News from Monday, June 5, 2023. Reported on Tuesday, June 6, 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.

Sources	Articles
Information Security Media Group	**Iowa Reports Third Big Vendor Breach This Year** The state government of Iowa reported to federal regulators a third major health data breach since April involving a third party vendor. In this case, the breach stems from an incident at dental health insurer MCNA Insurance Co., the firm disclosed late last month. The Iowa Department of Health and Human Services said hackers had compromised the protected health information of nearly 234,000 Iowa residents in an incident that affects nearly 9 million Americans across the country. Iowa is among more than 100 MCNA clients, which include other state health departments and Medicaid agencies, affected by the incident MCNA told Information Security Media Group that the nearly 234,000 Iowa Medicaid members reported by the state as being affected by the incident are also included in MCNA's total of affected individuals nationwide. This year, Iowa HHS has already reported to federal regulators two other large breaches involving incidents at business associates. One of those incidents affected 21,000 individuals. It involved a contractor, Telligen, which disclosed a 2022 hacking incident at a subcontractor, Independent Living Systems. The ILS breach affected about 4.2 million people nationwide On May 26, Iowa reported a breach involving business associate Amerigroup, which "inadvertently disclosed" the protected health information of 833 Iowa Medicaid members to 20 healthcare providers in paper explanation of payment notices. Three large breaches within weeks of each other illustrates vendor risk challenges that many state agencies face, said Keith Fricke, principal consultant consultancy tw-Security. Those issues include the large number of third parties that many state agencies deal with and the time it takes to conduct proper risk assessments of those vendors. "State agencies should try to manage the scope of vendor risk assessments by starting with ones falling into these categories: third parties storing, processing or transmitting large amounts of electronic PHI - and third parties having remote access into state agencies' networks," he told ISMG. **Microsoft Attributes MOVEit Transfer Hack to Clop Affiliate** Microsoft said an affiliate of the Russian-speaking Clop ransomware-as-a-service gang is behind a rash of attacks exploiting a recently patched vulnerability in Progress Software's managed file transfer product. A threat actor began exploiting a critical SQL injection vulnerability in MOVEit Transfer on May 27 and in some cases has taken data within minutes of deploying the web shells. Microsoft said the actor is Lace Tempest, also known as FIN11 or TA505. Known victims include British Airways, the BBC, U.K. drugstore chain Boots, and British payroll provider Zellis.

Sources	Articles
Bleeping Computer	**The Genesis Market Takedown – Keep Users Credentials Secure** For years, "dark" markets have contained stolen credentials for sale. One of the larger and more notorious markets was the Genesis Market, which was invite-only. Over five years, the market offered data on over 1.5 million computers and 80 million account access credentials, according to the US Justice Department. Recently, FBI and European law enforcement agencies arrested over 100 people in the takedown of the notorious Genesis Market. The operation was dubbed “Operation Cookie Monster.” The crime forum was taken down through a concerted effort to arrest those involved and a takedown of the associated web domains. Stealing credentials can be difficult, as it often requires patience and persistence. For those looking to exploit credentials, purchasing a stolen password from "dark" markets may be easier than stealing it themselves. These markets offer many different credentials for sale, some verified and some not. In fact, these marketplaces often resemble entirely legitimate businesses. They feature help desks and ticketing systems, making it easy and commonplace to buy stolen credentials. These exchanges often resemble traditional e-commerce sites and target buyers who may not be technically savvy but are in the market for such goods. The sheer volume of stolen credentials means that even if a few don't work, it only takes one or two with the correct information to be worthwhile and pay for the rest. This allows the markets to operate at scale without requiring every credential to work. As a result, stolen credential datasets are all the more valuable for threat actors. **KeePass v2.54 fixes bug that leaked cleartext master password** KeePass has released version 2.54, fixing the CVE-2023-32784 vulnerability that allows the extraction of the cleartext master password from the application's memory. When creating a new KeePass password manager database, users must create a master password, which is used to encrypt the database. When opening the database in the future, users are required to enter this master key to decrypt it and access the credentials stored within it. However, in May 2023, security researcher 'vdohney' disclosed a vulnerability and proof-of-concept exploit that allowed you to partially extract the cleartext KeepPass master password from a memory dump of the application. "The problem is with SecureTextBoxEx. Because of the way it processes input, when the user types the password, there will be leftover strings," explained vdohney in a KeePass bug report. "For example, when "Password" is typed, it will result in these leftover strings: •a, ••s, •••s, ••••w, •••••o, ••••••r, •••••••d." This dumper allows users to recover almost all master password characters apart from the first one or two, even if the KeePass workspace is locked or the program was closed recently.

Sources	Articles
The Hacker News	**The Annual Report: 2024 Plans and Priorities for SaaS Security** Over 55% of security executives report that they have experienced a SaaS security incident in the past two years — ranging from data leaks and data breaches to SaaS ransomware and malicious apps The SaaS Security Survey Report: Plans and Priorities for 2024, developed by CSA in conjunction with Adaptive Shield, dives into these SaaS security incidents and more. This report shares the perspective of over 1,000 CISOs and other security professionals and shines a light on SaaS risks, existing threats, and the way organizations are preparing for 2024. Anecdotally, it was clear that SaaS security incidents increased over the last year. More headlines and stories covered SaaS breaches and data leaks than ever before. However, this report provides a stunning context to those headlines. As seen in figure 1, an astounding 55% of organizations had a SaaS incident within the past 24 months. These incidents included data leaks (58%), malicious third-party applications (47%), data breaches (41%), and SaaS ransomware (40%), as seen in figure 2. One reason for the increase in security incidents is that current solutions aren't being deployed broadly enough. 7% of respondents claimed to have 100% of their SaaS stack monitored with 68% reporting that they were monitoring less than half their SaaS stack. The current SaaS security practices, like Cloud Access Security Brokers (CASB) and manual audits, are not enough to cover the SaaS stack. Unfortunately, these solutions are unable to meet the growing use and demands of the modern SaaS stack. Companies today have to secure hundreds of thousands of configurations and oversee thousands of user accounts while vetting thousands of third-party connected applications, which are beyond the capabilities of CASBs and overwhelm the resources of any manual effort. In response to increasing SaaS incidents, organizations report that they are now prioritizing SaaS Security. The survey shows that more executive-level leaders are involved in securing their SaaS stack and CISOs and security managers are seemingly transitioning from the role of controllers to that of governors in securing the SaaS stack. There are layers of responsibility involved in securing each app as oftentimes the ownership of the app sits in different business departments throughout the organization, while it's the security team that is the one ultimately responsible. **Magento, WooCommerce, WordPress, and Shopify Exploited in Web Skimmer Attack** Cybersecurity researchers have unearthed a new ongoing Magecart-style web skimmer campaign that's designed to steal personally identifiable information (PII) and credit card data from e-commerce websites. A noteworthy aspect that sets it apart from other Magecart campaigns is that the hijacked sites further serve as "makeshift" command-and-control (C2) servers, using the cover to facilitate the distribution of malicious code without the knowledge of the victim sites. Web security company Akamai said it identified victims of varying sizes in North America, Latin America, and Europe, potentially putting the personal data of thousands of site visitors at risk of being harvested and sold for illicit profits. "Attackers employ a number of evasion techniques during the campaign, including obfuscating [using] Base64 and masking the attack to resemble popular third-party services, such as Google Analytics or Google Tag Manager," Akamai security researcher Roman Lvovsky said. The idea, in a nutshell, is to breach vulnerable legitimate sites and use them to host web skimmer code, thereby leveraging the good reputation of the genuine domains to their advantage. In some cases, the attacks have been underway for nearly a month.

Sources	Articles
	"Rather than using the attackers' own C2 server to host malicious code, which may be flagged as a malicious domain, attackers hack into (using vulnerabilities or any other means at their disposal) a vulnerable, legitimate site, such as a small or medium-sized retail website, and stash their code within it," Akamai noted. The result of the attacks are two kinds of victims: legitimate sites that have been compromised to act as a "distribution center" for malware and vulnerable e-commerce websites that are the target of the skimmers.
Information Security Magazine	**Cloud Security is the Greatest Area of Concern for Cybersecurity Leaders According to EC-Council's Certified CISO Hall of Fame Report 2023** *A survey of global cybersecurity leaders through the 2023 Certified CISO Hall of Fame Report commissioned by the EC-Council identified 4 primary areas of grave concern: cloud security, data security, security governance, and lack of cybersecurity talent.* EC-Council, the global leader in cybersecurity education and training, recently released its Certified Chief Information Security Officer (CISO) Hall of Fame Report , honoring the top 50 Certified CISOs globally. This report reveals that approximately 50% of surveyed information security leaders identified cloud security as their top concern. Findings from the report suggest the top cybersecurity concerns with which organizations struggle and highlight the need for implementing robust security frameworks with skilled cybersecurity professionals to effectively contain emerging threats. On average, an enterprise uses approximately 1295 cloud services, while an employee uses at least 36 cloud-based services daily. Cloud security risk is real for businesses. Additional challenges identified in the report include third-party/vendor security management, network security, application security, endpoint security, rapid IT changes, business growth and expansion of hybrid work models, and an inadequate focus on cyber risk management. In a recent report published by IBM, the studied organizations experienced more than one data breach, reaching an all-time high frequency, and the cost of a data breach averaged USD 4.35 million. More than ever, businesses need strong, experienced cybersecurity leadership from individuals with reputable certifications. The respondents to the survey were cybersecurity leaders who hail from every region of the globe, with the highest concentrations in Asia and North America. These professionals were employed primarily in technology, financial services, government, retail, healthcare, education, transportation and automotive, and entertainment and hospitality. This Certified CISO Hall of Fame report and its accompanying survey is published annually to honor professionals from around the world for their exceptional leadership and professional contributions to the information security industry. The awardees demonstrate an exceptional understanding of the ever-evolving cybersecurity landscape, promoting the values of innovation, thought leadership, and collaboration through their work. "I am delighted to congratulate the newly inducted Certified CISOs into the 2023 Hall of Fame," says Jay Bavisi, President and CEO of EC-Council. "Their remarkable achievements and unwavering commitment to cybersecurity are truly inspiring. As industry leaders, they have been instrumental in driving innovation, enhancing security practices, and protecting organizations from ever-evolving threats. We take immense pride in their accomplishments and are confident that their expertise will continue to profoundly impact the cybersecurity landscape."

Source	Article
CISA	**CISA Adds Two Known Exploited Vulnerabilities to Catalog** CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. • CVE-2023-33009 Zyxel Multiple Firewalls Buffer Overflow Vulnerability • CVE-2023-33010 Zyxel Multiple Firewalls Buffer Overflow Vulnerability

Source	Long Form Article
Dark Reading by Jai Vijayan (7-9 Minute Read)	**Mass Exploitation of Zero-Day Bug in MOVEit File Transfer Underway** A threat group with likely links to the financially motivated group known as FIN11 and other known adversaries is actively exploiting a critical zero-day vulnerability in Progress Software's MOVEit Transfer app to steal data from organizations using the managed file transfer technology. MOVEit Transfer is a managed file transfer app that organizations use to exchange sensitive data and large files both internally and externally. Organizations can deploy the software on-premises, or as infrastructure-as-a-service or as software-as-a-service in the cloud. Progress claims thousands of customers for MOVEit including major names such as Disney, Chase, BlueCross BlueShield, Geico, and Major League Baseball. Researchers from Google's Mandiant security group who are tracking the threat believe the exploit activity may well be a precursor to follow-on ransomware attacks on organizations that have fallen victim so far. A similar pattern played out earlier this year after an attacker exploited a zero-day flaw in Forta's GoAnywhere file transfer software to access customer systems and steal data from them. The Microsoft Threat Intelligence team meanwhile said via Twitter today that it has attributed the attack to a baddie it calls "Lace Tempest," which is a financially motivated threat and ransomware affiliate that has ties to not only FIN11, but also TA505, Evil Corp, and the Cl0p gang. An initial investigation into the MOVit Transfer attacks by Mandiant showed that the exploit activity began on May 27, or roughly four days before Progress disclosed the vulnerability and issued patches for all affected versions of the software. Mandiant has so far identified victims across multiple industry sectors located in Canada, India, and the US but believes the impact could be much broader. "Following exploitation of the vulnerability, the threat actors are deploying a newly discovered LEMURLOOT Web shell with filenames that masquerade as human.aspx, which is a legitimate component of the MOVEit Transfer software," Mandiant said in a blog post June 2. The Web shell allows the attackers to issue commands for enumerating files and folders on a system running MOVEit Transfer software, retrieve configuration information, and create or delete a user account. Mandiant's initial analysis showed the threat actor is using LEMURLOOT to steal data that MOVEit Transfer users might have previously uploaded. "In some instances, data theft has occurred within minutes of the deployment of Web shells," Mandiant said. Further, LEMURLOOT samples on VirusTotal since May 28 suggest that organizations in several other countries including Germany, Italy, and Pakistan are also impacted. Mandiant is tracking the threat actor as UNC4857 and has described it as a previously unknown group with unknown motivations. But several artifacts from the group's attacks on MOVEit Transfer customers suggest a connection to FIN11, Mandiant said. FIN11 is a group that security researchers have associated with numerous financially motivated attacks on banks, credit unions, retailers, and other organizations since at least 2016. Progress itself has advised customers to review their MOVEit Transfer environments for suspicious activity during the past 30 days, suggesting the exploit activity may have been going on at least for that long. It has identified the vulnerability (now tracked as CVE-2023-34362) as an SQL injection error

Source	Long Form Article
	that affects all versions of its file transfer software. The flaw allows for unauthenticated access to MOVEit Transfer's database, the company noted, urging customers to patch the flaw on an emergency basis. The company's advisory included a sequence of mitigation steps that it recommends organizations take before they deploy the patch. Greynoise, which collects and analyzes data on Internet noise, says it has observed scanning activity related to MOVEit going back to March 3 and has recommended that customers should extend the window for their review to at least 90 days. John Hammond, senior security researcher at Huntress, says his company's investigation of the zero-day vulnerability in MOVEit Transfer suggests it could either be a SQL injection flaw as Progress has indicated, or it could be an unrestricted file upload vulnerability — or both. "We don't know the adversary's tooling just yet," Hammond says. While Progress has stated publicly that it is a SQL injection vulnerability, the full details of the attack chain and exploit remain unknown, he says. "The behavior that we see of staging a human2.aspx for this specific operation looks to be an uploaded file used for further persistence and post-exploitation after SQL injection," Hammond says. "The SQL injection vulnerability may open the door for this functionality by either bypassing authentication or leaking sensitive database information. But unfortunately, we aren't quite sure what or how yet." Meanwhile, Censys said it's search engine and Internet scanning platform had identified 3,803 hosts currently using the MOVEit service. Many of these instances are likely unpatched and therefore vulnerable to attack, Censys said. "What is particularly concerning is the diverse range of industries relying on this software, including the financial sector, education (with 27 hosts), and even the US federal and state government (with over 60 hosts)," Censys said in a June 2 blog post. The attack on MOVEit follows similar zero-day exploit activity that targeted Forta's GoAnywhere Managed File Transfer product in January. In that instance, the attackers leveraged a zero-day remote code execution flaw (CVE-2023-0669) in GoAnywhere to create unauthorized user accounts on some customer systems and used those accounts to steal data and install additional malware in the environment. Shortly after Forta's vulnerability disclosure, the Cl0p ransomware gang said it had exploited the issue at over 130 organizations worldwide. Security researchers expect file transfer technologies such as those from MOVEit and GoAnywhere to become increasingly popular targets for ransomware actors looking to pivot away from data encryption attacks to data theft. File transfer appliances and products from Accellion to GoAnywhere have become a valuable target for cybercriminals, says Satnam Narang, senior staff research engineer at Tenable. This is especially true for ransomware gangs such as Cl0p that have breached hundreds of organizations that rely on managed file transfer services to transfer sensitive data, he notes. "Businesses have come to rely on file transfer solutions over the years, which is why there are several different options available," Narang says. "By compromising file transfer solutions, threat actors are able to steal data on tens of hundreds of businesses." He adds, "By targeting individual file transfer instances, adversaries often have an opportunity to access very sensitive information. This proves to be valuable for threat actors, especially ransomware groups, who will threaten to leak the stolen data on the Dark Web."