FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 17 February 2025 | Issue 270

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 (phone)
- Business Email Compromise
- Unauthorized withdrawals
- Unauthorized Wire Transfer requests

System Vulnerabilities

Apache, Broadcom, Citrix, Cygwin, Debian, Dell, F5, GnuTLS, IBM, Lenovo, Linux, Microsoft, Mozilla, OpenSSH, Oracle, Red Hat, SUSE, Ubuntu, VMware, and WatchGuard.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: Acrobat Sign, Adobe SixBox, Board Operating Expense, Electronic Funds Transfer Completed, FIS, Gift Card Request, New Payroll Dates and Updated Paycheck Amounts, paypay-login-ne-jp, SAP spoofing, Sextortion, and Shared Document.

Threats, Malware, Cyber Campaigns, and Adversaries

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

NEWS AND RISK INFORMATION

AMD patches multiple vulnerabilities in embedded processors. "AMD has released security updates addressing multiple vulnerabilities in its EPYC and Ryzen Embedded processors, some of

which could allow arbitrary code execution, memory corruption, or privilege escalation." (Cybersecurity News)

Android's new feature blocks fraudsters from sideloading apps during calls. "The new in-call anti-scammer protections include preventing Android users from turning on settings to install apps from unknown sources and granting access to the Accessibility Services." (Hacker News)

CERT-In warns of high-severity vulnerabilities in Mozilla Firefox and Thunderbird. Mozilla has responded swiftly to these vulnerabilities, releasing a series of security fixes in updated versions, including Firefox 135, Firefox ESR 115.20, Firefox ESR 128.7, Thunderbird 135, and Thunderbird ESR 128.7. (The Cyber Express)

Inconsistent security strategies fuel third-party threats. "About 47% of organizations have experienced a data breach or cyber-attack over the past 12 months that involved a third party accessing their network, according to Imprivata and the Ponemon Institute." (Help Net Security)

Juniper warns of critical authentication bypass flaw in session smart routers. "Currently, Juniper SIRT is not aware of any malicious exploitation of the common vulnerabilities and exposures (CVEs) CVE-2025-21589 vulnerability. However, given the severity of the flaw, prompt action is crucial to prevent potential attacks." (SecurityOnline)

Man found guilty in SEC X account hack. "On 10 February, 25-year-old Eric Council Jr. pleaded guilty to hacking the SEC's X account in January 2024. The attack allowed his co-conspirators to make a fake announcement that Bitcoin ETFs were approved for listing on registered national security exchanges. The post caused Bitcoin's value to briefly jump by $1,000. The SEC confirmed the account was compromised through a SIM-swapping attack targeting the account holder's phone number and multi-factor authentication (MFA) was not enabled for the account. Using a hardware token or authentication app for MFA can prevent unauthorized access even after SIM swapping." (FS-ISAC)

Microsoft warns of a new XCSSET macOS malware variant used for cryptocurrency theft. "A new variant of the XCSSET macOS modular malware has emerged in attacks that target users' sensitive information, including digital wallets and data from the legitimate Notes app." (Bleeping Computer)

SonicWall and Palo Alto Networks flaws are under attack and have been added to the CISA list. **"**Authentication bypass vulnerabilities in SonicWall SonicOS SSLVPN and Palo Alto Networks PAN-OS have been added to the Known Exploited Vulnerabilities (KEV) catalog by the US Cybersecurity and Infrastructure Security Agency (CISA). The SonicOS SSLVPN flaw tracked as CVE-2024-53704, which was given a critical CVSS score of 9.8 by the National Institute of Standards and Technology (NIST), enables a remote attacker to hijack SSLVPN sessions and gain unauthorized access to the victim's network." (SC Media)

Two new OpenSSH bugs threaten enterprise security, uptime. "Qualys discovered the bugs (CVE-2025-26465 and CVE-2025-26466) in January, per its disclosure timeline. These vulnerabilities enable machine-in-the-middle (MitM) attacks and pre-authentication denial-of-service (DoS) attacks." (The Register)

The US indicts Russian nationals. "On 10 February, the United States Department of Justice unsealed criminal charges against Roman Berezhnoy and Egor Nikolaevich Glebov for allegedly operating a ransomware affiliate organization named 8Base. The individuals were arrested this week because of an international operation disrupting their organization. Their organization allegedly targeted over 1,000 public and private entities in the US and worldwide using the Phobos ransomware, receiving over $16 million in ransom payments. The 8Base ransomware group has previously targeted a variety of industries including finance, manufacturing, and education." (FS-ISAC)

THREATS OF THE WEEK

Distributed Denial of Service attacks targeting DNS highlight this week's risk.

DNS DDoS Attacks

Summary

FS-ISAC insurance council members report Domain Name Service Distributed Denial of Service (DNS DDoS) attacks.

DNS attacks attempt to disrupt the resolution and functionality of internet protocol (IP) addresses either by redirecting users to malicious websites or intercepting their internet traffic to gain unauthorized access.

DNS DDoS attacks can be mitigated by using rate limiting, access control lists, and DNS caching. You can also monitor DNS traffic and implement Domain Name System Security Extensions (DNSSEC).

Remediation

While there is no way to completely avoid becoming a target of a DDoS attack, administrators can take proactive steps to reduce the effects of an attack on their network.

- **Geographically distribute anycast DNS networks.** It expands the surface area to absorb large-scale attacks.
- **Increase record time-to-live (TTLs) values.** It helps reduce legitimate and illegitimate queries from reaching authoritative nameservers, saving nameserver bandwidth.
- **Disable DNS ANY requests.** That stops attacks from exploiting this record type to augment amplification attacks.
- **Relay DNS servers.** It can delay responses, saving bandwidth if a certain resolver is sending an excessive amount of traffic. Sophisticated servers can incorporate smaller rate-limiting logic (e.g. queuing requests from a specific resolver or client that is responsible for a spike in NXDOMAIN responses).

THREAT INTELLIGENCE UPDATE

Rising Cybercrime Benefits State-Backed Groups

State-backed groups use cybercrime to fund operations.

Summary

Google Threat Intelligence Group (GTIG) published a report that stated cybercrime comprises a majority of online malicious activity, benefiting state-backed advanced persistent threats (APTs).

APTs benefit from cybercrime as they can purchase cyber tools on the dark web or even co-opt criminal groups to conduct operations such as information stealing, service disruption, and more. Criminal and state-sponsored operators have overlapped for some time, but growing resource constraints and operational demands have encouraged APT groups to leverage tools and malware frequently used by criminal groups.

One example of this linkage is Russia's APT44 (aka Sandworm) using cybercriminal malware such as Radthief and Warzone in several campaigns in Poland and Ukraine. Chinese, North Korean, and Iranian threat actors have also been detected conducting cyber-attacks for espionage and financial gain. Yet even without collaboration with state-sponsored actors, cybercriminals remain a serious threat to critical infrastructure, particularly the financial sector.

GTIG recommends elevating cybercrime as a national security priority by prioritizing intelligence collection and analysis on cybercriminal organizations and enhancing international cooperation.

JUST FOR COMMUNITY INSTITUTIONS

Ghost (Cring) Ransomware Guide

Joint agency advisory regarding Ghost ransomware released

Summary

CISA, the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) jointly published a cybersecurity advisory, #StopRansomware: Ghost (Cring)

Ransomware. This advisory provides known indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with Ghost ransomware actors identified through FBI investigations.

Ghost actors target and compromise organizations that have outdated and/or unpatched versions of software and firmware on their internet-facing services. These malicious ransomware actors are known to use publicly available code to exploit CVEs to gain access to internet-facing servers. The known CVEs are CVE-2018-13379, CVE-2010-2861, CVE-2009-3960, CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207.

Remediation

Recommended mitigations and actions to protect against Ghost ransomware include:

- Maintaining regular system backups
- Patching known vulnerabilities
- Segmenting networks
- Requiring phishing-resistant MFA for access to all privileged accounts and email services accounts
- Training users to recognize and report phishing attempts

Institutions should review the advisory, IOCs, and TPPs and implement recommended mitigations to protect against the ransomware threat actor.

FRAUD UPDATE

Account Takeover Self-Service Wire Transfer Fraud

Summary

FS-ISAC members report self-service account takeover (ATO) wire transfers. Wire transfers come from guaranteed funds and can be immediately directed to the recipient's account. Cybercriminals may gain access to a victim's online account through a variety of methods:

Brute forcing username/password. A cybercriminal exploits weak passwords and lack of MFA.

Phishing emails. A cybercriminal sends a deceptive email to trick the victim into divulging their login credentials.

Phishing domains/websites. A cybercriminal uses a phishing website that looks like a legitimate online banking or payroll website to trick the victim into divulging their login credentials.

Social engineering. A cybercriminal impersonates a bank employee, customer support, or technical support staffer to manipulate the victim into divulging their login credentials.

Data breaches. A cybercriminal obtains the victim's login credentials from past data breaches or criminal forums that sell stolen data on dark web marketplaces.

Malware. A cybercriminal obtains the victim's login credentials via malware on the victim's device.

Remediation

To remain on guard against ATO, follow the tips below:

For financial services firms:

- Be careful about the information your institution or customers share online, including wire transfer instructions, account information, and other personal information. By openly sharing this data, you may innocently give scammers all the information they need to guess passwords or answer security questions.

- Always require unique complex passwords, enable two-factor (or multi-factor) authentication on any account that allows it, and never disable it.
- Require out-of-band verification for wire transfers, especially over a specific dollar amount determined by your risk management assessment.

For customers:

- Monitor financial accounts for irregularities, such as missing deposits.
- Use Bookmarks (Chrome) or Favorites (Edge) to log in to websites rather than clicking on Internet search results or advertisements — some are fraudulent and MFA will not protect you. For that reason, you should carefully examine the email address, URL, and spelling in any correspondence.
- Stay vigilant against phishing attempts. Be suspicious of unknown bank or other financial services employees who call you; don't trust caller ID. Offer to call them back after you look up the phone number yourself. Remember that companies generally do not contact you to ask for your username, password, or one-time password.

GOVERNMENT AND REGULATORY NEWS

UBPR Interest Rate Risk Analysis Page Content Changes

Summary

The Federal Financial Institutions Examination Council's (FFIEC) member agencies made changes to the Uniform Bank Performance Report's (UBPR) Interest Rate Risk Analysis page on or shortly after 22 February 2025. These changes, being led by the Task Force on Surveillance Systems, are part of a previously announced multi-year review of UBPR content.

More information on the changes to the UBPR Interest Rate Risk Analysis page is available at https://www.ffiec.gov/pdf/UBPR/2025_UBPRInterestRateRiskPageChanges.pdf.

OCC Releases Dodd-Frank Act Stress Test Scenarios for 2025

Summary

Section 165(i)(2) of the Dodd-Frank Act, as amended by the Economic Growth, Regulatory Relief, and Consumer Protection Act, requires certain financial companies, including certain national banks and federal savings associations, to conduct periodic stress tests.

Related Links

- 2025 Dodd-Frank Act Annual Stress Test Scenario Information
- *Policy Statement on the Principles for Development and Distribution of Annual Stress Test Scenarios*

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

- 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.

TLP GREEN

12120 Sunset Hills Rd, Reston
VA 20190