FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 7 October 2024 | Vol. 251

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

- Account takeover
- Call center
- CEO impersonation
- Credential pharming
- Customer validation
- Employee impersonation
- Fake invoice
- Gift card requests
- New account fraud
- Online account
- Wire transfer
- Withdrawal and enrollment

Threats, Malware, Cyber Campaigns, and Adversaries

- AgentTesla
- AsyncRAT
- Atera
- Badger (aka BOLDBADGER) Malware
- BRUTERATEL C4
- CarnavalHeist
- ClickFix / ClearFake
- Credential Pharming
- Credential Validation
- Fleetdeck
- Flax Typhoon
- Formbook
- Grandoreiro
- JsOutProx RAT
- Koi Loader/Stealer
- Latrodectus
- LandUpdate808
- NetSupport RAT
- Payroll Diversion
- Salt Typhoon
- SocGholish
- Ursa
- Xloader
- ZPHP

System Vulnerabilities

Adobe, Amazon, Android, Apache, Apple, Azure, Check Point, Cisco, Cygwin, Debian, DeepSpeed, Dell, F5, Extreme Networks, Fortinet, GitLab, GNOME, Google, IBM, Ivanti, Lenovo, Magento, Microsoft, Mozilla, Oracle, Red Hat, Samsung, SAP, Trellix, Ubuntu.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: 2FA: Review, ACH Information Alert, Client Support, Gift Card Request, GitLab, HP, ICCAN Domain Verification, Palo Alto, PAN-OS, Payment, Please Review Your Scheduled Project Details, Purchase Order, QR, Your Email Address Has Been Successfully Updated, Voicemail from, Wireshark, and Zoom Docs.

NEWS AND RISK INFORMATION

ACSC and CISA launch critical OT cybersecurity guidelines. ACSC and CISA have jointly launched a new guide called Principles of Operational Technology Cybersecurity. This guide aims to assist organizations, especially those in critical infrastructure sectors, secure their OT environments. (Info Security Magazine)

Andariel's hacking group shifts its focus to financial attacks on US organizations. Andariel, a North Korean state-sponsored threat actor, is conducting financial attacks on US organizations. While three organizations in the US were recently targeted in August 2024, no ransomware was successfully deployed. (The Hacker News)

Critical Apache Avro SDK RCE flaw impacts Java applications. A critical security flaw in Apache Avro SDK for Java has been revealed, allowing remote code execution on vulnerable systems. The vulnerability, CVE-2024-47561, affects all versions before 1.11.4. (Security Affairs)

LemonDuck unleashes crypto-mining attacks through SMB service exploits. A recent report by security researchers at Aufa and NetbyteSEC reveals the resurgence of the LemonDuck malware, exploiting the EternalBlue vulnerability in Microsoft's SMB protocol for crypto-mining. (NetbyteSEC)

SharePoint, OneDrive, and Dropbox targeted by BEC attacks. Microsoft researchers observed threat actors abusing legitimate file hosting services such as SharePoint, OneDrive, and Dropbox to launch business email compromise (BEC) attacks. threat actors send files with restricted access and "view-only" restrictions — files that typically can easily circumvent standard security controls. (SC World)

Report: phishing sites increasingly target mobile users. Phishing attacks targeting mobile devices have surged, with 82% of phishing sites focusing on mobile users, according to Zimperium Labs. The report attributes the increase to the growing use of personal devices for work, poor cyber hygiene, and AI-powered attackers. (CSO Online)

Threat actors are believed to be spreading the new Medusalocker variant since 2022. BabyLockerKZ has expanded its reach to different continents, shifting from Europe to South America in early 2023. Its ransomware has distinct features compared to MedusaLocker, such as unique storage keys and differences between Windows and Linux versions. (Cisco Talos)

Update: exploit released for TeamViewer flaws letting unprivileged users load arbitrary kernel drivers. These flaws enable attackers to execute arbitrary code and escalate privileges on Windows systems by exploiting inadequate cryptographic signature verification during driver installation. (Security Online)

White House official says insurance companies must stop funding ransomware payments. Insurance companies must stop issuing policies that incentivize making extortion payments in ransomware attacks, a senior White House official said on Friday. The call for the practice to end, which was made without any indication the White House was formally proposing to ban the practice, follows the fourth annual International Counter Ransomware Initiative (CRI) summit in the United States this week, where the 68 members of the CRI discussed tackling the problem. In an opinion piece in the Financial Times newspaper, Anne Neuberger, the U.S. Deputy National Security Adviser for cyber and emerging technologies, warned that ransomware was "wreaking havoc around the world." She wrote: "Some insurance company policies — for example covering reimbursement of ransomware payments

— incentivize payment of ransoms that fuel cybercrime ecosystems. This is a troubling practice that must end." (The Record)

THREATS OF THE WEEK

MoneyGram data theft and Iranian attacks on US politicos' accounts highlight this week's risks.

MoneyGram Cyber-Attack Confirmed

Summary

Following much speculation, MoneyGram confirmed that threat actors successfully stole customer information during a cyber-attack that led to an outage in September. Payments Dive said the shutdown potentially affected millions of people who rely on MoneyGram to send funds to and from some 200 countries and territories.

Stolen data included names, contact information, Social Security numbers, government-issued IDs, and in some cases, utility bills, bank account numbers, and transaction information.

MoneyGram recommends that its customers remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring their free credit reports.

Protection Against Iranian Account Targeting

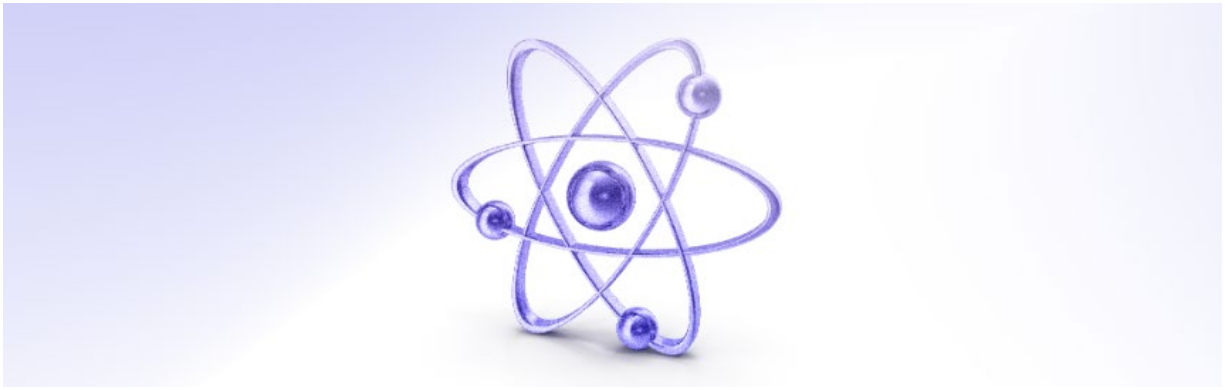
Summary

The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) jointly released a fact sheet, How to Protect Against Iranian Targeting of Accounts Associated with National Political Organizations.

Threat actors affiliated with the Iranian Government's Islamic Revolutionary Guard Corps (IRGC) are targeting and compromising the personal and business accounts of Americans, specifically those associated with national political organizations and campaigns, as well as individuals who have worked on issues related to Iranian and Middle Eastern affairs. IRGC's goal is to stoke discord and undermine confidence in US democratic institutions. This fact sheet provides steps that individuals and organizations can take to enhance their security and resilience to protect themselves against the techniques IRGC has been observed using.

CISA and the FBI urge individuals and national political organizations to apply the recommended mitigations, including protecting their sensitive accounts with phishing-resistant multifactor authentication (MFA).

Family members of targeted individuals are also encouraged to apply mitigations and best practices.



THREAT INTELLIGENCE UPDATE

New Report Reveals Mobile Phishing Trend

Mishing is the fraud-du-jour.

Summary

A recent report by CSO Online shows that over 80% of phishing sites now target mobile devices. Hold on, isn't that called smishing? Apparently, the devil is in the details – specifically, the medium that delivers the attack.

	Mishing	Smishing
Definition	A phishing scam that uses a medium other than email	A type of phishing that uses text messages or messaging apps

Mishing, phishing, smishing, and vishing are the tools bad actors use in social engineering attacks that use fraudulent messages to trick people. Perhaps the greatest difference is the way attacks are conducted. For example:

- Mishing: anything but email
- Phishing: Uses emails and links to steal information
- Smishing: Uses text messages or messaging apps to steal information
- Vishing: Uses voice calls and voicemails to steal information

Though mishing has been around for several years, it may be the fraud-du-jour amongst threat actors. Mobile phishing uses social engineering attacks targeting mobile devices to trick users into giving away their information or downloading malware. Mishing can take the form of SMS messages, phone calls, messaging platforms, or social media apps. This is a wider field of opportunity for the threat actor.

Mishing is effective in multiple environments and surfaces on mobile devices with various screen sizes, varying interfaces, and the ability to hide URLs. Mobile users without adequate speedbumps, such as security awareness training, are also more likely to tap first and ask questions later on a mobile screen than a computer.

So, What Are Common Mishing Tactics?

Effective tactics include:

- URL padding: A legitimate domain is included within a larger URL, but hyphens are added to make the real destination difficult to see
- Tiny URLs: Shortened URLs that direct users to malicious content
- Fake site URLs: Bad actors send fake site URLs via text messages, and users may not be able spot the fake due to the small screen size

Reducing Your Risk

To reduce your risk, use the security tools at your disposal: Mobile Device Management (MDM), multi-factor authentication (MFA), and password managers that generate and store complex passwords that protect systems from re-used password credentials. Require your customers and employees to use these tools as well.

JUST FOR COMMUNITY INSTITUTIONS

Building Cryptographic Agility in the Financial Sector

Improve business continuity when existing cryptography is compromised.

Summary

The cryptography that cybersecurity relies on is vulnerable to changing threats and technological advances, notably quantum computing. The sector needs to be able to change algorithms and architectures more efficiently than it does now in response to emerging risks. Embracing cryptographic (or crypto) agility will help financial services avoid these risks with fewer disruptions to business operations. However, there is no comprehensive definition of or transition governance framework for crypto agility.

To provide them, the FS-ISAC Post Quantum Cryptography Working Group drafted a seminal work on crypto agility, *Building Cryptographic Agility in the Financial Sector*. The Working Group defines crypto agility as a design principle that makes adapting cryptographic solutions or algorithms faster and more efficient in response to developments in cryptanalysis, emerging threats, technological advances, and/or vulnerabilities. The goal of crypto agility is to improve business continuity when existing cryptography is compromised.

The authors include subject matter experts from FS-ISAC, finance, academia, external authorities, and standards-setting bodies from around the globe. This paper defines crypto agility from a business perspective and offers technologists:

- architectural concepts
- a maturity model
- details on potential challenges
- a framework for implementing crypto agility
- insights on transition governance

The sector needs to start building those capabilities now. Though crypto agility speeds the transition process, institutions may not have time to swap algorithms when a threat arises.

Though written for the financial services sector, this first-of-its-kind effort to define crypto agility is crucial across industries. Please share with your networks and help the practice of cybersecurity embrace crypto agility.

Download your copy at https://www.fsisac.com/pqc-crypto-agility.

RESILIENCE

Cybersecurity Awareness Month Tip: Multi-Factor Authentication (MFA)

Summary

The use of MFA provides extra security for our online accounts and apps. This security could be a code sent via text or email or generated by an app, or biometrics like fingerprints and facial recognition. Using MFA confirms our identities when logging into our accounts.

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- Principles for Financial Institutions' Security and Resilience in Cloud Service Environments
- 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

- 3 September – 18 October | CAPS Exercise Banking
- 14 - 18 October | Cyber Range Exercise: Nebula Bank Offensive
- 16 October | A Strategic Approach to Resiliency
- 21 October CIAC Monthly Webinar
- 22 October | Member Success Session
- 27 - 30 October | Americas Fall Summit

View all Americas events

12120 Sunset Hills Rd, Reston
VA 20190