Q2 2022 Cyber Security Update

Cyber Security News: Regulatory/Government

- On May 13, 2022, the European Commission accepted a political agreement between the European Parliament and EU Member States on a new directive of measures for existing rules on the security of network and information systems (NIS Directive) across the Union. This enhanced directive will now cover "medium and large entities from more sectors that are critical for the economy and society, including providers of public electronic communications services, digital services, waste water and waste management, manufacturing of critical products, postal and courier services and public administration, both at central and regional level". [1]

- On April 13, 2022, U.S. government organizations -- the Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) -- jointly alerted that advanced persistent threat (APT) actors have developed custom-made tools which can penetrate multiple industrial control systems (ICS) and supervisory control and data acquisition (SCADA) devices. Once access to the operational technology is gained, the attackers can then compromise or disrupt the affected devices. [2]

- Cybersecurity researchers have found that multiple APT spear-phishing campaigns have been activated by cyber criminals who are utilizing links and documents referencing the Russia/Ukraine war. Attackers are targeting government departments with news articles on the war containing malicious macros. Check Point (CHKP)'s research shows that cyber-attacks have increased 16% worldwide since the start of the war, and by 10% and 17% within Russia and Ukraine, respectively. [3]

- A survey was done by Crossword Cybersecurity with more than 200 chief information security officers (CISO) and senior cybersecurity professionals in the UK. According to respondents, companies are now more exposed to cyber threats than ever before. 61% of respondents think they are, at best, only "fairly confident" at managing the current cyber threat exposure. Also, 40% of organizations think their existing systems will be outdated in the coming few years due to rapid changes in technological innovation, as well as changes in the threat landscape. [4]

- Government entities in small nations appear increasingly exposed to cyber threats due to a lack of resources and spending on preventing breaches, ransomware, and other cyber-attacks. For instance:

    - 27 government entities in Costa Rica were under attack in April-May 2022, and some of the worst affected included the Ministry of Finance and its two portals, the Virtual Tax Administration Portal (public tax collection portal), and the Information Technology for Customs Control portal. The attack caused a delay in payment of pensions, salaries, subsidies, and tax collection.[5]

    - Several government organizations in Peru encountered a ransomware attack in Q2 2022, including The Directorate General of Intelligence (DIGIMIN), the Citizen Platform (a public query platform for the Peruvian government, gob.pe), and the Ministry of Economy and Finance. [6]

Notable Attacks & Breaches

- **Italy's** fifth most populous city of Palermo was under cyber-attack on June 3. Local IT experts were trying to restore the systems for several days, during which all services, public websites, and online portals remained offline (even beyond June 6 when it was first reported to public). The city hosts 2.3 million tourists annually, all of whom could not access online bookings for tickets to museums and theaters, or even confirm their reservations at sports venues. Full time residents were also impacted. Vice City ransomware group on June 9 claimed responsibility for the attack and threatened to publish the leaked data if the ransom was not paid. [7,8]

- On May 16, engineering giant **Parker-Hannifin Corporation** disclosed a data breach that exposed employees' personal information including social security numbers, financial accounts, health plan ID numbers, and other details. The breach was carried out by the Conti ransomware gang sometime between March 11 and March 14, impacting up to 58,000 employees. The gang started publishing the stolen information on April 1, when they released 3% of the dataset. On April 20, they went on to release the full dataset. [9]

- Japanese media giant **Nikkei Group** detected a cyberattack on its systems at their Singapore offices on May 13, though it was reported to the press only on May 19. The internal systems were immediately shut down to prevent and minimize any further impact. At the time of reporting to the press, the company did not notice any data leaks. In 2019, the company lost $29 million through a single wire transfer in a high-profile business email compromise (BEC) scam. [10,11]

- On a day when the **Costa Rica** government elected its 49th president (May 8), it had to declare a national emergency after the country was attacked by the Conti ransomware gang. The gang published 97% of the 672 gigabytes (GB) of leaked data belonging to various government agencies. The Ministry of Finance was the first to get impacted, and is still evaluating the magnitude of the cyberattack. The Conti gang demanded a $10 million ransom, which the government refused to pay. [12]

- **Coca-Cola** was a victim of a cyberattack when the Stormous gang breached its systems and stole 161 GB of data. The gang offered a small cache of data for sale on their website, with an asking price of 1.65 Bitcoin. The company has not confirmed that its data was stolen, but has been in touch with law enforcement agencies. It is the first time Stormous has posted a stolen data set. [13]

- On April 22, the finance minister of the Brazilian state of **Rio de Janerio** disclosed that it was hit by a cyberattack. The LockBit ransomware gang reportedly stole 420 GB data from the state's finance department, and demanded a ransom payment in exchange for not publishing the data. [14]

- Wind turbine firm **Nordex** also got attacked by Conti, which forced the company to shut down its operations after an early detection. The intrusion happened on March 31 and was reported on the company website on April 2, with Conti claiming responsibility on April 14. The gang has not leaked any data yet, indicating that they either could not steal any data, or that perhaps a negotiation was ongoing between the company and the gang for a ransom payment. [15,16]

- On April 11, Japanese technology giant **Panasonic** disclosed a cyberattack that occurred at its Canadian operations in February, less than six months after it was previously targeted by cyber gangs. Conti claimed responsibility for the attack and is said to have stolen 2.8 GB of data from the company. Panasonic's previous cyberattacks took place in November 2021 and December 2020. [17]

- The BlackCat ransomware gang attacked **Florida International University** on April 11. The gang claims to have stolen 1.2 terabytes (TB) of contracts, accounting documents, social security numbers, email databases and more from students, teachers, and staff. Cybersecurity experts confirmed the stolen data included sensitive information from staff and students. [18]

- Conti also attacked **Snap-on**, an American automotive tool manufacturer, which disclosed the breach on April 7. The company detected unusual activity in their network around March 1 to March 3, and it immediately shut down its systems. The company also revealed that important information about its employees was stolen. According to BleepingComputer,

Mitchell1 – one of Snap-on's subsidiaries – suffered an outage caused by a cyberattack, although Snap-on did not reveal this publicly. Conti initially leaked 1 GB of the stolen data, but quickly removed it from their site suggesting that Snap-on may have paid the ransom amount. [19]

- Indonesian government-controlled oil & gas giant **Perusahaan Gas Negara (PGN)** was struck by the Hive ransomware gang on April 3. The company did not respond to the news, but their website was down after the attack took place. [20]
- Several universities, colleges, and public school systems were targeted by cyberattackers in April and May. In the U.S., some of the victims included A&T University in North Carolina, Austin Peay State University in Tennessee, Kellogg Community College in Michigan, Mercyhurst University in Pennsylvania, Fort Summer Municipal schools in New Mexico, Washington Local Schools in Ohio, Martin University in Indianapolis, and North Orange County Community College in California. Other institutions affected outside the U.S. included De MontFort School in Eversham in the U.K., and Regina Public Schools in Canada. [21]

New Products

- In June 2022, **VMware, Inc.** (NASDAQ: VMW) introduced Contexa, its full-fidelity threat intelligence capability that offers significant improvements to its unique lateral security offering across multi-cloud environments for both modern and traditional applications. With Contexa, VMware is restructuring traditional security analytics by analyzing telemetry from the hybrid cloud, networks, and various systems to detect threats.[22,23]
- In June 2022, **Fortinet** (NASDAQ: FTNT) introduced FortiRecon, a complete Digital Risk Protection Service (DRPS) that includes a powerful combination of machine learning, automation capabilities, and FortiGuard Labs cybersecurity experts to manage a company's risk posture and advise meaningful action to protect their brand reputation, enterprise assets, and data. FortiRecon adds to Fortinet's existing portfolio of early detection and advanced response products, which includes FortiNDR, FortiXDR, FortiDeceptor, in-line sandboxing, as well as advanced automation with FortiAnalyzer, FortiSIEM and FortiSOAR.[24] In May 2022, **Fortinet** introduced FortiNDR, a new network detection and response offering that utilizes powerful artificial intelligence and pragmatic analytics to enable faster incident detection and an accelerated threat response.[25]
- In June 2022, **CrowdStrike Holdings** (NASDAQ: CRWD) added new features to its Falcon extended defense and response platform while expanding its CrowdXDR Alliance with new strategic partners. CrowdStrike Asset Graph is a new graph database fueled by the CrowdStrike Security Cloud that provides users a 360-degree view of managed and unmanaged assets. Additionally, CRWD launched Humio for Falcon, a new service that helps to extend the amount of time that telemetry data can be retained. Along with this, management declared it has expanded the reach of the Falcon Extended Detection and Response (XDR) service to enable integration with security tools and platforms from Menlo Security, Ping Identity, and Vectra AI. [26,27]
- In June 2022, **Cisco Systems** (NASDAQ: CSCO) launched the unified Secure Access Service Edge (SASE). This platform will include security across hybrid and multi-cloud environments with capabilities for securely connecting people, applications and devices located anywhere. The platform will help to ensure threat prevention, detection, response, and remediation at scale, with no vendor lock-in.[28,29]

M&A and IPO Activity

Inside NQCYBR Index Activity:

- Private equity firm **Thoma Bravo** plans to completely acquire identity and access management powerhouse **SailPoint** (NYSE: SAIL) for $6.9 billion. As per the announcement of the deal on April 11, the PE firm will pay $65.25/share to all shareholders of SailPoint, which represented a 48% premium to SAIL's 90-day average stock price. The company's management actively

looked for new bidders in the "go-shop" period that expired on May 16, 2022 but failed to get alternate bidders. In August 2014, Thoma Bravo bought a majority stake in SailPoint, and took it public in 2017. The deal is expected to close by year-end 2022, subject to shareholder approval and fulfilling regulatory requirements. [30,31] SailPoint was removed from the index on June 20, 2022.

- On April 6, investment firm Turn/River Capital announced an acquisition of Israel-based **Tufin** (NYSE: TUFN), a security policy management firm, for $570 million in cash. The agreement included a 30-day "go-shop" period until May 5, 2022. The $13.00 per share all-cash offer represented a 44% premium over Tufin's closing share price on April 5, 2022, but still less than the $14.00 per share price when the company went public in April 2019. The deal comes at a relatively low valuation multiple of 5x 2022 revenues (FY 2021 revenue at $110.9 million) when compared to other listed cybersecurity firms. Shareholder and regulatory approvals are pending for the deal, which is expected to close on June 30, 2022. [32] Tufin was removed from the index on June 20, 2022.

Outside NQCYBR Index Activity:

- On June 7, **IBM** (NYSE: IBM) announced it will acquire **Randori**, an early-stage attack surface management (ASM) startup based in Boston, Massachusetts, signaling the IT giant's cybersecurity expansion initiatives. Randori sells technology to help defenders conduct simulated hacking attacks on a continuous basis, which IBM plans to fold into its own products. The employee skills of Randori will add to IBM's X-Force offensive cybersecurity team. The financial terms of the deal were not disclosed, but Randori raised approximately $30 million in venture capital funding since its launch four years ago, including a recent $20 million Series A round led by Harmony Partners. The deal is expected to close in the next few months. [33]

- On June 1, Florida-based **ReliaQuest**, a security operations vendor, announced its intention to acquire threat intelligence startup **Digital Shadows** in a deal valued at $160 million. The acquisition equips the operations team to detect and quickly respond to threats with real-time internal and external visibility. ReliaQuest had previously raised $300 million from leading global investment firm KKR in August 2020, with participation from Ten Eleven Ventures and ReliaQuest founder and CEO Brian Murphy. The boards of both companies have approved the proposal, which is now subject to closing requirements and regulatory approvals. [34,35,36]

- On April 28, **Synopsys** (NASDAQ: SNPS) announced an acquisition of **White Hat Security** in an all-cash deal for $330 million. SNPS is a California-based electronic design company. With the acquisition of White Hat, the company is entering the dynamic application security market (DAST). SNPS previously acquired Coverity for $375 million, Black Duck Software for $550 million, and Cigital to enhance its cybersecurity capabilities in a big way. According to Jason Schmitt, general manager of the Software Integrity Group at Synopsys, the White Hat Security deal merges two companies that are "strategically aligned, with a shared vision for delivering SaaS-based security testing services and building security into the software development life cycle." The deal was completed on June 23. [37]

- On April 12, investment firm **Kohlberg Kravis Roberts & Co. (KKR)** agreed to acquire privately-held **Barracuda Networks** from Thoma Bravo. Financial terms of the deal were not disclosed, but Reuters reported the value to be nearly $4 billion. Barracuda, founded in 2003, is best known for its email, web, and network security solutions, and counts more than 200,000 customers around the world. During Thoma Bravo's ownership, the company expanded and enhanced its cybersecurity offerings, generating annual revenues of approximately $500 million. KKR's investments in the cybersecurity sector also include Ping, Cylance, DarkTrace, ForgeRock, NetSPI and Optiv, among others. [38]

Venture Capital and Other Private Markets Activity:

- On June 2, **JupiterOne**, a cybersecurity startup based in North Carolina, announced it raised $70 million – another sign of investors' interest in the cyber asset attack surface management (ASM) space. The new Series C financing is in addition to $49 million raised in earlier rounds, and values the company at upwards of $1 billion. The company's technology is available

through a cloud-native Software as a Service (SaaS) platform, and is used to help enterprises easily map, analyze, and secure complex cloud environments. [39]

- On June 1, **Paladin Capital Group**, a cybersecurity and technology investment firm, announced the closing of its Cyber Fund II with $370 million in total funds raised. "At a time when cybersecurity could not be more important, Cyber Fund II is investing in digital solutions of absolute need to advance, sustain, and defend critical infrastructure and modern society," said Michael Steed, Founder and Managing Partner of Paladin Capital Group. The fund has already invested in companies including Corellium, Nisos, and Virtuoso. [40]
- On May 24, **Semperis**, a New Jersey-based enterprise identity protection vendor, announced that it had raised $200 million in Series C funding, valuing the company at more than $1 billion and bringing the total amount raised to $254 million. The funding was led by **KKR**. Ten Eleven Ventures, Paladin Capital Group, Atrium Health Strategic Fund, Tech Pioneers Fund, and Insight Partners also invested. The company currently has two products to offer:
    - Semperis Directory Services Protector, which helps organizations protect Active Directory
    - Semperis Active Directory Forest Recovery, which is designed to help organizations recover following an attack [41]
- On May 11, California-based email security vendor **Material Security**, in a series C venture capital funding round, announced the raising of $100 million. The funding values the company at $1.1 billion just two years after rolling out its first product. Material offers security teams the ability to redact sensitive content in email – even older archived mail – and make them available only after a two-factor verification. Their technology is marketed as helping with email data leak prevention, account takeovers, phishing herd immunity, and other visibility and admin controls. [42]
- On May 10, San Francisco-based email security vendor **Abnormal Security** announced the raising of $210 million, bringing the total amount raised to $285 million since its founding in 2018. The new round of funding comes at a valuation of $4 billion and was led by Insight Partners, with additional investment from Greylock Partners and Menlo Ventures. The company uses artificial intelligence (AI) to detect abnormal behavior and stop threats such as business email compromise (BEC) before they can reach the inbox. The company plans to use the funds for product development and expansion into Europe, Japan, and Asia. [43]
- On May 3, California-based infrastructure access management firm **Teleport** announced a Series C funding round of $110 million from Bessemer Venture Partners valuing the firm at $1.1 billion. The firm had previously raised $59.2 million. As the widespread adoption of hybrid and work-from-home arrangements continues, Teleport's solution reduces the complexity to secure remote access to cloud assets and increases the security of remote access management. [44]
- On April 20, **ThreatLocker** raised $100 million in a Series C funding from General Atlantic, with additional investment from Arthur Ventures and Elephant VC. The Florida-based company was founded in 2017 and operates as a zero-trust endpoint security provider. The company claims their solutions can block known and unknown application vulnerabilities. The funds will be utilized for product development and for global expansion. [45]
- On April 19, **Fortress Information Security** announced that it raised $125 million from Goldman Sachs Asset Management. The company had previously raised $40 million between 2015-2020. The company plans to use the funds to help secure supply chains for critical industry operators and government agencies. Developed in collaboration with electric utility companies, its premier offering is now being used to secure 40% of the U.S. power grid. [46]
- On April 13, **Critical Start**, a Texas-based managed detection and response (MDR) solutions provider, announced that it raised more than $215 million from private equity firm Vista Equity Partners. The firm provides MDR, incident response, forensic services, and security monitoring and analytics services that can integrate with existing endpoint detection and response (EDR), endpoint protection platforms (EPP), and security information and event management (SIEM) tools. [47]
- **Ten Eleven Ventures** announced it had raised $600 million for a cybersecurity investment fund. [48]

- **SYN Ventures** raised $300 million for investments in cybersecurity, industrial security, national defense, privacy, regulatory compliance, and data governance companies. [49]
- Israel's **YL Ventures** announced it had raised $400 million for a fund that will invest in seed-stage rounds of approximately 10 cybersecurity startups at a pace of 3 startups per year.[50]

[1] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2985
[2] https://www.cisa.gov/uscert/ncas/alerts/aa22-103a
[3] https://www.infosecurity-magazine.com/news/global-apt-ukraine-war-phishing/
[4] https://www.helpnetsecurity.com/2022/05/26/organizations-cyber-strategy/
[5] https://www.reuters.com/world/americas/cyber-attack-costa-rica-grows-more-agencies-hit-president-says-2022-05-16/

[6] https://blog.cyble.com/2022/05/30/cyberattacks-on-government-machinery/
[7] https://www.bleepingcomputer.com/news/security/italian-city-of-palermo-shuts-down-all-systems-to-fend-off-cyberattack/
[8] https://www.bleepingcomputer.com/news/security/vice-society-ransomware-claims-attack-on-italian-city-of-palermo/
[9] https://www.bleepingcomputer.com/news/security/engineering-firm-parker-discloses-data-breach-after-ransomware-attack/
[10] https://www.bleepingcomputer.com/news/security/media-giant-nikkei-s-asian-unit-hit-by-ransomware-attack/
[11] https://www.bleepingcomputer.com/news/security/media-giant-nikkei-loses-29-million-to-bec-scammers/
[12] https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/
[13] https://www.bleepingcomputer.com/news/security/coca-cola-investigates-hackers-claims-of-breach-and-data-theft/
[14] https://therecord.media/rio-de-janeiro-finance-department-hit-with-lockbit-ransomware/
[15] https://www.bleepingcomputer.com/news/security/wind-turbine-firm-nordex-hit-by-conti-ransomware-attack/
[16] https://www.nordex-online.com/en/2022/04/nordex-group-impacted-by-cyber-security-incident/
[17] https://techcrunch.com/2022/04/11/panasonic-canada-ransomware/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKD3Aw5iEYfRIUKvwwDEyYEdOgj6PwSMEeVD1nU_WM86VpLaZ3knA99V67K8YThLkNWZ3_3ioUnZlktFGgcOoDd5lSTmfr-VgvlOs4-BtHzg8CAlUW5BzGjkr7wBHFpUG182YSc5xDEFt6yf2pRamRR6DifjdnUn2pbO1RwcOuEG&_guc_consent_skip=1655290236
[18] https://therecord.media/blackcat-ransomware-group-claims-attack-on-florida-international-university/
[19] https://www.bleepingcomputer.com/news/security/snap-on-discloses-data-breach-claimed-by-conti-ransomware-gang/
[20] https://techmonitor.ai/technology/cybersecurity/hive-ransomware-gang-pgn
[21] https://www.blackfog.com/the-state-of-ransomware-in-2022/#April

[22] https://news.vmware.com/releases/contexa-threat-intelligence
[23] https://www.scmagazine.com/editorial/brief/cloud-security/contexa-threat-intelligence-database-by-vmware-launches

[24] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2022/fortinet-unveils-new-digital-risk-protection-to-empower-security-and-executive-teams

[25] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2022/fortinet-introduces-self-learning-ai-capabitilies-new-network-detection

[26] https://siliconangle.com/2022/06/06/crowdstrike-announces-new-products-adds-new-crowdxdr-alliance-members/
[27] https://securityboulevard.com/2022/06/crowdstrike-adds-automated-asset-discovery-to-cloud-platform/

[28] https://www.crn.com/slide-shows/security/20-hottest-cybersecurity-products-at-rsac-2022/21?itc=refresh
[29] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2022/m05/an-argument-for-sase-and-legacy-integration.html
[30] https://www.securityweek.com/thoma-bravo-take-sailpoint-private-69b-all-cash-deal

[31] https://www.businesswire.com/news/home/20220517005418/en/SailPoint-Announces-Expiration-of-%E2%80%9CGo-Shop%E2%80%9D-Period
[32] https://www.securityweek.com/tufin-agrees-570-million-acquisition-30-day-go-shop-option
[33] https://www.securityweek.com/ibm-acquire-randori-attack-surface-management-tech
[34] https://www.securityweek.com/reliaquest-buy-digital-shadows-160-million
[35] https://www.reliaquest.com/newsroom/press-release/reliaquest-raises-over-300-million-growth-financing-kkr-led/
[36] https://www.wsj.com/articles/reliaquest-to-buy-digital-shadows-for-160-million-11654081200
[37] https://www.securityweek.com/synopsys-acquire-white-hat-security-330m-all-cash-deal
[38] https://www.securityweek.com/kkr-acquire-barracuda-networks-thoma-bravo
[39] https://www.securityweek.com/cloud-security-startup-jupiterone-lands-70-million-unicorn-valuation
[40] https://www.securityweek.com/paladin-capital-closes-372-million-cyber-fund-ii
[41] https://www.securityweek.com/semperis-banks-200-million-scale-enterprise-id-protection-tech
[42] https://www.securityweek.com/email-security-vendors-score-billion-dollar-valuations
[43] https://www.securityweek.com/email-security-firm-abnormal-security-raises-210-million-4-billion-valuation
[44] https://www.securityweek.com/identity-based-infrastructure-access-firm-teleport-raises-110-million
[45] https://www.securityweek.com/threatlocker-raises-100-million-zero-trust-endpoint-security-solution
[46] https://www.securityweek.com/fortress-raises-125-million-secure-critical-industry-supply-chains
[47] https://www.securityweek.com/mdr-provider-critical-start-lands-215-million-growth-investment
[48] https://www.securityweek.com/ten-eleven-ventures-raises-600m-fund-cybersecurity-investments
[49] https://www.securityweek.com/syn-ventures-closes-300m-fund-cybersecurity-bets
[50] https://www.securityweek.com/yl-ventures-closes-400-million-cybersecurity-investment-fund

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.