FS-ISAC

Community Institution & Associations Risk Summary Report

Week of 10 June | 2024 Edition | Vol. 235

Follow Us

TLP GREEN | Americas Cyber Threat Level: Guarded | 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).

June Community Institution and Associations Council [CIAC] meeting. The next FS-ISAC CIAC meeting will occur on 24 June 2024 at 3:30 PM ET. Register to attend today using the link in your Outlook invitation. (FS-ISAC CIAC)

FBI recovered 7,000 LockBit keys. At a conference on 5 June, FBI Cyber Division Assistant Director Bryan Vorndran announced the Bureau obtained over 7,000 decryption keys for LockBit ransomware throughout their investigation and takedown efforts. In addition to the FBI reaching out to identified victims in the batch of 7,000, Mr. Vorndran urged LockBit victims to visit the Internet Crime Complaint Center (IC3) to file a complaint, reclaim their data, and get back online. In February 2024, FBI and law enforcement partners took down the LockBit infrastructure and released 2,500 decryption keys in an operation dubbed "Operation Cronos." (FS-ISAC GIO)

Federal agencies reported over 32K cyber incidents in 2023. The Office of Management and Budget's Federal Information Security Modernization Act report to Congress said more than 32,000 cybersecurity incidents were reported by federal agencies, nearly a 10% increase over a year earlier. Violations of acceptable use policy and email phishing were the biggest attack vectors. (Federal News Network)

As the bad guys get smarter, all data breaches are major. There are no insignificant data breaches anymore, because criminals "who have demonstrated their ability to steal data from some of the largest corporate networks in the world may very well possess the ingenuity to exploit even a minimal information set," argues Dirk Schrader of IT security provider Netwrix. In this commentary, Schrader cites a recent breach at Dell, which called the individuals' information swiped "not a significant risk." (Tech Radar)

Malicious AutoIt script delivers Vidar stealer via drive-by downloads. The attack utilized Java dependencies and a malicious AutoIt script to disable Windows Defender and decrypt the Vidar payload. The user was lured to a website claiming to offer a Windows activator but was in fact hosting the malware. (eSentire)

New Agent Tesla campaign targeting Spanish-speaking people. This campaign leverages multiple techniques to deliver the Agent Tesla core module, such as using known MS Office vulnerabilities, JavaScript code, PowerShell code, fileless modules, and more, to protect itself from being analyzed by researchers. (Fortinet)

Ransomware insurance: A viable option? Seventy-three percent of respondents to Veeam's ransomware trends survey reported their cyber-insurance premiums increased at the time of their last renewal, 44% had their deductible increased, and 14% had coverage benefits reduced. Of organizations whose data was ransomed in 2023, 86% could have used insurance to cover the cost; however, only 65% chose to do so. Twenty-one percent decided not to use their insurance, paying the ransom without making a claim. One in three organizations could not recover their data after paying the ransom. (Veeam)

Researchers urge immediate action on new EmailGPT vulnerability exposing users to data breach. By coercing the AI service, attackers can force the leakage of standard system prompts or execute unauthorized prompts, paving the way for various forms of exploitation. The implications of this EmailGPT vulnerability are profound. (Cyber Express)

TellYouThePass ransomware exploits recent PHP RCE flaw to breach servers. The TellYouThePass ransomware gang has been exploiting a recently patched vulnerability (CVE-2024-4577) in PHP to deliver web shells and execute ransomware on targeted systems. (Bleeping Computer)

This Week's Top Risks

Security is Everyone's Responsibility

Threats, Malware, Cybercampaigns, and Adversaries

- Agent Tesla
- ASYNCRAT/AZORULT
- Balada
- Business email compromise and impersonation use of texts; credential pharming, harvesting, and validation scams.
- CLEANBOOST aka CleanUp aka Broomstick)
- Clop
- JanelaRAT
- Koi Loader/Stealer
- Lokibot
- Mispadu
- Ousaban
- Oyster
- PHORPIEX
- QUICKBIND (aka WarmCookie aka Badspace
- Remcos
- SectopRAT
- SocGholish
- SolarMarker (aka Jupyter)
- XLoader
- ZPHP

Hardware and System Vulnerabilities (multiple)

- Adobe, Apple, Cisco, Debian, Dell, F5, Fortinet, Google, IBM, LenelS2, Lenovo, Magento, Microsoft, Mozilla, NVIDIA, Oracle, PHP, Red Hat, Samsung, SAP, Serv-U, Solar Winds, Tenable, Trend Micro, Ubuntu, and VMware.

Themed Phishing Campaigns

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

Subject Keywords: A debit card transaction, ACTION ITEM, Action Item: Verify And Follow Up, DocuSign, OVERDUE REMINDER!!, Quotation, Review Check run/Pay app, Staff Performance Report, Teams, Time Sheet, We've detected some suspcious debit card activity.

Threats of the Week

Snowflake, Ink Trails, and VPN attacks highlight this week's risks

Update: Snowflake Security Incident

Overview

According to a security vendor blog post that has since been taken down, the threat actor ShinyHunters claimed they obtained data from many companies after gaining access to the systems of cloud services provider, Snowflake. Snowflake confirmed it is observing and investigating an increase in malicious activity targeting its customers' accounts. However, Snowflake denied that the data breaches originated from its products.

According to Snowflake, this activity stems from identity-based attacks on individuals at victim organizations (e.g., information-stealing malware that steals credentials for accounts without multi-factor authentication) rather than malicious activity targeting Snowflake itself. Snowflake published guidance for investigating and preventing malicious activity. Snowflake released a joint advisory with CrowdStrike and Mandiant, confirming attackers used stolen credentials to target customers who had not enabled multi-factor authentication.

Snowflake added that while one employee's demo account was compromised using stolen credentials, this account did not provide threat actors access to sensitive data, production environments, or corporate systems. Ticketmaster, one of the companies that was breached, confirmed the breach originated from a 20 May compromise of its Snowflake account. An FS-ISAC member shared Snowflake URLs from Infostealer logs that are likely related to ongoing activity. FS-ISAC assesses the data provided can be helpful for the company's threat-hunting teams. FS-ISAC created a channel in CONNECT dedicated to this activity.

On 10 June, Mandiant attributed the attacks to UNC5537 who targeted hundreds of organizations worldwide and frequently extorted victims for financial gain. The investigation showed that approximately 165 clients potentially had their data stolen.

Ink Trails by LilacSquid: PurpleInk, InkBox, and InkLoader

Summary

Cyware Labs reported on a new data theft threat campaign revealed by Cisco Talos. Active since 2021, this new campaign is attributed to an advanced persistent threat (APT) actor named LilacSquid.

Cyware Labs reports that LilacSquid targets a diverse range of victims, including IT organizations developing software for research and industrial sectors in the US, energy sector organizations in Europe, and the pharmaceutical sector in Asia, indicating the threat actor's industry-agnostic approach to data theft. This campaign employs MeshAgent, an open-source remote management tool, and a customized version of QuasarRAT, dubbed PurpleInk, as primary implants after compromising vulnerable application servers exposed to the internet.

The data theft campaign exploits vulnerabilities in public-facing application servers and compromised RDP credentials to deploy various open-source tools, such as MeshAgent and SSF. Apart from PurpleInk, the threat actor uses two malware loaders named InkBox and InkLoader. Notably, multiple TTPs in this campaign overlap with North Korean APT groups, such as Andariel and its parent group, Lazarus.

The campaign aims to establish long-term access to compromised organizations, enabling LilacSquid to siphon data to attacker-controlled servers. Successful exploitation of the vulnerable application results in the deployment of a script that sets up working directories for the malware and then downloads and executes MeshAgent from a remote server. On execution, MeshAgent connects to its C2, conducts preliminary reconnaissance, and begins downloading and activating other implants on the system, such as SSF and PurpleInk.

Talos observed LilacSquid deploying InkLoader with PurpleInk only when it could successfully create and maintain remote sessions via RDP by exploiting stolen credentials for the target host. A successful RDP login leads to the download of InkLoader and PurpleInk, copying these artifacts into desired directories on disk, and subsequently registering InkLoader as a service that starts to deploy InkLoader and, in turn, PurpleInk.

Remediation

The LilacSquid campaign highlights the persistent and evolving nature of APT actors. As LilacSquid continues to evolve its arsenal and refine its operations, organizations must remain vigilant and implement regular vulnerability assessments, access control mechanisms, and comprehensive incident response plans. Collaboration and information sharing among the cybersecurity community are vital in combating the persistent threats posed by such groups and protecting against data theft and potential supply chain compromises.

Check Point VPN Attacks

Overview

The number of attacks exploiting Check Point VPN vulnerability CVE-2024-24919 increased significantly over the past week. Check Point released a "hotfix" for the bug on 28 May, and noted in an update this week that exploitation attempts began on 7 April. The vulnerability allows threat actors to access sensitive information on Check Point's Security Gateway. In certain scenarios, threat actors could move laterally and increase network privileges. Thousands of devices remain unpatched. Historically, US officials have warned that vulnerabilities in VPNs and similar technologies present a high risk to organizations because threat actors target flaws in these technologies.

Artificial Intelligence and Financial Stability Conference

Summary

On 6-7 June 2024, the Financial Stability Oversight Council (FSOC) in partnership with the Brookings Institution, hosted a two-day conference on Artificial Intelligence (AI) and Financial Stability. Innovations in AI can offer many benefits, such as reducing costs and improving efficiencies, but they can also introduce or exacerbate risks to the financial system. This conference was an opportunity for the public and private sectors to convene to discuss potential systemic risks posed by AI in financial services, to explore the balance between encouraging innovation and mitigating risks, and to share insights on effective oversight of AI-related risks to financial stability.

Webcasts

To view each day's webcast, visit the below links:

- 6 June, https://usdotyorktel.rev.vbrick.com/#/videos/bd9da801-056d-41e8-a90f-07daaa53b3dd
- 7 June, https://www.youtube.com/live/F3MndJf9a70

Six Steps to Effective Learning

Are you seeing the type of results you expect to see?

Summary

Aristotle said, "For the things we have to learn before we can do them, we learn by doing them."

Financial institutions are required to provide security awareness training – yet the continuing concern is whether the training has the desired effect on its audience.

Hornetsecurity conducted a survey of industry professionals worldwide and revealed that 8% of organizations offer adaptive training that evolves based on the results of regular security tests. The survey also shows that:

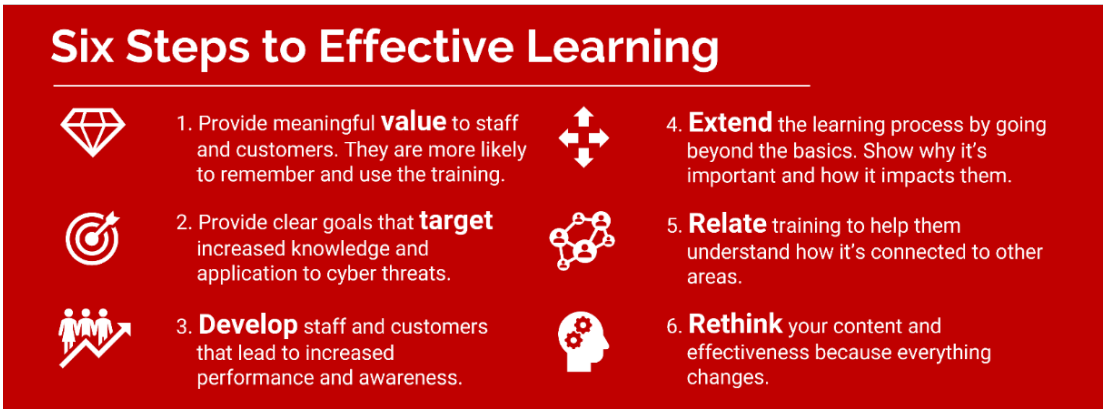
- Thirty-one percent of respondents reported that their training was unengaging or only slightly engaging.
- Seventy-nine percent of organizations believe their IT security awareness training to be at least moderately effective.
- Thirty-nine percent reported that the training does not adequately cover recent or AI-powered cyber threats.
- Twenty-three percent suffered a cyber incident in the last year. Notably, 94% of these organizations strengthened their security by implementing additional controls post-incident.
- Fifty-two percent of respondents noted that end-users often ignore or delete identified email threats without reporting them, and 38% forget the training content, showing the need for ongoing and engaging training enhancements.
- Twenty-three percent suffered a cyber incident in the last year. Notably, 94% of these organizations strengthened their security by implementing additional controls post-incident.

Clearly, training could be more effective than it is. When creating and implementing a solid training program, think in terms of the following six steps that will help your employees and customers leave the exercise with the knowledge and wisdom they need to apply what they have learned.

Six Steps to Effective Learning

If you are not seeing the type of results you expect to see it's never too late to begin experimenting with new methods to reach and influence staff and customers.

Remember, hitting the sweet spot of reaching your audience and having them remember and implement what they've learned dramatically increases the effectiveness of your security program.



The report concludes by saying that 79% of organizations attribute the prevention of cybersecurity incidents directly to their IT security training programs, while 92% acknowledge that the training has enabled end-users to spot security threats across various media, not just email.