News from Monday, January 31, 2023. Reported on Monday, February 1, 2023.

Live links are embedded throughout today's briefing. To see the actual URL, hover your mouse over the link for a moment before clicking. These links were copied directly from the web site of the source article. Tyler Cybersecurity has not performed any testing on the sites / links for security.

Source	Article
Bleeping Computer	**Exploit released for critical VMware vRealize RCE vulnerability** Horizon3 security researchers have released proof-of-concept (PoC) code for a VMware vRealize Log Insight vulnerability chain that allows attackers to gain remote code execution on unpatched appliances. VMware patched four security vulnerabilities in its vRealize log analysis tool last week, two being critical and allowing remote attackers to execute code on compromised devices. Both are tagged as critical severity with CVSS base scores of 9.8/10 and can be exploited as part of low-complexity attacks that don't require user interaction. The first (CVE-2022-31706) is a directory traversal bug, and the second (CVE-2022-31704) is a broken access control flaw. They can be abused to inject maliciously crafted files into the operating system of impacted appliances. VMware also fixed a deserialization vulnerability (CVE-2022-31710) which triggers denial of service states, and an information disclosure bug (CVE-2022-31711) that attackers can use to gain access to sensitive session and application info. Horizon3 published a blog post on Friday containing additional information on how three of them could be chained by threat attackers to execute code remotely as root on compromised VMware vRealize appliances. The researchers also released a list of indicators of compromise (IOCs) that network defenders could use to detect exploitation within their networks after warning one day earlier that they're going to release that targets this bug chain. While there are only a few dozen instances publicly exposed on the internet, according to Shodan data, this is to be expected given that VMware vRealize Log Insight appliances are designed to be accessed from inside an organization's network. **OpenAI releases tool to detect AI-written text** OpenAI has released an AI text classifier that attempts to detect whether input content was generated using artificial intelligence tools like ChatGPT. "The AI Text Classifier is a fine-tuned GPT model that predicts how likely it is that a piece of text was generated by AI from a variety of sources, such as ChatGPT," explains a new OpenAI blog post. OpenAI released the tool today after numerous universities and K-12 school districts banned the company's popular ChatGPT AI chatbot due to its ability to complete students' homework, such as writing book reports and essays, and even finishing programming assignments. However, when analyzing content generated by ChatGPT and You.com's AI chatbot, it had a lot of difficulties detecting if the text was AI-generated. As educators will likely use the new AI Text Classifiers to check if students cheated on their homework assignments, OpenAI warns that it should not be used as the "sole piece of evidence" for determining academic dishonesty. "Our classifier is not fully reliable," warns OpenAI.

Source	Article
	"In our evaluations on a 'challenge set' of English texts, our classifier correctly identifies 26% of AI-written text (true positives) as 'likely AI-written,' while incorrectly labeling human-written text as AI-written 9% of the time (false positives)." **Over 29,000 QNAP devices unpatched against new critical flaw** Tens of thousands of QNAP network-attached storage (NAS) devices are waiting to be patched against a critical security flaw addressed by the Taiwanese company on Monday. Remote threat actors can exploit this SQL injection vulnerability (CVE-2022-27596) to inject malicious code in attacks targeting Internet-exposed and unpatched QNAP devices. QNAP also assigned this bug a CVSS base score of 9.8/10 and said it could be abused in low-complexity attacks by unauthenticated malicious actors without requiring user interaction. One day after QNAP released security updates to address this critical vulnerability, Censys security researchers published a report revealing that just over 550 out of more than 60,000 QNAP NAS devices they found online were patched. "Censys has observed 67,415 hosts with indications of running a QNAP-based system; unfortunately, we could only obtain the version number from 30,520 hosts. But, if the advisory is correct, over 98% of identified QNAP devices would be vulnerable to this attack," senior security researcher Mark Ellzey said. "We found that of the 30,520 hosts with a version, only 557 were running QuTS Hero greater than or equal to 'h5.0.1.2248' or QTS greater than or equal to '5.0.1.2234,' meaning 29,968 hosts could be affected by this vulnerability." Luckily, since this flaw is not yet abused in the wild and proof-of-concept exploit code hasn't yet surfaced online, there's yet time to patch these vulnerable NAS devices and secure them from attacks. **Microsoft: Over 100 threat actors deploy ransomware in attacks** Microsoft revealed today that its security teams are tracking over 100 threat actors deploying ransomware during attacks. In all, the company says it monitors over 50 unique ransomware families that were actively used until the end of last year. "Some of the most prominent ransomware payloads in recent campaigns include Lockbit Black, BlackCat (aka ALPHV), Play, Vice Society, Black Basta, & Royal," Microsoft said. "Defense strategies, however, should focus less on payloads but more on the chain of activities that lead to their deployment," since ransomware gangs are still targeting servers and devices not yet patched against common or recently addressed vulnerabilities. Meanwhile, LockBit, Hive, Cuba, BlackCat, and Ragnar ransomware operators have kept breaching and trying to extort a steady stream of victims throughout 2022. Nevertheless, ransomware gangs saw a massive revenue drop of around 40% last year as they were only able to extort roughly $456.8 million from victims throughout 2022, after a record-breaking $765 million in the previous two years, according to blockchain analytics company Chainalysis. However, this significant decline was not driven by fewer attacks but by their victims' refusal to pay the attackers' ransom demands. This year has started with a big win against ransomware groups after the Hive ransomware data leak and Tor payment dark web sites were seized as part of an international law enforcement operation involving the U.S. Department of Justice, the FBI, the Secret Service, and Europol.

Source	Article
	After hacking into Hive's servers, the FBI distributed more than 1,300 decryption keys to Hive victims and gained access to Hive communication records, malware file hashes, and details on 250 Hive affiliates. **Microsoft releases emergency updates to fix XPS display issues** Microsoft has released out-of-band (OOB) updates for some .NET Framework and .NET versions to address XPS display issues triggered by December 2022 cumulative security updates. Users will experience null reference exceptions and images or glyphs displaying incorrectly when viewing XPS documents rendered using affected Windows Presentation Foundation (WPF) based apps. "This update addresses a known issue which might cause XPS documents which utilize structural or semantic elements like table structure, storyboards, or hyperlinks to not display correctly in WPF-based readers," Microsoft added today. One of the workarounds requires you to run a PowerShell script to address the compatibility issue with last month's security updates for .NET Framework and .NET: 1. Download the PowerShell script 2. Open a PowerShell prompt as an administrator 3. Within the prompt, navigate to the directory where the script was downloaded 4. Run the command within the prompt: .\kb5022083-compat.ps1 -Install (you can use -Uninstall to remove the workaround) Redmond has shared an alternate workaround that can be used if the PowerShell script fails, which requires disabling the enhanced security behavior for XPS documents.
The Hacker News	**Additional Supply Chain Vulnerabilities Uncovered in AMI MegaRAC BMC Software** Two more supply chain security flaws have been disclosed in AMI MegaRAC Baseboard Management Controller (BMC) software, nearly two months after three security vulnerabilities were brought to light in the same product. Firmware security firm Eclypsium said the two shortcomings were held back until now to provide AMI additional time to engineer appropriate mitigations. The issues, collectively tracked as BMC&C, could act as springboard for cyber-attacks, enabling threat actors to obtain remote code execution and unauthorized device access with superuser permissions. The two new flaws in question are as follows - • CVE-2022-26872 (CVSS score: 8.3) - Password reset interception via API • CVE-2022-40258 (CVSS score: 5.3) - Weak password hashes for Redfish and API Specifically, MegaRAC has been found to use the MD5 hashing algorithm with a global salt for older devices, or SHA-512 with per user salts on newer appliances, potentially allowing a threat actor to crack the passwords. CVE-2022-26872, on the other hand, leverages an HTTP API to dupe a user into initiating a password reset by means of a social engineering attack, and set a password of the adversary's choice. CVE-2022-26872 and CVE-2022-40258 add to three other vulnerabilities disclosed in December, including CVE-2022-40259 (CVSS score: 9.9), CVE-2022-40242 (CVSS score: 8.3), and CVE-2022-2827 (CVSS score: 7.5).

Source	Article
HIPAA Journal	**Feds Warn of Malicious Use of RMM Software in Callback Phishing Attacks** Cybercriminals are increasingly using legitimate remote monitoring and management (RMM) software in their attacks, according to a recent joint alert from the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The campaign was first identified in October 2022 and involves callback phishing. The emails used in this campaign are difficult for email security solutions to identify as malicious as they contain no malicious hyperlinks or attachments. The emails notify the recipient about an impending charge and a phone number is provided in the email for the user to call if they want to avoid the charge being applied. The charges typically relate to a software solution that is coming to the end of a free trial. The user is told that the full price of the software will be charged to the user's account if no action is taken. Due to the high cost of the software, there is a reasonably high chance that the number will be called. The call is answered, and social engineering techniques are used to convince the user to navigate to a malicious domain and download software, which they are told is required to remove the software and prevent the charge. The software connects to a second-stage domain and downloads a portable version of legitimate remote access software such as AnyDesk and ScreenConnect. If executed, the software will connect to the attacker's RMM server and provide the attacker with access to the user's device. The self-contained, portable versions of these remote access solutions do not require an installation, and as such do not require administrator privileges. Organizations may have security controls in place to prohibit the installation of this software on the network, but portable versions will bypass these security controls and will allow the attacker to access the user's device as a local user. They can then move to other vulnerable machines within the local intranet or establish persistent access as a local user service. One of the main aims of these attacks is to trick users into logging into their bank accounts to initiate a refund scam. The attackers remain connected while the user accesses their bank account, and the user's bank account summary is modified to make it appear that an excess amount of money had been refunded. The user was then told to refund the excess to the operator of the scam.
SANS	**Microsoft Urges Organizations to Patch On-Premises Exchange Servers** Microsoft is warning customers that "attackers looking to exploit unpatched Exchange servers are not going to go away" and exhorting them to apply the most recent Cumulative Update and Security Update for Exchange server. The post also notes that users should "occasionally perform manual tasks to harden the environment, such as enabling Extended Protection and enabling certificate signing of PowerShell serialization payloads." **Update Available to Fix OpenEMR Vulnerabilities** Researchers from Sonar have detailed three vulnerabilities in the open-source health record and medical practice management software OpenEMR. The flaws – an unauthenticated file read, authenticated local file inclusion, and authenticated reflected XSS – could be exploited to execute arbitrary system commands and steal patient data. All three flaws are fixed in OpenEMR version 7.0.0. **ISC Patches Multiple BIND Vulnerabilities** The Internet Systems Consortium (ISC) has published four advisories to address high severity vulnerabilities in its Berkeley Internet Name Domain (BIND) 9. All of the flaws affect the named BIND9 daemon, which is an authoritative name server and a recursive resolver.

Source	Bulletin
ICS-CERT	**CISA Releases One Industrial Control Systems Advisory** CISA released one Industrial Control Systems (ICS) advisory on January 31, 2023. This advisory provides timely information about current security issues, vulnerabilities, and exploits surrounding ICS. CISA encourages users and administrators to review the newly released ICS advisory for technical details and mitigations: • ICSA-23-31-01 Delta Electronics DOPSoft

Source	Long Form Article
Dark Reading by Jonathan Watson	**Are Your Employees Thinking Critically About Their Online Behaviors?** A confused marketing team member nervously buys $1,000 worth of Amazon gift cards after receiving purchasing instructions via text from the "boss." The entire sales team mindlessly accepts cookies while visiting competitor websites and skips through privacy disclosures when downloading new apps to gather business intel. Your phone vibrates, and it's a client. They're demanding to know why sensitive customer information is in an unsecured Google Doc. These panic-inducing scenarios are familiar to most modern IT and security leaders and share something in common. Each hypothetical breakdown is the result of employees — and the digital public as a whole — being lulled into a false sense of security regarding their online behaviors. While IT and security leaders are aware of the accelerating landscape of digital threats, employees are less prepared, creating a risk for every organization. **Security Theater Distracts from Steady Improvements** We've seen the introduction of major privacy legislation to curb the rise in digital threats, which I fully support. However, sweeping laws like GDPR and regulations established stateside have had an effect or outcome more as security theater than as actual protections. What's security theater? It's a set of rules or guidelines that offer the appearance of security but don't guarantee it. Users aren't blameless, either. Security theater can also occur when consumers grow apathetic about well-intentioned protections. For example, while cookie notifications demonstrate transparency about how and where websites track and use customer data, does anyone read the full privacy statements? Do users understand the consequences of what they click? Or are they too inundated with notifications to notice? Until digital literacy and safety standards become mandatory in school curricula, the best way to ensure your employees are well-versed in the risks of their online actions is reframing thinking through improved security training and education. As a technology leader, you know each employee is an endpoint capable of inviting risk into the organization. But that also means employees can become safeguards against threats, too — when adequately prepared and in the right headspace. **Remove the Smoke and Mirrors** In addition to mandatory and routine training and security tools, the best way to ensure employees are vigilant about potential risks is to help them reframe their online mindset while encouraging them to leverage critical thinking in evaluating and defending against internal and external threats. Helping employees develop a healthier understanding of what's at stake when they engage online — and the value of the information they interact with once there — can strengthen digital habits and build more mindful, proactive thinking when faced with a threat or even before one occurs.

Source	Long Form Article
	Here are three mindset shifts to start with: 1. **Understand data's fundamental value**. Employees — and most online consumers — don't give much thought before hitting "accept all" when encountering cookies. Similarly, users skim or even skip privacy notices on apps or when signing up for services. These behaviors can feel perfunctory because these types of security notifications are nonstop when we engage online — and because "accepting" doesn't often seem like the value exchange that it is. If you can help employees understand the value of their data, they're more likely to realize how precious every online decision is and think more critically before clicking and accepting. Considering that one in three US workers has little to no skills using digital devices, a significant missing component to more robust security is workplace digital literacy training that focuses on the specific threats faced by your organization and industry. 2. **Act with intention**. When people realize the value of their data, they're more vigilant and protective of it. But your employees should also feel encouraged to proactively ask questions about risks and formulate better ways to protect themselves. For example, your teams should have access to and familiarity with a standardized communication plan for when they receive phishing texts or emails. Instead of simply deleting these threats, all employees should screenshot communications, forward images to the department in charge of security, and immediately alert fellow team members of the text. A discerning eye for security threats is only the first step — next, your employees should feel prepared to handle suspicious activity when encountered. 3. **Follow data best practices**, no matter the context. It's important to determine if your employees understand that customer data is sacred no matter how far removed from your actual clients. A good example of this concept comes from where I sit in legal tech. Our law firm customers deal daily with topics including divorce, bankruptcy, complex real-estate purchases, and more with their clients. Naturally, these legal proceedings cover a tremendous amount of personal, sensitive data stored on our platform. We take the protection of this information extremely seriously, knowing that a breach of this information cannot be undone and may ruin lives, and we work to improve our protective mechanisms. Protection against threats takes a team effort. As a result, we encourage our law firm clients to ensure that all their employees understand their role in protecting private information. We inform customers of security best practices — like using a password manager and enabling two-factor authentication, avoiding sending or sharing documents from unsecured accounts or devices, and putting contingency plans in place if sensitive client information is accidentally shared. When employees understand how their day-to-day behaviors — no matter how small — can expose sensitive data, they're less likely to introduce risk in the first place. While you strive to train employees on how to protect data in every scenario, building a habit of vigilance reduces the amount of reactive problem-solving required in the first place. Improving your employees' fundamental understanding and respect for the value of data shields your organization from digital threats. But without reinforcing this understanding through ongoing mindset shifts, the status quo and security theater of repetitive privacy notifications will make employees feel more complacent. With complacency comes risk — so, are your employees thinking critically about their online behaviors? And are you thinking critically about it, too?