FS-ISAC

Community Institution & Associations Risk Summary Report

Week of 6 May | 2024 Edition | Vol. 230

Follow Us

TLP GREEN

Americas Cyber Threat Level: Elevated

DHS Terrorism Threat Level: Elevated

In This Issue

Threats of the Week

News and Risk Information

Summary

Below are some top news and risks the Financial Services Information Sharing Analysis Center (FS-ISAC) has observed this week for community institutions (CIs).

Cyber Threat Level: Elevated. The Americas Threat Intelligence Committee (TIC) voted to raise the AMER Cyber Threat Level to Elevated. The TIC assesses that ongoing Scattered Spider activity targeting the Financial Services Sector, including FS-ISAC members, demonstrates an increased cyber threat from a credible, sophisticated actor or group. Implementation of additional cybersecurity measures may be warranted. FS-ISAC members are encouraged to review previously published Scattered Spider mitigation guidance and the April Scattered Spider Activity Cluster Alert and implement recommendations as appropriate. (FS-ISAC)

SEC sparks CISO role re-evaluation. Cybersecurity expert Joseph Steinberg breaks down the latest cybersecurity disclosure rules from the Securities and Exchange Commission and demonstrates how legal action against chief information security officers and other leaders forces a reevaluation of roles. "Essentially, the onus has shifted as to who is responsible," Steinberg says, adding, "Instead of viewing cyber incidents as something that happened to a company ... the new rules basically say that if an incident occurs, the company's management and board are responsible to ensure that they adequately explain to the world what happened." (Newsweek)

Attackers steal API keys, and OAuth tokens, in Dropbox Sign breach. In a filing with the Securities and Exchange Commission, Dropbox said for subsets of users, a threat actor accessed phone numbers, hashed passwords, and certain authentication information, such as API keys, OAuth tokens, and multi-factor authentication. Security pros saw this as a major blow to Dropbox and e-signatures in general because over the three decades since the rise of the web in the 1990s people were starting to get used to doing business with e-signatures. (SC Media)

Critical GitLab account takeover flaw added to CISA's KEV Catalog. The Cybersecurity & Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) Catalog added a critical GitLab vulnerability that could enable account takeover. The vulnerability tracked as CVE-2023-7028, enables an attacker to craft a specially formatted HTTP request that causes a password reset email to be sent to an unverified attacker-controlled email address, a GitLab spokesperson previously told SC Media. The flaw has a critical CVSS score of 10, as assessed by GitLab, and a high score of 7.5, as assessed by NIST. (SC Magazine)

Helping small businesses reduce their risk. According to a recent report by Ping Identity, only 45% of organizations use multi-factor authentication (MFA) to protect themselves against fraud. The report, based on responses from 700 IT decision-makers across the US, UK, France, Germany, Australia, and Singapore, reveals a pressing need for organizations to enhance their identity protection strategies, with 97% having challenges with identity verification and 48% lacking confidence they have the technology in place to defend against AI-related attacks. (Digital Transactions)

Novel TunnelVision attack impacts virtually all VPN apps through DHCP server manipulation. The TunnelVision attack is a newly discovered method that can compromise the security of most Virtual Private Network (VPN) applications by diverting traffic away from the encrypted tunnel, exposing it to potential interception. The researchers note this hasn't been seen in the wild. (ARS Technica)

This Week's Top Risks

Security is Everyone's Responsibility

Threats, Malware, Cybercampaigns, and Adversaries

- Agent Tesla
- Astaroth
- Balada
- Business email compromise and impersonation use of texts; credential pharming, harvesting, and validation scams.
- DarkGate
- DBatLoader RAT
- Eugenloader
- Formbook
- GuLoader
- JsOutProx RAT
- Latrodectus
- Lokibot
- NetSupport
- PHORPIEX
- SocGholish
- SolarMarker (aka Jupyter)
- Xworm
- Zloader
- ZPHP

Hardware and System Vulnerabilities (multiple)

- Adobe, Android, Apple, Avaya, Debian, Dell, F5, GNU, Google, IBM, Intel, Juniper, Lenovo, Microsoft, Mozilla, Oracle, Red Hat, Samsung, and Ubuntu.

Themed Phishing Campaigns

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

Subject Keywords: 2023 Tax Returns, Follow-Up!!!, (7) Incoming Failed Messages, Payment Receipts, purchase order, Remittance Notification, Request for Tender Quotation!, SC-246214, Shared a Folder, Someone has made an offer for your item, United Rentals Inc: Invoice, and Your Document.

Threats of the Week

STORM-0539 and Damselfly highlight this week's risks

Beware "The Storm"

Summary

As of January 2024, the FBI noted a cybercriminal group labeled STORM-0539, also known as Atlas Lion, targeting national retail corporations; specifically the gift card departments within their corporate offices. STORM-0539 used smishing campaigns to target employees and gain unauthorized access to employee accounts and corporate systems. Once they gained access, STORM-0539 actors used phishing campaigns to target other employees to elevate network access and target the gift card department to create fraudulent gift cards. Some of the techniques, tactics, and procedures (TTPs) observed by STORM-0539 actors included:

- They target employees' personal and work mobile phones in retail departments with smishing campaigns.
- They use a sophisticated phishing kit that can bypass multi-factor authentication.
- Once an employee's account is compromised, they perform surveillance on the business network to identify the gift card business process and then pivot to employee accounts covering that specific portfolio.
- Once in the network, they attempt to access secure shell (SSH) passwords and keys in addition to targeting credentials of employees in the gift card department.
- After successfully gaining access to the corporate gift card department, they create fraudulent gift cards using compromised employee accounts.
    - In one instance, a corporation detected STORM-0539's fraudulent gift card activity in their system and instituted changes to prevent the creation of fraudulent gift cards. STORM-0539 actors continued their smishing attacks and regained access to corporate systems. Then, the actors pivoted tactics to locating unredeemed gift cards and changed the associated email addresses to ones controlled by STORM-0539 actors to redeem the gift cards.
- They exfiltrate employee data including names, usernames, and phone numbers, which could be exploited by the actors for additional attacks or sold for financial gain.

Remediation

- Provide education and training for employees on how smishing/phishing scams work, how to identify them, and how to report them. Ensure there is a mechanism and process for employees to report smishing/phishing attacks.
- Provide education to employees regarding being cautious about sharing sensitive information, including login credentials, when communicating via phone or web-based programs and not clicking on suspicious links. Requests for sensitive information should be verified through alternative approved methods. Urgent requests via SMS should be treated with caution.
- Require multi-factor authentication on as many accounts and login credentials as possible. When practical, use phishing-resistant authentication options.
- Employ anti-virus and anti-malware solutions and make sure they are updated regularly.
- Consider using network and end-point SMS filtering and anti-phishing tools.
- Enforce a strong password policy, such as requiring strong and unique passwords for all password-protected accounts, employing lock-out rules for failed login attempts, restricting the reuse of passwords, and requiring the secure storage of passwords.
- Implement security monitoring tools that log network traffic to establish baseline activity, and that enable detecting and addressing abnormal network activity, including lateral movement on a network.
- Enforce the principle of least privilege throughout the organization's network. Account privileges should be clearly defined and regularly reviewed and adjusted as necessary.
- Maintain and enforce a Bring Your Own Device policy (BYOD). Provide education and training to employees on the BYOD policy.
- Phishing Guidance: Stopping the Attack Cycle at Phase One: CISA Phishing Guidance

Damselfly Buzzes Around a Network Near You

Summary

The Damselfly Advanced Persistent Threat (APT) group, also known as APT42, has been actively utilizing custom backdoor variants, NiceCurl and TameCat, to infiltrate Windows machines. These backdoors are primarily delivered through spear-phishing campaigns, marking a significant escalation in the capabilities and focus of this Iranian state-sponsored hacking group. The NiceCurl and TameCat backdoors represent a sophisticated toolkit in Damselfly's arsenal, enabling threat actors to gain initial access to targeted environments discreetly. According to Broadcom report, the group's activities have been primarily directed at energy companies and other critical infrastructure sectors across the US, Europe, and the Middle East. Using custom backdoors like NiceCurl and TameCat, coupled with spear-phishing campaigns, enables these actors to maintain persistence in their targeting networks, and to carry out their missions with a high degree of secrecy and efficiency.

Risk

NiceCurl, a VBScript-based malware, is designed to download and execute additional malicious modules, enhancing the attackers' control over compromised systems.

Cont'd.

Remediation

In addition to using a robust anti-virus solution, institutions should employ an audit security solution and network monitoring tools, secure endpoints, monitor the network, update and patch networks daily, and migrate to a zero-trust environment that MFA protects. Finally, ensure each device is protected by a host firewall.

It's Time to Talk About Ransomware - Again

Profits may be down, but ransomware attacks are up

What We Know

- "Roughly one-third of all breaches involved Ransomware or some other Extortion technique. Pure Extortion attacks have risen over the past year and are now a component of 9% of all breaches. The shift of traditional ransomware actors toward these newer techniques resulted in a bit of a decline in Ransomware to 23%. However, when combined, given that they share threat actors, they represent a strong growth of 32% of breaches. Ransomware was a top threat across 92% of industries." – *Verizon 2024 DBIR Report*
- "In 2023, ransomware payments reached a record high of $1.1 billion, which is almost double the $567 million paid in 2022. The average ransomware attack cost $5.13 million in 2023, which includes detection, escalation, notification, post-breach response, and lost business. This is a 13% increase from 2022." – *Fisher Phillips*
- "In 2023, organizations worldwide detected 317.59 million ransomware attempts, which is an 84% increase from 2022." – *Verizon 2024 DBIR Report*

Summary

Depending on the vendor report you read, the number of companies polled, and the response ratio, ransomware is still a problem. The cybercriminals behind the United Healthcare attack were a Russia-based ransomware gang known as ALPHV or BlackCat. UnitedHealth Group paid a $22 million ransom and an additional $3.3 billion to providers affected by the cyberattack on its subsidiary Change Healthcare.

At A Glance

Table 1 reveals an excerpt of the number of security incidents and breaches by victim industry and organization size in Verizon's report.

	INCIDENTS				BREACHES			
Industry	Totals	Small (1–1,000)	Large (1,000+)	Unknown	Total	Small (1–1,000)	Large (1,000+)	Unknown
Finance (52)	3,348	75	122	3,151	1,115	54	87	974
Healthcare (62)	1,378	54	21	1,303	1,220	41	18	1,161

Table 1. Number of security incidents and breaches by victim industry and organization size

What It Means

A data breach easily results in identity theft once personally identifiable information is exposed to unauthorized individuals. Organized groups can post/sell the data on dark websites resulting in lingering problems for consumers and damage to their perception of your institution to the point that some will seek alternative banking services. That can impact your bottom line and shareholder value.

Additional Consequences

- Financial losses
- Reputational damage
- Loss of customers
- Higher loan spreads
- Increased collateral requirements
- More demanding loan terms

Trust But Verify

Preparedness includes what you can't anticipate. Financial institutions must have and maintain business resiliency and disaster recovery plans, but do those plans consider the impact on customer perception when customers can't access their money? Is your institution ready for your worst cyber incident?

FS-ISAC and Sheltered Harbor invite C-Suite executives to a special virtual roundtable discussion about how you can survive a severe cyber outage. Pre-register today to reserve your seat!

- When: 15 May 2024
- Time: 3:00 PM ET, 12:30 PM PT
- Registration link: https://fsisac.zoom.us/webinar/register/WN_Jr31lwelSOacrHMzR2m9Fw