Community Institution & Associations Risk Summary Report

Week of 10 April | 2023 Edition | Vol. 172

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

CISA releases update to Zero-Trust maturity model. The Cybersecurity and Infrastructure Security Agency (CISA) released Zero Trust Maturity Model (ZTMM) version 2, which provides a roadmap for agencies to reference as they transition towards a zero trust architecture. While the Zero Trust Maturity Model is specifically intended for federal agencies, all organizations should review this guidance and take steps to advance their progress toward a zero-trust model. (CISA)

Privacy advocates voice concerns about new chatbots. Some companies are setting restrictions for employee use of large language models due to privacy and regulatory compliance concerns. Mark McCreary, the co-chair of Fox Rothschild's privacy and data security practice unit, says it's unclear what happens to data user's input into artificial intelligence tools, and Steve Mills, chief AI ethics officer at Boston Consulting Group, says even asking LLM chatbots to summarize meeting notes raises the risk that confidential business information will be inadvertently disclosed. (CNN)

Samsung employees unwittingly leaked the company's secret data by using ChatGPT. Samsung Electronics is warning its employees of the potential risks associated with the use of ChatGPT, explaining that there is no way to prevent the leak of the data provided to OpenAI's chatbot service. (Security Affairs)

What CISOs are looking out for in 2023. Chief information security officers are seeing greater investment in cybersecurity as well as an increase in threats and regulations. Among the challenges CISOs face this year are building cultures of security in organizations, using automation to boost efficiency, limiting the attack surface amid remote working and various networks, and watching out for threats from within organizations. (Infosecurity)

Apple Releases Security Updates for Multiple Products. Apple has released security updates to address vulnerabilities in multiple products. An attacker could exploit some of these vulnerabilities to take control of an affected device. (CISA)

Hackers switch gears in QuickBooks, PayPal email attacks. Hackers are using legitimate free QuickBooks and PayPal accounts to defraud companies in what researchers are calling a new approach after the recent crackdown on business email compromise attacks. Employees will need to take a new line to spot these rogue accounts by slowing down, increasing invoice scrutiny, and using data loss prevention software, researchers say. (SC Media)

Iranian hackers caught carrying out destructive attacks under ransomware guise. The Iranian nation-state group known as MuddyWater has been observed carrying out destructive attacks on hybrid environments under the guise of a ransomware operation. According to new findings from the Microsoft Threat Intelligence team, the threat actor targeted both on-premises and cloud infrastructures in partnership with another emerging activity cluster dubbed DEV-1084. (Hacker News)

This Week's Top Risks

Security is Everyone's Responsibility

Threats, Malware, Cybercampaigns, and Adversaries

- AdsVNC Malware
- Agent Tesla
- AZORULT
- Business email compromise and impersonation use of texts; credential pharming, harvesting, and validation scams
- CryptoClippy ransomware
- Emotet/Trickbot/Ursnif
- Formbook/DBatLoader
- FusionCore
- Havoc Demon
- IceID
- JsOutProx RAT
- Lokibot
- NanoCore
- NetSupport
- Qbot/QakBot
- Silence.Downloader
- SocGholish
- TrueBot
- Wandering Spider

Hardware & System Vulnerabilities (multiple)

- Adobe, Amazon, Apple, Arista, Aruba, Cisco, Cygwin, Debian, Dell, DocuSign F5, Fortinet, FortiOS, Google, IBM, Juniper, Junos, Lenovo, McAfee, Microsoft, Mozilla, Oracle, Red Hat, SAP, SUSE, and Ubuntu.

Themed Phishing Campaigns

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

Subject Keywords: Adjustment Needed, Application, Benefit, Better Business Bureau, Buyer Signed, Central Nassau, Counseling Service, DAIQ Architects, Employee, FedEx, HR, Incoming Payment, Intralinks, Invoice, LB006284792, Legal Review, Locust Hill, Netflix, NEW P04564, O365, Purchase Order, QuickBooks, Right of Use, SBA, Shipping Documents, signed charter agreement, SKM, and Workplace Benefit.

Threats of the Week

System vulnerabilities and targeted online storage, highlight this week's risks

Zimbra Flaw Added to CISA's KEV List

Summary

CISA added a cross-site scripting flaw in the Zimbra Collaboration Suite (ZCS) (CVE-2022-27926) to their Known Exploited Vulnerabilities list. It has been exploited by a pro-Kremlin hacking group called Winter Vivern (TA473) since February 2023 in attacks against several NATO-aligned governments, diplomats, and military webmail portals. The attacks are likely an attempt to conduct politically motivated espionage operations. Although this activity has not yet targeted the financial sector, the use of ZCS in many small to mid-tier organizations widens the potential attack surface.

Online Storage Solutions Being Targeted

Summary

Two internet-facing backup solutions have recently been targets of compromise. Mandiant reports the exploitation of three high-severity flaws in the Veritas Backup Exec software via a publicly available Metasploit module since 22 October 2022. After the compromise, the threat actor performed reconnaissance and then downloaded the ALPHV ransomware payload.

This includes three high-severity flaws in the Veritas Backup Exec Agent software (CVE-2021-27876, CVE-2021-27877, and CVE-2021-27878) that could lead to the execution of privileged commands on the underlying system. The flaws were fixed in a patch released by Veritas in March 2021.

- CVE-2021-27876 (CVSS score: 8.1) - Veritas Backup Exec Agent File Access Vulnerability
- CVE-2021-27877 (CVSS score: 8.2) - Veritas Backup Exec Agent Improper Authentication Vulnerability
- CVE-2021-27878 (CVSS score: 8.8) - Veritas Backup Exec Agent Command Execution Vulnerability

Western Digital

Western Digital also announced that its network was recently breached and certain data was harvested from multiple systems. Five days into a massive outage impacting its cloud services, Western Digital finally provided customers with a workaround to access their files. Since 2 April, the outage has prevented users from accessing files stored on their WD NAS devices, as it required access to the company's cloud services.

The complete list of services that were down throughout this week includes My Cloud, My Cloud Home, My Cloud Home Duo, My Cloud OS 5, SanDisk ibi, and SanDisk Ixpand Wireless Charger, together with linked mobile, desktop, and web apps.

A Bleeping Computer article wrote, "While customers expressed concerns that Western Digital's servers were hacked to push out remote factory reset commands to all affected devices, the company denied the rumors and said that its network had not been breached."

A knowledge base article provides detailed information on how to toggle on Local Access. Local access is already enabled for My Cloud OS5 (My Cloud PR series and EX series) products. As a precaution, the My Cloud service is offline while they investigate, impacting access to user data.

The Rise and Fall of Illicit Marketplaces

The fall of the Genesis Market, but does this mean the downfall of illicit marketplaces?

Summary

Last week saw the fall of one online black market, Genesis Market, and at the same time, security researchers warned of the rise of a new illicit market, STYK. One of the largest online hacker marketplaces, Genesis Market was dismantled by the FBI and Dutch law enforcement last week in an effort known as Operation Cookie Monster. Genesis Market was one of the major shops selling stolen consumer and corporate account identities. Genesis specialized in digital identities using "bots" to harvest fingerprints, cookies, saved logins, and autofill form data. The market sold access to accounts belonging to several companies used extensively by the financial services sector including PayPal, Gmail, LinkedIn, and Zoom.

While Genesis Market was taken down this week, a new illicit marketplace, STYK, emerged this year offering financial fraud services. STYK offers one-stop shopping for financial fraud. Styx offers a list of vendors selling compromised credit cards, cryptocurrency, e-commerce account credentials, online banking accounts, ID-related data, and payment data.

- The marketplace shows *Fraud Store* and *Bearss* as reputed vendors for data theft. These vendors feature stolen data for victims in the US, Canada, the Netherlands, the UK, and other countries.
- The popular intrusion vectors used include business loan data, phishing attacks targeting CPAs, social engineering, and other scams.

(Cont'd)

Significant to the financial sector, the site offers money laundering services based on commissions related to the popularity of the institution and the complexity of the cash-out process, including the tactics the launderers will have to deploy to successfully circumvent a payment platform's anti-fraud filters. The market directs users to Telegram channels where bots interact with buyers and provide samples of the products available.

Styx features a dedicated Trusted Sellers section, where the founders presumably list vetted reliable vendors to increase trust in the platform. It uses Telegram channels where various automated bots interact with buyers and provides samples of the products offered for sale to add reliability and trust. If the user shows interest in buying any service, they are instructed to first add the amount to their Styx wallet with a specified amount in cryptocurrency.

Styx stands as an example of how cybercrime marketplaces are evolving into enterprise-like businesses, aiming to become a one-stop shop for adversaries. As Styx and other similar darknet marketplaces continue to operate, it is crucial for organizations and individuals – especially those related to the financial sector - to prioritize cybersecurity measures to protect sensitive information and mitigate the risks associated with illegal online activities.

Cybersecurity Risks During Mergers and Acquisitions

Making sure the merger and acquisition process goes without a hitch

Summary

Statista reports that in 2022, there were 314 mergers and acquisition (M&A) transactions valued at more than one billion US dollars in the United States. The overall number of M&A deals in the 12 months ending 31 December 2022 amounted to 18,072, down from 23,161 in the previous year.

Additionally, there have been 29 mergers since 1 January 2023. Perhaps you've recently been involved in one, or one has been announced and you are undergoing the process.

Mergers and acquisitions are high-risk transactions with several factors in play that include market response, your competition, shareholder value, technical compatibility, the unknown – and of course cybersecurity risks.

Did You Know These M&A Factors?

According to PCBB, for banks with $1B and less in assets, factors in deciding whether to acquire another bank include:

- *Deposit base*
- *Lending team or talented lenders*
- *Loan portfolio mix*
- *Branch locations in attractive or growing markets*
- *Demonstrated loan growth*

Other factors are the opportunity to enhance technology, new business lines or niches, and executive talent.

Cybersecurity Landscape

Thoroughly understanding the current cybersecurity landscape is crucial. What are the current cybersecurity risks to the institution? What are the additional or residual risks facing you before, during, and after the acquisition? Due to size, risk, and complexity, it is important to document these in a report and ensure the other institution understands any change in practices or standards.

Does Your Institution Have an M&A Strategy?

One critical part of your institution's strategy involves reading your information security and technology personnel early in the process. Some critical questions and or points for consideration early on in the process include:

- *Have you required that a current security assessment be performed before the acquisition?*
- *To what degree has security been incorporated into their information systems?*
- *What does their regulatory IT examination indicate?*
- *Do you understand the surrounding risks to both of the institution's data? (e.g. customer and institution financial and information assets, GDPR)*
- *Are you evaluating the skill set of personnel? Is there sufficient expertise who can handle increased workloads, are there knowledge gaps? Also, are there upset personnel who may deliberately sabotage the merging of two institutions or illegally benefit by leaking information that could result in additional financial risk?*

Failed Institution Take Over

Institutions involved in regulatory seizures face unique challenges such as the failed institution's poor financial rating and additional problems that were manifested and tolerated included in any regulatory or internal audit reports. There is a careful balance in the time the institution is seized and reopened under the assigned institution – customer confidence that their assets are safe and the stability of the financial services industry is another crucial consideration.

Forging a Resilient Future

The countdown has begun for FS-ISAC's FinCyber Today event in Orlando, Florida on 1-4 October 2023. If you have something on your mind and want to share it, the call for presentations is now open through 16 May. View full guidelines, instructions, and recommendations for the CFP process here.