March 2023

Q1 2023 Cyber Security Update

Cyber Security News/Insight

- The cybersecurity market grew by double-digits over the past five years. Worldwide, cybersecurity revenue is expected to grow to $173.5 billion in 2023 with the market's largest segment, Security Services contributing about $91.2 billion[1]. Post 2023, the market is estimated to grow at a compound annual growth rate (CAGR) of 10.9% through 2027, resulting in a market size of $262.4 billion, according to Statista[2].This growth is expected to be led by the cyber solution segment with an estimated CAGR of 14.9% and a resultant market size of $143.5 billion in 2027[3] followed by the security services segment with an estimated CAGR of of 6.8% and a resultant market size of $118.8 billion in 2027[4]. Region-wise, the largest market for cybersecurity is the U.S. which is expected to have a market size of $69.7 billion in 2023. During the period 2023-2027, it is expected to grow at a CAGR of 10.1% to a market size of $102.3 billion by 2027.[5]
- According to Cybersecurity Ventures, cybercrimes are expected to cost about $8 trillion in 2023 with the cost expected to grow at a CAGR of 15% to $10.5 trillion in 2025[6]. Ransomware remains one of the most prevalent forms of attack. According to Moody's, critical infrastructure including electric, gas and water utilities and hospitals face very high cyber risk exposure, while banks, telecommunications, technology, chemicals, energy and transportation services face high risk[7]. A McKinsey report predicts that the estimated addressable market in cybersecurity is a staggering $1.5-$2.0 trillion with only ~10% of the market penetrated at current levels.[8]
- The White House released the new US National Cybersecurity Strategy in March 2023, which seeks to protect critical infrastructure and increase collaboration with international bodies[9]. The Cybersecurity Infrastructure Security Agency (CISA) has been rolling out programs to stop cyberattacks since its inception. Its recent actions include the release of a joint Cybersecurity Advisory (CSA) with the FBI to stop ransomware attacks, with a focus on the Royal ransomware variant which has attacked US and international organizations since September 2022 onwards[10,11]. In addition, it has expanded its free of cost beta mobile app vetting service, which was initially authorized in February 2023, acknowledging the service's key role in combating a growing risk of mobile app vulnerabilities threatening Federal Civilian Executive Branch (FCEB) agencies.[12]
- The Department of Defense (the DoD) is expected to finalize Assessing Contractor Implementation of Cybersecurity Requirements and Cybersecurity Maturity Model Certification (CMMC) program in May 2023, which will require contractors in the DoD supply chain to obtain certification for compliance with cybersecurity procedures.[13]
- In December 2022, the EU published a draft approval of the EU – U.S. Transatlantic Data Privacy Framework to unlock transatlantic data flows, after striking a primary deal in March 2022. This deal is expected to enable multinational companies to easily transfer personal data from Europe to the US.[14]
- In EU, the NIS2 directive[15] which requires members of the EU to create the necessary cyber crisis management structure, increase harmonization regarding security requirements and reporting obligations, encourage member states to cover issues regarding the supply chain, vulnerability management, core

internet and cyber hygiene in their national cybersecurity strategies became effective in January 2023. The deadline for implementation for the member states is October 2024.[16]

- The European Parliament banned TikTok from staff devices over cybersecurity concerns during the last week of February 2023. The decision applied to only those devices overseen by the EU's executive branch. Previously, the White house directed federal agencies to remove TikTok from all government-issued devices.[17]
- In March 2023, Dell formed an alliance with CrowdStrike to provide cybersecurity solutions. Through the new strategic alliance, organisations can manage cyber threats and protect endpoints, cloud workloads, identity and data. CrowdStrike will also be available across a broad set of Dell offerings, including with the purchase of Dell commercial PCs in the coming months.[18]

Cybersecurity – Notable Ransomware Attacks and Breaches in Q1 2023

- On March 10, cloud computing vendor Blackbaud (NASDAQ: BLKB) was fined a $3 million civil penalty by the Securities and Exchange Commission (SEC) for misleading disclosures to investors related to a 2020 ransomware attack impacting more than 13,000 customers. The SEC found Blackbaud's claim that the ransomware attacker did not access donor bank account information or social security numbers to be misleading. Blackbaud agreed to cease and desist from committing violations and pay a $3 million civil penalty.[19]
- On March 2, US based fintech banking platform Hatch Bank suffered a data breach after hackers stole the personal information including social security numbers of ~140,000 customers from the company's Fortra GoAnywhere MFT secure file-sharing platform. The breach detected on January 29 was reported to the public only in March. While the company did not reveal the attacker's identity, the Clop ransomware gang told BleepingComputer that they were behind these attacks. Hatch Bank's financial technology allows small businesses to access bank services from other financial institutions.[20]
- On February 23, BlackBasta ransomware group attacked Satellite broadcast provider Dish Network (NASDAQ: DISH) which affected several of its subsidiaries including SlingTV and Boost Mobile forcing the company to shut down its IT systems. The company confirmed the attack only on February 28. The attackers may have stolen personal information belonging to employees, customers, or both.[21]
- On February 22, a ransomware attack at Dole PLC (NYSE: DOLE) resulted in plant shutdowns in North America and product shortages at some grocery stores. The company claimed that the impact on its operations was limited. The shutdown indicated that the attackers may have used a malware to target the company.[22]
- On February 17, the US Marshals Service (USMS) fell victim to a ransomware attack that resulted in sensitive law enforcement information including returns from legal process, administrative information, and personally identifiable information being compromised. The incident involved a standalone system and was disconnected from the network. The USMS is one of America's highest ranking law enforcement authorities, and possesses highly sensitive information related to national security, witness protection programs and convicted felons.[23]
- On February 14, the LockBit ransomware gang published the stolen data from Royal Mail, UK's leading mail delivery service, which was targeted by the gang on January 10. Royal Mail had a lengthy negotiation with the gang and was able to obtain some proof of data theft but refused to pay the ransom demand of $80 million. Royal Mail's international postal service remained affected for over a month with efforts in the interim to bring back its operation online.[24,25]

- On February 14, a small group called Al-Toufan targeted Bahrain's international airport and took down their websites. The group claimed responsibility for the attack to mark the 12-anniversary of an Arab Spring uprising in the country.[26]
- On February 13, application delivery controller (ADC) provider A10 Networks (NYSE: ATEN) revealed a cyberattack from the Play ransomware group. The company initially identified the attack on January 23 and mentioned that the attack did not impact products or solutions used by its customers and did not result in any data theft. The California-based company provides software and hardware ADCs covering next-gen and 5G networks, cloud security and threat intelligence.[27]
- On February 10, Pepsi Bottling Ventures, the largest privately-held bottler of Pepsi-Cola products in the US, informed individuals that their personal information was stolen. The monthlong breach was discovered on January 10, but internal investigations revealed that the first breach occurred on December 23 and the company blocked the unauthorized access on January 19. The company has taken steps to improve its security.[28]
- On February 10, multiple medical groups in the US namely Regal Medical Group, Lakeside Medical Organization, ADOC Medical Group and Greater Covina Medical in the Heritage Provider Network in California disclosed a ransomware attack that occurred on December 1, 2022, making patient information available to cybercriminals. The entities affected collectively sent a notice of breach to the California Attorney General's office noting that the data of 3.3 million patients were exposed in the attack including sensitive patient data.[29]
- On February 9, Canada's largest bookstore Indigo (TSE: IDG) was targeted by cyber attackers, preventing customers from accessing their website and to only accept cash payments at their stores. According to reports from Kela, a cyber intelligence company the stolen information was sold in the cybercrime market. The company confirmed that the personal information of both current and former employees were stolen in the attack by the LockBit ransomware gang.[30,31]
- On February 8, a ransomware attack forced the City of Oakland, US to take its information technology (IT) systems offline without affecting the core services like 911 and emergency services. The Play ransomware group began to leak the stolen data containing confidential documents, employee information, passports, and IDs.[32,33,34]
- On February 8, AmerisourceBergen (NYSE: ABC), an American drug distributor with multiple distribution centers in the United States, Canada and the UK disclosed a cyberattack from the Lorenz ransomware group on one of its subsidiaries. The incident came to light after the threat actors started publishing the entire stolen data. The threat actors set the post date to November 1, 2022, which suggested that the breach happened a few months back, even though the files were published later.[35]
- On February 6, the semiconductor equipment maker MKS Instruments (NASDAQ: MKSI) disclosed to investors about a cyberattack that occurred on February 3. MKSI's production systems had to be shut down and may cost the company upwards of $200 million in lost or delayed sales. Analysts at Cowen, a broker, estimate the final impact to be $500 million on the quarterly sales. As of February 28, the company was yet to recover from the impact of the cyberattack and was unable to file its annual report on time.[36,37]
- On February 2, UK-based car retailer Arnold Clark informed customers that their personal data was stolen as a result of a cyberattack on December 23. A ransomware group claimed to have stolen gigabytes of sensitive information. The firm has more than 200 dealerships in England and Scotland. The ransomware group named Play claimed credit for the attack, published a huge amount of stolen information, released 31 archive files of 500 megabytes (Mb) each, totaling roughly 15 gigabytes (Gb) on their website and threatened to publish more if the ransom was not paid.[38]

- On January 31, UK based software company **ION Group** became a victim of LockBit ransomware gang. The company's products are used by financial institutions, banks and corporations for trading, investment management and market analytics. The attack impacted ION Cleared Derivatives, a division of ION Markets, affecting some of its services. However, the attack forced US and Europe based customers to switch to manual processing of the trades, causing significant delays and affected some of the biggest banks, brokerages and hedge funds. The LockBit gang claimed to have stolen the data and threatened to publish the files on February 4. LockBit later claimed that the ransom amount was paid, declining to specify the amount. ION group did not comment on the payment.[39,40]
- On January 20, **Yum Brands (NYSE: YUM)**, the parent company behind KFC and Taco Bell revealed it had to close 300 hundred restaurants in the UK for a day. The company said that the attackers stole company data but found no evidence that customer data was stolen. The company took several security measures to enhance system protection and does not expect the attack to cause material impact to its business. It is also not known if YUM has paid the ransom money.[41]
- On January 20, **Costa Rica's** Ministry of Public Works and Transport (MOPT) announced that the department suffered a cyber-attack on January 17 where twelve encrypted servers were found. Six months before the attack, Costa Rica was targeted by the Conti ransomware gang which resulted in several government agencies being affected including the Ministry of Finance.[42]
- On January 9, Norway based industrial risk management and assurance solutions provider **DNV** disclosed a ransomware attack on its ship management software which impacted 70 of its customers and 1,000 vessels as it had to shut down the servers. However, the company clarified that the server outage does not affect any other DNV services. The identity of the attacker and the nature of data stolen is yet to be ascertained.[43]
- On January 5, cloud space company **Rackspace** was a victim after the Play ransomware group targeted the company's exchange servers and accessed the Personal Storage Table (PST) of 27 customers out of a total of nearly 30,000 customers. Play group apparently used the exploitation method involving a customer's credentials to gain access to the servers. CrowdStrike, which helped investigate the incident, has not found any evidence that the threat actor actually viewed, obtained, misused, or disseminated emails or data in the PSTs for any of the 27 Hosted Exchange customers in any way. Multiple lawsuits have been filed against Rackspace since the incident was disclosed.[44,45]
- On January 4, a database containing 235 million unique records of **Twitter** users and email addresses were posted on an online hacking forum. The information appears to have been collected via web-scraping rather than by hacking into Twitter systems and likely compiled in late 2021. It poses threats against people who use their Twitter handles to make statements against the government and individuals. In August 2022, a database containing information of 5.4 million Twitter users were offered for sale by hackers. Hackers could attempt to reset passwords to email addresses and control the accounts.[46,47]
- On January 3, **Canadian Copper Mountain Mining Corporation** (TSE: CMMC), producing an average of 100 million pounds of copper equivalent per year, announced the shut-down of its systems in the prior week due to a cyberattack on December 27. The company did not divulge details on the type of ransomware attack and how its systems were breached.[48]
- On January 3, **Wabtec Corporation** (NYSE: WAB) disclosed a data breach after a LockBit ransomware attack exposed personal and sensitive information. The company announced that hackers breached their systems and installed malware as early as March 15, 2022. The breach was detected by the company only on June 26, their internal investigation concluded on November 23, and the company started informing the affected individuals on December 30.[49]

- In other ransomware attacks, schools and universities have become a frequent target of cyber attackers. Some of the victims in the US include Xavier University, Swansea Public Schools, Bristol Community College, Des Moines Public Schools, Wawasee Community School Corporation, Nantucket Public Schools, Tucson Unified School District, Mount Saint Mary College, California Northstate University, Minneapolis Public Schools. Some others that were affected globally included Okanagan College in Canada, the University of Duisburg-Essen in Germany, Munster Technological University (MTU) in Ireland.[50]

New Products

- Palo Alto Networks (PANW) launched its cloud infrastructure in Switzerland in February 2023. This will allow Swiss customers to access the company's security capabilities while meeting data residency needs. The new cloud location will provide access to Palo Alto's products like Prisma® Access, Cortex and AIOps for Swiss customers.[51]

- In March 2023, Fortinet (FTNT) introduced its enhanced new products and services for operational technology (OT) environments as an expansion of its Fortinet Security Fabric for OT[52]. Prior to this, in February 2023, the company launched its Fifth-generation security processing unit (FortiSP5), which delivers significant secure computing power advantages over traditional CPU and network ASICs at lower cost and power consumption with the ability to enable new secure infrastructure across branch, campus, 5G, edge compute, operational technologies, and more[53]. In February 2023, during the Annual Meeting by the World Economic Forum (WEF), the company, with the support of Banco Santander (SAN), Microsoft (MSFT), and PayPal (PYPL) launched the Cybercrime Atlas, a tool to help organizations in mapping the cybercrime landscape that covers criminal operations, structures, and networks.[54]

- Cloudflare (NET) introduced several new Zero Trust email security solutions in January 2023, which are expected to tackle multichannel phishing attacks, provide data loss prevention and help speed up deployments [55]. These new solutions integrate Cloudflare Area 1 email security and its Zero-Trust platform.[56]

- Darktrace Plc (DARK) has introduced an AI enhanced product called PREVENT/OT in February 2023 which identifies the paths adversaries may take to attempt to disrupt the operations of critical infrastructure.[57] The company claims that this product helps in visualizing pathways within information technology (IT) and operational technology (OT) that lead to critical infrastructure assets, empowering defenders to harden environments and stay steps ahead of the adversary.[58]

Cybersecurity – M&A and IPO Activity in Q1 2023

Inside NQCYBR Index Activity:

- In January 2023, Cygna Labs, a highly specialized software developer with a focus on serving enterprises worldwide and a leading provider of DDI, cloud security, and compliance technology, announced today that it has entered into a definitive agreement to acquire NCC Group's DDI business[59].

- In January 2023, OneSpan Inc. (NASDAQ: OSPN), the digital agreements security company, today announced that it has agreed to acquire ProvenDB, an Australia-based startup that delivers secure storage and vaulting for documents based on blockchain technology, to provide an industry-leading trust model for high assurance contracts and documents. ProvenDB will extend the capabilities of OneSpan's Transaction

Cloud Platform to both public and private blockchains and serve as a modern technological foundation for high assurance business processes for Web3[60].

- In January 2023, OpenText (NASDAQ: OTEX and TSX: OTEX) completed the acquisition of Micro Focus in a cash and debt deal valuing Micro Focus International (London: MCRO) at $5.8 billion. The purchase price paid is 2.3x of Micro's trailing twelve months (TTM) revenue and 6.7x TTM adjusted EBITDA. Micro Focus builds and delivers enterprise cybersecurity solutions to their customers and technology leaders with trusted, intelligent solutions that give them insights, protection, compliance and resiliency. Micro Focus was removed from the index shortly after the acquisition was announced in 3Q'22[61, 62].
- In mid-February 2023, Zscaler announced an agreement to acquire a startup focused on protecting against attacks that target software-as-a-service, as concerns grow about the security of data in SaaS applications. The startup, Canonic Security, had exited stealth a year ago with technology that allows organizations to assess the security of applications and integrations that are connected to a certain SaaS app, before granting access to their own business applications. Terms of the acquisition deal were not disclosed. Canonic Security had announced raising just $6 million in funding[63].
- In February 2023, Identity and access management (IAM) company Okta has acquired threat intelligence firm Bad Packets. Bad Packets' extensive honeypot network will be used to bolster Okta's customer identity focus, threat insights, and overall technology offering[64].
- In February 2023, Trend Micro has acquired India-based security operations center (SOC) technology provider Anlyz to expand its orchestration, automation and integration capabilities. With this deal, Trend Micro also adds a new R&D center in India. [65]

Outside NQCYBR Index Activity:

- On January 20, private equity firm Thomas Bravo announced plansto to spend $1.3 billion to acquire Canadian software firm Magnet Forensics (TSX: MAGT) through its newly created Morpheus entity. Thoma Bravo plans to combine Magnet Forensics with Grayshift, a company that also sells digital forensics software and tools and in which it has a majority stake. The purchase price represents a 87% premium to the closing price on October 5, 2022, the last day prior to Thoma Bravo's submission of its initial non-binding proposal for an acquisition of the Company. The Magnet deal is expected to close in the second quarter of 2023. [66, 67]

Venture Capital and Other Private Equity Activity:

- In January 2023, private equity firm Bema Capital Investments acquired Beryllium InfoSec, a company that provides compliance and other cybersecurity services to government and defense industrial base organizations. [68]
- In January 2023, Iron Bow Technologies, which provides cybersecurity and other IT solutions to private and government organizations, announced buying GuardSight in an effort to expand its cybersecurity portfolio with GuardSight's SecOps and managed detection and response (MDR) capabilities. [69]
- In January 2023, Taiwan-based video intelligence, IoT technology and cybersecurity solutions provider Gorilla Technology Group has acquired UK-based SeeQuestor, whose technology turns CCTV video into actionable intelligence. [70]
- On February 15, USbased Descope raised $53 million in seed funding from Lightspeed Venture Partners and GGV Capital. The company plans to take on Okta's AuthO and other big companies in the

customer identity and authentication space. Descope's technology lets developers add authentication, user management and authorization capabilities to consumer and business applications with only a few lines of code. The company's target customers are small to mid-market software companies looking to outsource the authentication and user management workloads from vendors. Rishi Bhargava, co-founder of Descope had previously created Demisto before selling the company to Palo Alto Networks for $560 million in 2019.[71]

- On February 8, late-stage company Skybox Security closed a $50 million financing round from private equity firms including CVC Growth Funds, Pantheon, and J.P. Morgan taking the total amount raised to $335 million. Skybox product suite includes tools for firewall management, automated change management, network assurance, vulnerability control and threat intelligence.[72]

- On January 31, Saviynt, an Identity and access governance vendor, raised $205 million, led by AB Private Credit Investors' Tech Capital Solutions group, an affiliate of global investment management firm AllianceBernstein. Saviynt's technology in the intelligent identity and access governance category help organizations secure critical apps, data, and infrastructure in the cloud.[73]

- On January 25, Forward Networks raised $50 million in a series D Funding taking the total amount raised to $110 million. The recent round of funding was led by MSD Partners, with participation from Section 32, Omega Venture Partners, Goldman Sachs Asset Management, Threshold Ventures, A. Capital and Andreessen Horowitz. The company that specializes in security and reliability solutions for large enterprise networks provides attack surface management, vulnerability management and security posture management capabilities. [74]

- On January 6, US based secure access service edge (SASE) provider Netskope raised $401 million in an oversubscribed financing round led by Morgan Stanley Tactical Value, with participation from CPP Investments, Goldman Sachs Asset Management, and Ontario Teachers' Pension Plan. The total amount raised by the company stands at $1.5 billion. Combining security access service edge (SASE) and borderless SD-WAN technologies, the company's platform covers web security, data and threat protection, data loss prevention (DLP), Cloud Access Security Broker (CASB), and content filtering. In 2021, Netskope raised $300 million at a $7.5 billion valuation.[75]

[1] https://www.statista.com/outlook/tmo/cybersecurity/worldwide#revenue

[2] https://www.statista.com/outlook/tmo/cybersecurity/worldwide#revenue

[3] https://www.statista.com/outlook/tmo/cybersecurity/cyber-solutions/worldwide

[4] https://www.statista.com/outlook/tmo/cybersecurity/security-services/worldwide

[5] https://www.statista.com/outlook/tmo/cybersecurity/united-states

[6] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[7] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[8] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

[9] https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/

[10] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a

[11] https://www.cisa.gov/news-events/alerts/2023/03/02/fbi-and-cisa-release-stopransomware-royal-ransomware

[12] https://www.cisa.gov/news-events/news/under-promise-early-success-cisa-expands-its-beta-mobile-app-vetting-service

[13] https://www.wsj.com/articles/quarterly-cyber-regulations-update-february-2023-7c2af844

[14] https://www.wsj.com/articles/quarterly-cyber-regulations-update-february-2023-7c2af844

[15] https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF

[16] https://www.wsj.com/articles/quarterly-cyber-regulations-update-february-2023-7c2af844

[17] https://edition.cnn.com/2023/02/28/tech/tiktok-eu-ban-intl-hnk/index.html

[18] https://cionews.co.in/dell-crowdstrike-partner-for-cybersecurity-solutions/

[19] https://www.securityweek.com/blackbaud-fined-3m-for-misleading-disclosures-about-2020-ransomware-attack/

[20] https://www.bleepingcomputer.com/news/security/hatch-bank-discloses-data-breach-after-goanywhere-mft-hack/

[21] https://www.bleepingcomputer.com/news/security/dish-network-confirms-ransomware-attack-behind-multi-day-outage/

[22] https://www.securityweek.com/ransomware-attack-forces-produce-giant-dole-to-shut-down-plants/

[23] https://www.securityweek.com/ransomware-attack-hits-us-marshals-service/

[24] https://www.computerweekly.com/news/365531392/Royal-Mail-refused-to-pay-66m-LockBit-ransom-demand-logs-reveal

[25] https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-claims-royal-mail-cyberattack/

[26] https://www.securityweek.com/hackers-target-bahrain-airport-news-sites-to-mark-uprising/

[27] https://www.securityweek.com/play-ransomware-group-claims-attack-on-a10-networks/

[28] https://www.securityweek.com/pepsi-bottling-ventures-discloses-data-breach/

[29] https://www.bleepingcomputer.com/news/security/california-medical-group-data-breach-impacts-33-million-patients/

[30] https://www.bleepingcomputer.com/news/security/largest-canadian-bookstore-indigo-shuts-down-site-after-cyberattack/

[31] https://www.securityweek.com/canadian-bookstore-chain-indigo-says-employee-data-stolen-in-ransomware-attack/

[32] https://www.bleepingcomputer.com/news/security/city-of-oakland-systems-offline-after-ransomware-attack/

[33] https://www.bleepingcomputer.com/news/security/city-of-oakland-declares-state-of-emergency-after-ransomware-attack/

[34] https://www.bleepingcomputer.com/news/security/ransomware-gang-leaks-data-stolen-from-city-of-oakland/

[35] https://www.bleepingcomputer.com/news/security/drug-distributor-amerisourcebergen-confirms-security-breach/

[36] https://www.reuters.com/technology/chip-equipment-maker-mks-instruments-says-it-is-investigating-ransomware-attack-2023-02-06/

[37] https://www.ft.com/content/b8669140-8dde-493e-bb30-f5f1e9830804

[38] https://www.securityweek.com/uk-car-retailer-arnold-clark-hit-by-ransomware/

[39] https://www.bleepingcomputer.com/news/security/ransomware-attack-on-ion-group-impacts-derivatives-trading-market/
[40] https://www.reuters.com/technology/ion-starts-bring-clients-back-online-after-ransomware-attack-source-2023-02-07/
[41] https://www.securityweek.com/ransomware-shuts-hundreds-yum-brands-restaurants-uk/
[42] https://www.databreaches.net/bits-n-pieces-trozos-y-piezas-24/
[43] https://www.securityweek.com/ransomware-attack-dnv-ship-management-software-impacts-1000-vessels/
[44] https://www.securityweek.com/rackspace-completes-investigation-ransomware-attack/
[45] https://www.securityweek.com/play-ransomware-group-used-new-exploitation-method-rackspace-attack/
[46] https://www.securityweek.com/database-containing-235-million-twitter-user-records-available-free/
[47] https://www.washingtonpost.com/technology/2023/01/04/witter-leak-emails-handles/
[48] https://www.securityweek.com/ransomware-attack-forces-canadian-mining-company-shut-down-mill/
[49] https://www.bleepingcomputer.com/news/security/rail-giant-wabtec-discloses-data-breach-after-lockbit-ransomware-attack/
[50] https://www.blackfog.com/the-state-of-ransomware-in-2023/
[51] https://www.paloaltonetworks.com/company/press/2023/palo-alto-networks-goes-all-in-with-new-cloud-infrastructure-investment-in-switzerland
[52] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2023/fortinet-introduces-specialized-cybersecurity-products-services-for-ot-environments
[53] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2023/fortinet-unveils-new-asic-accelerate-networking-security-convergence-across-network-edges
[54] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2023/fortinet-helps-launch-cybercrime-atlas-initiative
[55] https://www.cloudflare.com/press-releases/2023/cloudflare-announces-comprehensive-email-security-and-data-protection-tools/
[56] https://www.cloudflare.com/press-releases/2023/cloudflare-announces-comprehensive-email-security-and-data-protection-tools/
[57] https://darktrace.com/news/darktrace-announces-prevent-ot-for-critical-infrastructure
[58] https://darktrace.com/news/darktrace-announces-prevent-ot-for-critical-infrastructure
[59] https://www.prweb.com/releases/2023/01/prweb19119626.htm
[60] https://www.onespan.com/about/news/onespan-acquire-blockchain-technology-provider-provendb-bring-secure-vaulting-future
[61] https://www.prnewswire.com/news-releases/opentext-buys-micro-focus-301734613.html
[62] https://www.microfocus.com/en-us/cyber-resilience/security-partner
[63] https://ir.zscaler.com/news-releases/news-release-details/zscaler-announces-industry-first-integrated-saas-supply-chain
[64] https://www.securityweek.com/cybersecurity-ma-roundup-34-deals-announced-in-february-2023/
[65] https://newsroom.trendmicro.com/2023-02-22-Trend-Micro-Acquires-SOC-Technology-Expert-Anlyz
[66] https://www.securityweek.com/thoma-bravo-to-buy-magnet-forensics-in-1-3b-transaction/
[67] https://www.thomabravo.com/press-releases/magnet-forensics-inc.-enters-into-definitive-agreement-to-be-acquired-by-thoma-bravo
[68] https://www.prnewswire.com/news-releases/beryllium-and-cuick-trac-secure-investment-from-bema-capital-301728658.html
[69] https://www.businesswire.com/news/home/20230126005231/en/Iron-Bow-Technologies-Announces-Acquisition-of-GuardSight-Inc.-to-Bolster-Cybersecurity-Portfolio
[70] https://www.globenewswire.com/news-release/2023/01/18/2591354/0/en/Gorilla-Technology-Group-Completes-Asset-Acquisition-of-SeeQuestor.html
[71] https://www.securityweek.com/descope-targets-customer-identity-market-with-massive-53m-seed-round/
[72] https://www.securityweek.com/skybox-security-raises-50m-hires-new-ceo/
[73] https://www.securityweek.com/saviynt-raises-205m-founder-rejoins-as-ceo/
[74] https://www.securityweek.com/forward-networks-raises-50-million-in-series-d-funding/
[75] https://www.securityweek.com/sase-company-netskope-raises-401-million/

Disclaimer:

Nasdaq® is a registered trademark of Nasdaq, Inc. The information contained above is provided for informational and educational purposes only, and nothing contained herein should be construed as investment advice, either on behalf of a particular security or an overall investment strategy. Neither Nasdaq, Inc. nor any of its affiliates makes any recommendation to buy or sell any security or any representation about the financial condition of any company. Statements regarding Nasdaq-listed companies or Nasdaq proprietary indexes are not guarantees of future performance. Actual results may differ materially from those expressed or implied. Past performance is not indicative of future results. Investors should undertake their own due diligence and carefully evaluate companies before investing. ADVICE FROM A SECURITIES PROFESSIONAL IS STRONGLY ADVISED.