for JAVA. One of the most urgent issues, CVE-2024-47578, affects SAP NetWeaver AS for JAVA (Adobe Document Services). This vulnerability, combined with two related CVEs—CVE-2024-47579 and CVE-2024-47580—allows for severe exploitation risks. (Cybersecurity News)

Vulnerability in WPForms plugins affects 6 million WordPress sites and enables payment refunds and subscription cancellation. The vulnerability assigned a CVSS v3.1 base score of 8.5, allowing authenticated attackers with subscriber-level privileges or higher to execute unauthorized refunds of Stripe payments and cancellations of Stripe subscriptions. (Wordfence)

THREATS OF THE WEEK

Holiday fraud and Deloitte's alleged breach highlight this week's risks.

Summary

According to the Internet Crime Complaint Center's (IC3) 2023 report, non-payment and non-delivery scams cost people more than $309 million that year. Credit card fraud accounted for another $173 million in losses.

Scams include:

- Non-delivery scams, where you pay for goods or services you find online, but you never receive your items
- Non-payment scams, where you ship purchased goods or services, but you never receive payment for them
- Auction fraud, where a product you purchase was misrepresented on an auction site
- Gift card fraud, where a seller asks you to pay with a pre-paid card

As Americans move past the holiday season, the Internal Revenue Service and its Security Summit partners want to alert taxpayers and tax professionals to avoid scams and protect their sensitive data from identity thieves during the upcoming 2025 tax season.

Taxpayers should be wary of a variety of email scams. Throughout the year, taxpayers should be aware of different types of email phishing scams that identity thieves and scam artists commonly use.

Alleged Deloitte Breach

Summary

On 4 December, the Brain Cipher ransomware group listed Deloitte UK on its victim site. Brain Cipher claimed to have stolen more than 1TB of compressed data from the company as part of the alleged breach. As of 6 December, a Deloitte spokesperson informed InfoSecurity that its investigation indicates the allegations relate to a single client's system outside the Deloitte network, and "no Deloitte systems have been impacted." The name of the allegedly impacted client has not been made public at this time.

Brain Cipher emerged in June 2024 and used payloads based on LockBit 3.0 after it targeted an Indonesian data center and caused significant disruption to the government and other critical services in the country.

THREAT INTELLIGENCE UPDATE

Productivity Versus Cybersecurity

Which is more important?

Summary

Productivity – it's a noun the US workforce is all too accustomed to. 'Doing more with less' is a standard with which smaller community institutions are familiar.

What happens with demands for higher productivity competing with cybersecurity guidelines? There is going to be conflict. Applications may be created with specific goals in mind; however, giving one to an employee means expanding application use in a manner the developer couldn't foresee. Security practitioners are left looking to balance productivity and security.

At financial institutions, employees have and do access to confidential customer and financial information daily; however, a question worth asking is how are they doing so – on-site, hybrid, remote?

Access, Risk, and the Modern Workforce

Help Net Security recently reported on a survey conducted by CyberArk titled, "Access, Risk, and the Modern Workforce" which surveyed 14,003 employees in the UK, USA, France, Germany, Australia, and Singapore to uncover workforce behaviors to which security teams are most keen to put a stop to. Participant responses revealed:

- Two-thirds (66%) say they perform one or more highly valuable (for an attacker) actions with the tools or systems they access and use at work, with two in five (40%) downloading customer data, a third (33%) altering critical or sensitive data and just over three in 10 (30%) approving large financial transactions.

- The findings also show that this level of access is standard across departments, showing that privilege is no longer reserved for IT admins.

- All (100%) employees surveyed access work applications and services from their corporate device, including access communications and collaboration tools e.g. Teams, Slack, Outlook (52%), IT admin and management tools (41%), and customer-facing apps (34%). These are business-critical applications that contain sensitive and privileged data. Meanwhile, four in five (80%) of those surveyed also access work applications and services from personal devices.

- Almost half (49%) of people surveyed use the same login credentials to access multiple work-related applications and almost two in five (36%) use the same login credentials for personal and workplace applications and services.

- Over a third (35%) use external personal storage services to store and share workplace-related information with external parties and three in 10 (30%) share workplace-related passwords and credential logins with co-workers.

While the majority of employees do not intend to harm their employer, mistakes raise additional risks, without including adversarial attacks.

Productivity Priorities Versus Security

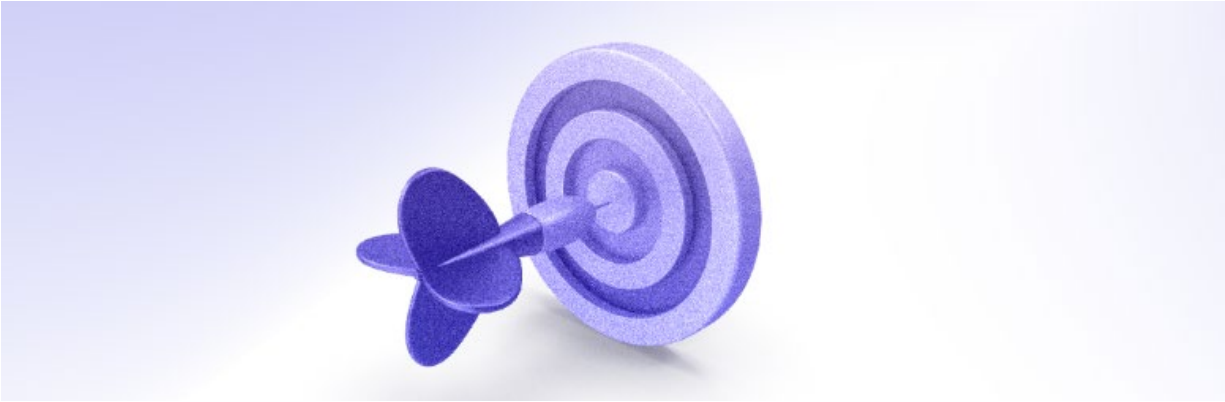
The data shows that a high percentage (65%) of employees surveyed are finding ways to get around cybersecurity policies in the name of productivity and that this is not a question of which security policies are bypassed, but which ones are bypassed on any given day. Over a quarter (27%) of those surveyed use one password across multiple accounts to avoid aggravation, while a fifth (20%) say they use personal devices as WiFi hotspots.

While the report only highlights high-risk activity, it is not broken down by industry, yet it's a topic worthy of discussion when you think about risk management.

Solutions?

In addition to rising productivity requirements, provide employees with guidelines that help them achieve those requirements in a safer environment.

Institutions can make decisions based on management's risk appetite, size, and complexity; however, there are available solutions that should be considered including, requiring the use of multifactor authentication, establishing security controls for hybrid and remote workers, prohibiting access to internet email accounts and storage, providing employees with an easy-to-use encryption tool, as well as other system policies, reporting and monitoring.



JUST FOR COMMUNITY INSTITUTIONS

Beginning 2025 On the Right Path

Our multi-series report focuses on helping you to be safe in 2025.

Summary

Community institutions will face increased challenges in the upcoming year – sticking to some basic principles will assist in reducing your risk. Additionally, revisiting your resiliency, incident response, and vendor management programs is essential to achieving regulatory and business goals and guidelines. Finally, continue your education programs for employees and customers alike.

For the next several weeks, we will focus on compliance training and available tools to help you in 2025.

Introduction

Regardless of whether you work with a training department or are responsible for employee and customer service security awareness training, reaching your audience is not only a sound business practice – it's a regulatory requirement. Security awareness levels for employees, consumers, and commercial customers vary, which is why your training programs should be engaging, enticing, and sustainable.

Areas to consider include:

1. Plotting your course
2. Leadership buy-in
3. Training that matters to your audience
4. Straight-forward content that is easily understood by the lowest common denominator
5. Continuous security bulletins
6. Using real-life phishing, malware, and social engineering examples

Security Awareness Training for Board Members and Employees

Training ensures personnel have the necessary knowledge and skills to perform their job functions. Training should support security awareness and strengthen compliance with security and acceptable use policies. Ultimately, management's behavior and priorities heavily influence employee awareness and policy compliance, so training and the commitment to security should start with management. Management should educate users about their security roles and responsibilities and communicate them through acceptable use policies.

Management should hold all employees, officers, and contractors accountable for complying with security and acceptable use policies and should ensure that the institution's information and other assets are protected. Management should have the ability to impose sanctions for noncompliance.

The board of directors and senior management set the tone and direction for an institution's use of IT. Also, the board should approve several critical activities including the IT strategic plan, information security program, and other IT-related policies.

The board may delegate the design, implementation, and monitoring of specific IT activities to management or a committee - in smaller or less complex financial institutions that may not have steering committees, these functions would be performed by management, IT department personnel, the board, or a board committee. When given the time to consider the complex nature of information the technology, the changing threat landscape, and the increasing complexity of cyber-campaigns every human is susceptible to being hacked given time, condition, and opportunity.

One cannot expect an institution to understand the granular aspects of important issues if its Board members do not. To carry out their responsibilities, board members should understand IT activities and risks. Therefore, the awareness content should fit the audience.

In our next issue, we shall discuss size and complexity.

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- 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

- 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

- 16 December | December CIAC Webinar
- 15 January | Tampa Bay Member Forum (co-hosted by Raymond James)
- 15 January | Tampa Bay Community Connection
- 29 January | CIAC & COFFEE
- 29 January | Member Success Session for New IntelX Users
- 9-12 March 2025 | Americas Spring Summit
- 3 June 2025 | FinCyber Today Canada

View all Americas events

TLP GREEN

12120 Sunset Hills Rd, Reston
VA 20190