FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 28 October 2024 | Vol. 254

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
- Customer validation
- Employee impersonation
- New account fraud
- Online account
- Withdrawal and enrollment

Threats, Malware, Cyber Campaigns, and Adversaries

- Astaroth
- AsyncRAT
- Badger (aka BOLDBADGER) Malware
- ClickFix / ClearFake
- Credential Pharming
- Credential Validation
- Formbook
- Grandoreiro
- JsOutProx RAT
- Latrodectus
- LandUpdate808
- NetSupport RAT
- Payroll Diversion
- Salt Typhoon
- SocGholish
- StrelaStealer
- UnitedFullz Telegram Bot
- Ursa
- VenomRAT
- Xloader

System Vulnerabilities

Apache, Apple, Cisco, Debian, Dell, F5, Fortinet, Google, HP, Hitachi, IBM, Lenovo, Mozilla, Oracle, Palo Alto, Red Hat, ServiceNow, Siemens, Ubuntu, VMware, and Xerox.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: ***URGENT*** CLOSING, ADJST Aging Report, Adobe, AHC, Balanced aged report from A/R, BambooHR, DIRECT DEPOSIT UPDATE REQUEST, DocuSign, Fax Form, Gift Card, I need your help, “Important: Subscription Payment Failed Error payment #995635295 required,” Immediate Response Required, Invoice 3525, IRS, PAYMENT ASSISTANCE, QR Phishing, Payroll Diversion, Purchase Order, Spotify Subscription Payment Failed, SSA, Urgent attention is Required, Urgent response!!, and Wilson.

NEWS AND RISK INFORMATION

Black Basta ransomware poses as IT support on Microsoft Teams to breach networks. In a recent campaign observed by Rapid7 and ReliaQuest, Black Basta flooded employees' inboxes with emails and then contacted them through Microsoft Teams, posing as corporate help desks to assist with spam issues. (Bleeping Computer)

CISA: Microsoft SharePoint vulnerability is under active exploit. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added the Microsoft SharePoint Deserialization Vulnerability CVE-2024-38094 to its Known Exploited Vulnerabilities (KEV) catalog. (Dark Reading)

CVE-2024-9488 (CVSS 9.8): authentication bypass flaw in wpDiscuz plugin, over 80,000 sites at risk. A critical authentication bypass vulnerability has been discovered in wpDiscuz, a widely used WordPress plugin with over 80,000 active installations. This vulnerability tracked as CVE-2024-9488 and assigned a CVSSv3 score of 9.8, could allow unauthenticated attackers to hijack user accounts, including those with administrative privileges. (Security Online)

Delta Air Lines sues CrowdStrike over July system meltdown. Delta Air Lines accused Crowdstrike of "installing an exploit in Delta systems" – referring to the endpoint security vendor's July 19 update – in a lawsuit filed Friday. (Data Breach Today)

Embargo ransomware gang deploys customized defense evasion tools. The Embargo ransomware group uses custom Rust-based tools to bypass cybersecurity measures, as noted by ESET researchers. The toolkit includes MDeployer and MS4Killer, with MS4Killer uniquely compiled for each victim's system. (Infosecurity Magazine)

Evasive Panda using the new CloudScout toolset to steal data from Google Drive, Gmail, and Outlook. A toolset called CloudScout developed by the APT group Evasive Panda is targeting Taiwanese institutions to extract cloud-based data. The attacks, discovered by ESET, exploit session cookies stolen by MgBot plugins to access cloud services. [Read the *Top 10 Chinese Threat Actors* below.] (ESET Security)

Free decryptor released for Mallox ransomware. Avast released a free decryption tool to assist victims of the Mallox ransomware attacks. Mallox, also known as Fargo, TargetCompany, and Tohnichi, operates under a ransomware-as-a-service business model and targets Microsoft SQL servers. (gendigital)

New Qilin ransomware encryptor features stronger encryption and evasion techniques. Security researchers have discovered a new version of the Qilin ransomware, named Qilin.B. This new strain features stronger encryption using AES-256-CTR with AESNI capabilities, as well as retaining ChaCha20 for older systems. (Bleeping Computer)

Notorious hacker group TeamTNT launches new cloud attacks for crypto mining. The TeamTNT cryptojacking group is preparing for a new large-scale campaign targeting cloud-native environments to mine cryptocurrencies and rent out breached servers to third parties. (Aquasec)

Threat actor abuses Gophish to deliver new PowerRAT and DCRAT. The campaign involves modular infection chains requiring the victim's interaction, with the malware being delivered through Maldoc or HTML-based methods. The phishing emails use the Russian language, fake Yandex Disk links, and spoofed VK pages. (Cisco Talos)

THREATS OF THE WEEK

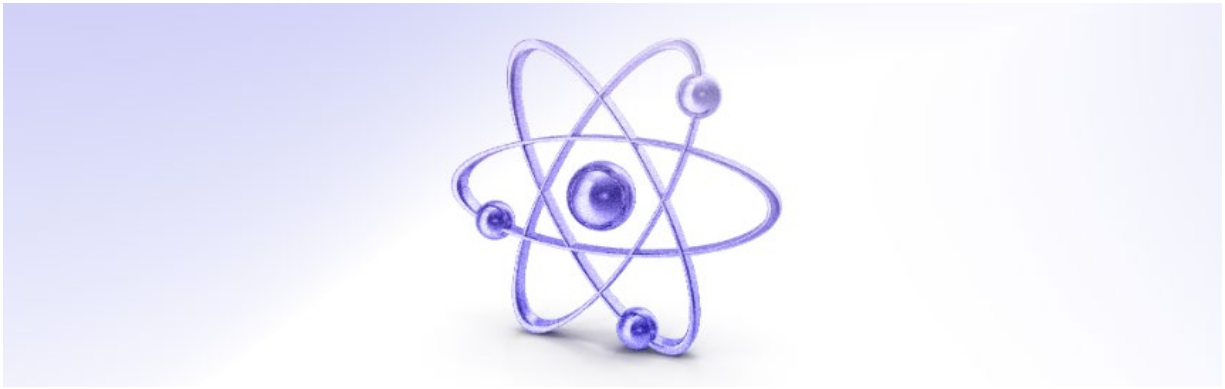
Reemerging malware highlights this week's risks

Bumblebee is Back … and It Stings!

Summary

Netskope reported that its Threat Lab team had found a new infection chain delivering Bumblebee malware. This is the first reported occurrence of a Bumblebee campaign since the May 2024 Operation Endgame took down Bumblebee and other malware dropper botnets.

The initial infection starts via a malspam email luring the victim to download a ZIP file and extract and execute the file inside it. Notably, the new Bumblebee infection chain executes the final Bumblebee payload in memory, avoiding the need to write the DLL on disk, as previous campaigns have.



THREAT INTELLIGENCE UPDATE

Top 10 Chinese Threat Actors

Insight into the Chinese government military: threats, techniques, and mitigation

Summary

The following excerpts from this report come from Lloyds Banking Group plc.

The People's Liberation Army (PLA) Military wing of the Chinese Communist Party operates a dedicated cyber warfare branch against foreign adversaries. The Ministry of State Security (MSS) is the core intelligence service of the Chinese government, focusing on foreign espionage operations and political security. This organization operates with most Chinese state-backed threat actors.

The rise of China has reshaped the global geopolitical landscape and seeks to challenge the US as the world's eminent superpower. China is seeking regional dominance in Asia, securing its territorial integrity, and growing its economic influence.

China/UK relations are at a low ebb, mired in disputes over human rights, democracy, territorial sovereignty, trade, and China's increasingly close ties to Russia. In March 2024, then Prime Minister Rishi Sunak described China as 'the greatest threat to the UK's economic security.'

Cyber is a key weapon in China's strategic arsenal, with a sophisticated capability and proven intent to conduct industrial-scale espionage campaigns to further its strategic aims. China poses the greatest cyber espionage threat to financial services firms' IP and data, and that of suppliers and clients. Financial institutions being part of critical national infrastructure (CNI) and holding vast amounts of data of strategic value, are highly likely an attractive cyber espionage target for the Chinese state.

Top 10 Threat Actors

Considering the elevated Chinese cyber threat to the financial sector, suppliers, and clients, Lloyds Banking Group plc identifies 10 specific Chinese threat actors pose the highest threat. These threat actors are listed in descending order from greatest threat to least**,** reflecting their capabilities and projected intention to attack the financial sector in the foreseeable future.

Ministry of State Security (MSS). Est. 1941	**People's Liberation Army (PLA). Est. 1927**
1. Wicked Panda 2. Judgement Panda 3. Circuit Panda 4. Aquatic Panda 5. Stone Panda 6. Keyhole Panda	Vixen Panda Vanguard Panda **Unknown** Emissary Panda Mustang Panda

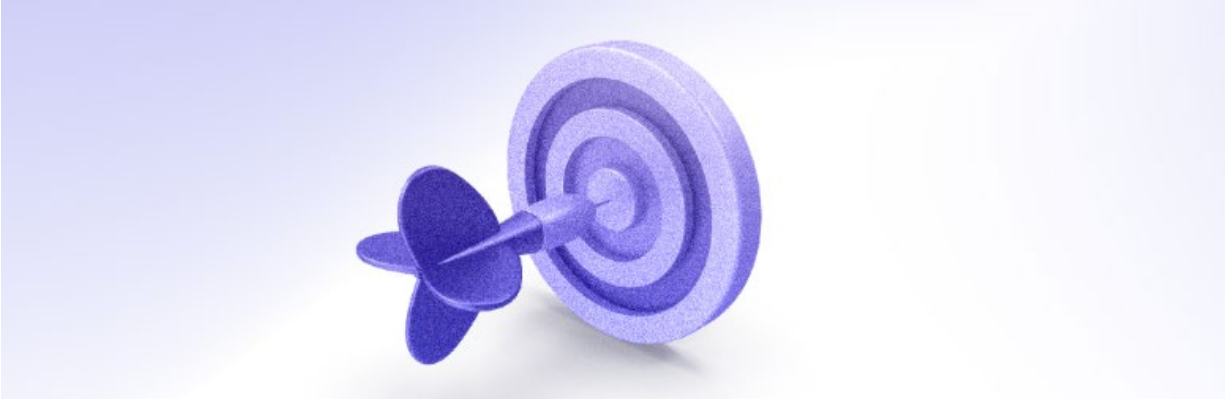
Techniques and Mitigation

The techniques below are the most commonly used across all 10 threat actors and the most referenced mitigations as per the MITRE ATT&CK framework.

Techniques	**Mitigations**
T1574.002 – Hijack Execution Flow: DLL Side-Loading T1071.001 – Application Layer Protocol: Web Protocols T1560.001 – Archive Collected Data: Archive via Utility T1562.001 – Impair Defenses: Disable or Modify Tools T1564.003 – Hide Artifacts: Hidden Window T1005 – Data from Local System T1190 – Exploit Public-Facing Application T1055 – Process Injection T1140 – Deobfuscate/Decode Files or Information T1102 - Web Service	• Privileged Account Management • Network Intrusion Prevention • Execution Prevention • Behavior Prevention on Endpoint • Audit • User Account Management • Update Software • Network Segmentation • Application Developer Guidance • User Training

Related Content

A full breakdown of each Panda is available for members in Share. Here



JUST FOR COMMUNITY INSTITUTIONS

Gaining the Upper Hand on Ransomware

Size, complexity, and risk appetite are just words to ransomware threat actors. Here's how to gain an upper hand against ransomware threat actors.

Summary

Akira, Beast, Black Basta, Embargo, Fog, Golang, LockBit, macOS NotLockBit, Qilin, Play, and RansomHub – are new ransomware applications in circulation. Size, complexity, and risk appetite are just words to threat actors who do not care what size your institution is, who your customers are, or the damage they cause – you are just a payday. How can a smaller institution gain an upper hand against ransomware threat actors?

Ransomware is one of the few threats that can disable a financial services institution and is a serious threat to national infrastructure. Increasingly innovative, aggressive, and frequent, ransomware attacks can disrupt customer services, halt business operations, and damage the institution's standing with customers and regulators.

Our two-part series on ransomware will discuss solutions, look at building a crisis management team, and share food for thought about whether an institution should pay a ransom.

Let's Talk Solutions

Below are solutions you should be using or implementing. Remember, ransomware attacks will not stop until they no longer offer value to the threat actors.

Use non-erasable and non-modifiable backup systems to duplicate data and system configurations:

- Regularly back up critical data and system configurations to isolated environments. If segmentation is in place and backups are preserved, the impact of an attack may be manageable.
- Test backups at least annually in real-world technical exercises to ensure backups can be restored quickly and completely during an attack. Cloud computing makes testing and restoration easier, but some firms may only be able to test restoration of certain critical functions. A robust restoration plan, likely on a separate new infrastructure, will take a great deal of effort, especially in large firms.

Regularly update and patch software:

- Updates and patches reduce initial infection potential from technical and social engineering attacks.
- Where the risk is acceptable, automate patch management to ensure consistent application of updates across all systems, reducing human error and delays.
- If patching is delayed, develop standard processes to implement mitigation strategies like virtual patching utilizing a web application firewall (WAF).

Use a zero-trust and least-privilege policy with multi-factor authentication, and require strong passwords for every employee, device, and account:

- Implement a zero-trust approach where all users and devices, inside or outside the network, are authenticated, authorized, and continuously validated before gaining access to applications and data.
- Leverage resources like NIST 800-207 Zero Trust Architecture to develop your strategy.

Train employees in their role in cybersecurity:

- Conduct regular training sessions to educate employees on the latest cybersecurity threats, including phishing, social engineering, and the dangers of clicking on unknown links or downloading unverified attachments. People who understand the potential impact of clicking on external links or reusing passwords will generally take more care about their activities.

Develop an incident response plan specific to ransomware attacks:

- Detail the steps to be taken immediately upon detection, including isolation, communication, and recovery procedures.
- Conduct regular tabletop exercises and full-scale drills to ensure that all team members are familiar with the response plan and can act quickly and effectively under pressure. Exercises allow you to review and update plans to adapt to evolving threats and changes in your organization.

Implement EDR, DLP, and firewall solutions.

- Implement Endpoint Detection and Response (EDR) solutions. EDR solutions monitor endpoints (computers, servers, mobile devices) for suspicious activity, and respond to threats in real-time to disrupt ransomware before it can spread.

Implement Data Loss Prevention (DLP) solutions.

- DLP solutions monitor and control the movement of sensitive data, helping to prevent exfiltration attempts by cybercriminals.
- Use firewalls, configured closed by default, with active blocking. When deploying firewalls, look at internal segmentation as well. One example is agent-based micro-segmentation augmentation of traditional firewalls, which minimizes the potential impact of encryption malware.
- Another key control for exfiltration monitoring is a SWG/DNS firewall that can detect data being stolen and prevent users from going to malicious websites.

Tune in next week as we discuss developing and implementing a crisis management plan.

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- 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

- 18 November | November CIAC Webinar
- 4 December | Americas Member Success Session
- 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