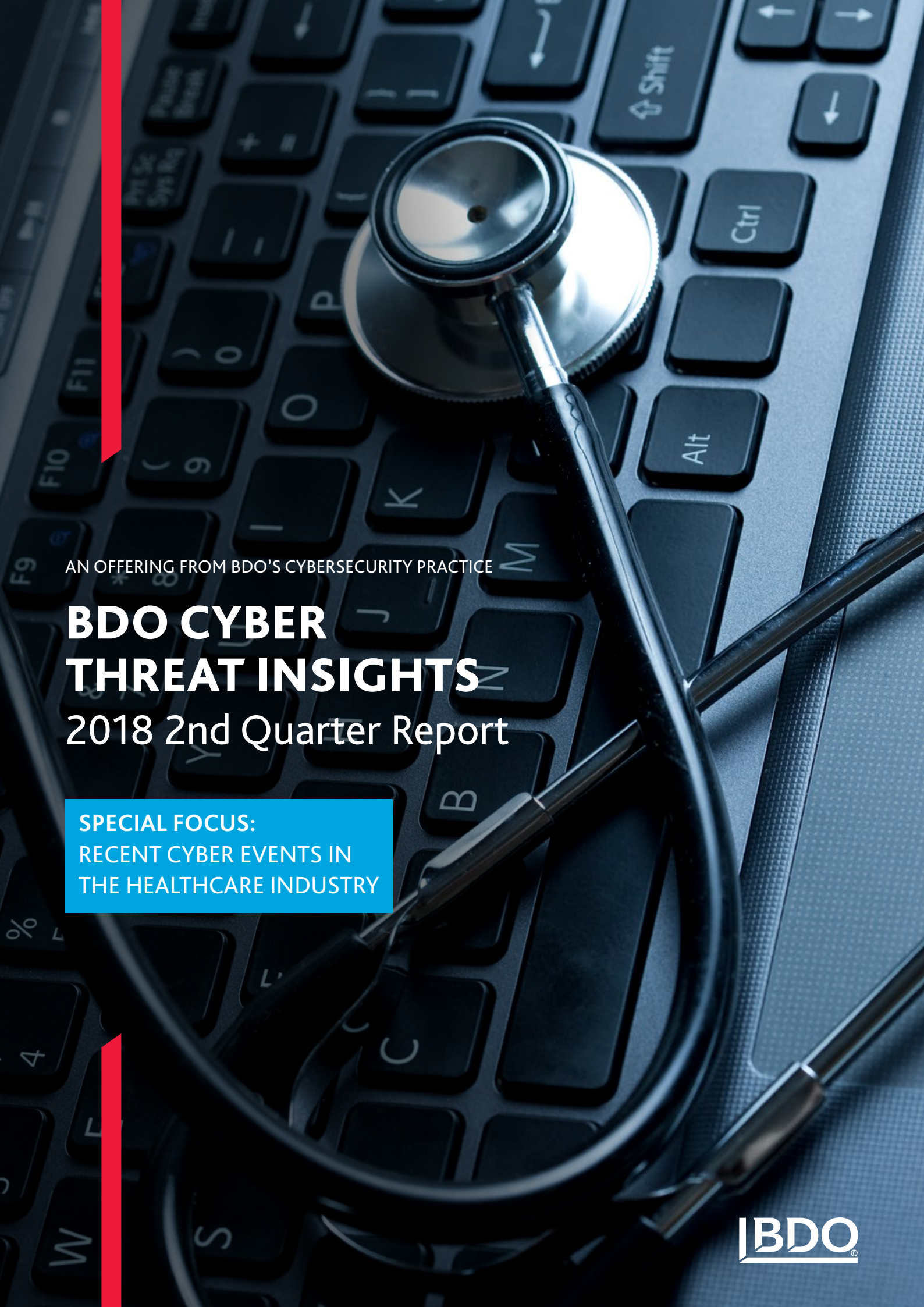


AN OFFERING FROM BDO'S CYBERSECURITY PRACTICE

BDO CYBER THREAT INSIGHTS

2018 2nd Quarter Report

SPECIAL FOCUS:
RECENT CYBER EVENTS IN THE HEALTHCARE INDUSTRY

BDO

In this issue

Preface

Nation-backed cyber-criminal activity stole the spotlight in a review of cyber activity during the first half of 2018.

Russia and China continue to be the most prominent cyber actors, both via:

- **Nation-State cyber warfare groups, such as APT28 and APT29.** These groups are highly capable and have considerable resources. In recent years, they have steadily begun focusing on espionage, destructive attacks and disinformation propagation via social media platforms and other media outlets.
- **Cyber-Criminal groups, with Cobalt and Carbanak being the most noteworthy.** These groups target a wide gamut of sectors, notably financial and healthcare organizations. A joint international operation arrested an individual suspected to be behind these groups in March.[1] However, their operations have not been disrupted; Cobalt successfully executed a large phishing campaign in May.[2]
- **Several Chinese attack campaigns also surfaced during the first half of the year.** The two most notable attacks were against western defense/military targets, giving a reminder of China's cyber capabilities and intentions. APT15, a Chinese-affiliated cyber espionage group, stole sensitive records and information from the UK military. Chinese hackers stole over 600GB of data regarding submarines and classified weapon systems from a defense contractor of the U.S. Navy.

In May, an attack against Banco de Chile affected 9,000 computers and corrupted 500 servers, enabling the attackers to steal $10 million dollars via the SWIFT system. The attack is currently attributed to North Korea and was the first time that a financially motivated attacker targeting a large financial organization executed a financial heist in conjunction with a sophisticated and fully realized wiper attack.

This modus operandi will force organizations and companies across all industries to re-evaluate how they can better respond to and mitigate multi-vector attacks that take place against several systems. Furthermore, cyber-attack contingencies must be modified to allow a rapid, yet organized, shut-down of an organization's computer systems to survive such attacks.

Special Recommendations

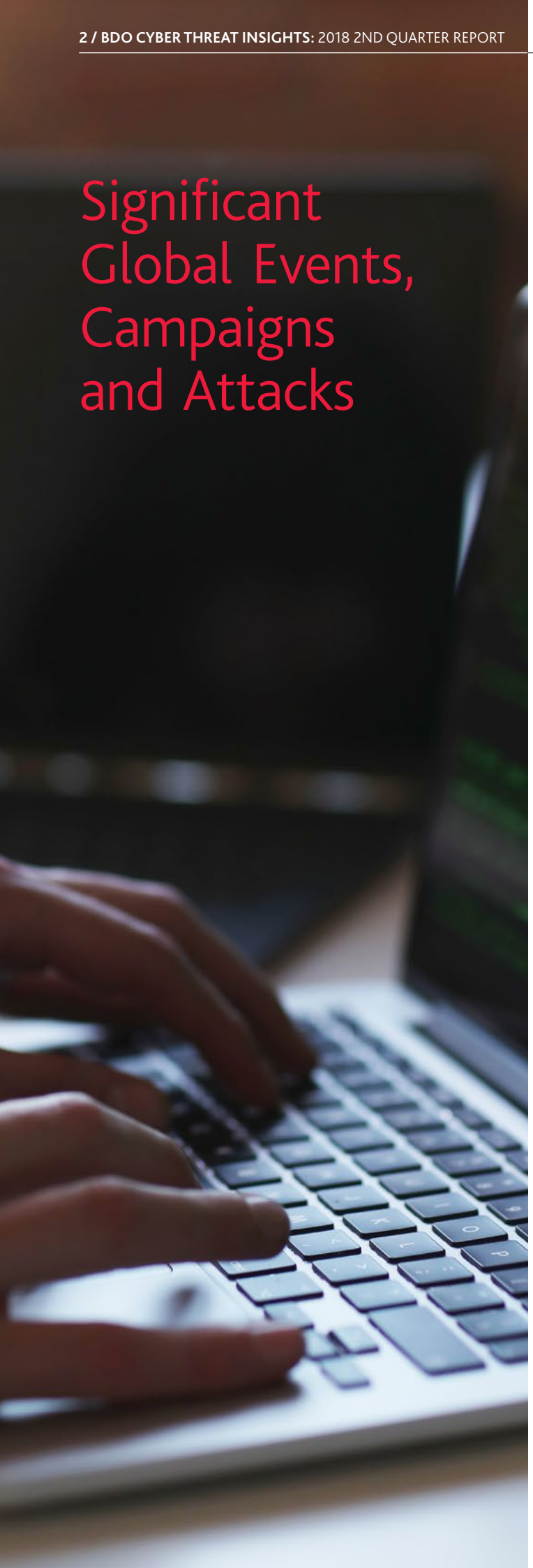
1. **Prepare for complexity:** Criminals are increasingly employing advanced evasive techniques, and more nation-state standard tools are being used for high profile cyber-attacks. This is likely to spread quickly through many industries and countries, raising the importance of monitoring and detection of your environment.
2. **Be ready for the unexpected:** Organizations must conduct more scenario planning to address unanticipated outcomes during an attack. This is a critical step in establishing cyber defense procedures to handle multi-vector attacks against several systems, either simultaneously or as part of an escalation. Reviewing the implementation of a 'kill-switch' for various systems in case of a large-scale and sophisticated, destructive attack is important to consider.
3. **Establish a resource plan:** Emergency scenarios are under-budgeted for by a factor of three. Many firms cannot or do not bring the appropriate skills and teams within an appropriate timeframe during an emergency; advanced planning for additional resources is highly recommended.

Best regards,
BDO Cyber Threat Insights Team

1 https://securityaffairs.co/wordpress/70675/cyber-crime/carbanak-gang-arrest.html

2 https://threatpost.com/despite-ringeaders-arrest-cobalt-group-still-active/132306/

Read more



Significant Global Events, Campaigns and Attacks

CHINESE APT15 STEALS MILITARY DOCUMENTS FROM U.K. GOVERNMENT CONTRACTOR

The Chinese-affiliated threat agent APT15 reportedly penetrated U.K. government contractor systems, effectively gaining access to highly sensitive military technology information, according to a report by NCC Group, published on March 10, 2018.[3]

The incident in question was discovered in May 2017, when a contractor providing a range of services to Britain's government suffered a network breach by the threat actor. NCC Group's analysis of the incident yielded that two new backdoors, dubbed RoyalCli and RoyalDNS, were used by the actor, as well as BS2005, a tool previously affiliated with APT15.

APT15 operated on the compromised network between May 2016 until late 2017 and affected over 30 hosts during that time. The initial point of entry into the network remains unclear; however, the attackers gained domain administrator credentials by using the open-source tool Mimikatz, which later facilitated the seizure of a VPN certificate that was used to access the victim's network remotely.

3 https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

Read more ▶

CHINESE APT TARGETS U.S. SATELLITE AND TELECOMS COMPANIES

A Chinese threat group has been targeting satellite, communications, geospatial imaging and defense organizations in the United States and Southeast Asia for espionage and/or destructive purposes, according to a Symantec report from June 19, 2018.[4]

The latest wave of attacks was carried out by the threat actor Thrip. The actor seemed focused on operations, deliberately infecting systems that run software to monitor and control satellites and geospatial imaging applications. This focus suggests a destructive motive. Other targets included three different telecom operators based in Southeast Asia and a defense contractor.

How are these attacks being carried out?

Thrip uses a wide range of tools and custom-made malware on its targets. However, the group is increasingly relying on "living off the land" tactics (the use of legitimate operating system features or network tools to compromise targets) and open-source tools. This renders the malicious activity more difficult to detect and attribute, as it blends in within larger legitimate processes.

In this particular attack campaign, the actor employed several tools and techniques:

- A previously unknown custom Trojan called Catchamas, an information stealer that contains additional features designed to avoid detection. [5] Catchamas is built to obtain various information from infected computers, including keystrokes, clipboard data, screenshots based on specified keywords in the window title and network adapter information.
- An updated variant of Rikamanu, a Trojan attributed to Thrip that logs keystrokes made on a compromised computer.[6]
- PsExec, a legitimate Microsoft Sysinternals tool for executing processes on other systems, which installed the malware and enabled lateral movement on the compromised networks.
- PowerShell, a Microsoft scripting tool used to run commands to download payloads, traverse compromised networks and carry out reconnaissance.

MASSIVE MYHERITAGE BREACH COMPROMISES ACCOUNT DETAILS OF 92 MILLION USERS

On June 4, 2018, the Israeli genealogy and DNA testing company MyHeritage announced that it experienced a data breach that compromised the account details of 92,283,889 users who had registered on its website on or before Oct. 26, 2017, the date the breach occurred.[7]

MyHeritage was alerted to the breach when an unidentified security researcher found a file named "myheritage" on a private server not related to the company. The file contained the email addresses and hashed passwords of more than 92 million users. After receiving the file from the researcher on June 4, 2018, the company's IT security team launched an investigation to determine what had occurred.

According to the company's statement, the security researcher reported that no other data related to MyHeritage was found on the private server. Furthermore, there was no evidence that the data in the file was ever used by the attackers. Since Oct. 26, 2017, the company has not detected any activity indicating that additional MyHeritage accounts have been compromised.

No payment details were compromised in this incident, as MyHeritage does not store this information on its servers. Other types of sensitive data, such as family trees and DNA data, is stored on separate systems from those storing user email addresses. MyHeritage said it has no reason to believe any other system was compromised. Upon learning about the incident, the company set up an Information Security Incident Response Team to investigate the incident and hired an external forensics firm.

MyHeritage is taking steps to inform the relevant authorities, including those pertaining to the EU's General Data Protection Regulation (GDPR). The company plans to implement a two-factor authentication (2FA) feature for user accounts in case the malicious actors manage to decrypt the hashed passwords. Meanwhile, MyHeritage is urging all registered users to change their account passwords.

4 https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

5 https://www.symantec.com/security-center/writeup/2018-040209-1742-99

6 https://www.symantec.com/en/sg/security-center/writeup/2015-072710-4212-99

7 https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/#

Read more ▶

WORLD'S LARGEST DDOS-AS-A-SERVICE WEBSITE TAKEN DOWN BY EUROPOL

In an operation dubbed "Operation Power Off," law enforcement agencies from around the globe seized and shut down the infrastructure of the world's largest DDoS-as-a-service website, webstresser[.]org.[8]

As of April 2018, Webstresser had 136,000 registered users who requested about four million attacks on various financial institutions and governments.

Once the domain of skilled and sophisticated attackers, disruptive DDoS attacks are now offered as a service by criminal actors, which effectively allows anyone with a vendetta or other motivation to launch such attacks on any chosen target. The services provide buyers with user-friendly interfaces that allow them to customize their attack according to categories such as duration, volume and method. In some cases, providers of DDoS-as-a-service demand ransoms from targets in exchange for calling off a planned attack. As opposed to traditional ransomware attacks, victims may be extorted prior to even losing any data.[9] Crimeware-as-a-service is a lucrative business and earns cybercriminals about U.S. $1.6 billion per year, with DDoS-as-a-service generating about U.S. $13 million of revenue per year.

MULTIPLE REX MUNDI CYBERCRIME GROUP MEMBERS ARRESTED BY EUROPOL

In a joint international operation between various law enforcement agencies, Europol has arrested 15 members of the hacker extortion group Rex Mundi over the past year. The latest arrests took place in early June, when a French national was apprehended in Thailand.

The group, whose name is Latin for "king of the world," has been publicly active since 2012. Their main modus operandi is hacking organizations, stealing sensitive data and demanding a ransom by threatening to publicly leak the data unless they are paid. The group demanded payment almost exclusively in Bitcoins.

The group's Pastebin post from 2015 reads: *"Rex Mundi is a collective of hackers. We hack for fun, for the thrills and, most importantly, for profit."*

The group made a name for themselves after successfully targeting large international companies and organizations including Domino's Pizza, Swiss bank Banque Cantonale de Geneve (BCGE), French loan company Credipret, Belgian payroll firm Easypay Group and French diagnostic laboratory Laboratoire de Biologie Médicale.[10]

The international operation, which was supported by the Joint Cybercrime Action Taskforce (J-CAT) [11], was launched following a major cyber-attack against an unnamed U.K. company in May 2017. [12] The group demanded U.S. $770,000 for not disclosing the stolen data, or U.S. $1.1 million for information on how the group compromised the firm's systems.

CRIMINALS LEVERAGE SPOOF WANNACRY PHISHING EMAILS TO EXTORT BITCOIN

On June 22, 2018, the National Fraud and Cyber Crime Reporting Centre in the U.K. reported [13] an attempt by cybercriminals to leverage the notoriety of the WannaCry Trojan to extort Bitcoins from victims.

In the span of two days, Action Fraud received almost 300 reports of phishing emails designed to dupe victims into believing that their computer was infected with WannaCry.

The phishing emails claimed to be from the "WannaCry-Hack-Team," using the misspelled subject line "Attantion WannaCry." The attackers claimed all of the victim's devices were hacked and threatened to encrypt and permanently delete files if a 0.1 Bitcoin (U.S. $650) payment wasn't received. Since the user's system was not ever infected, these were only empty threats. Despite the fact that WannaCry malware infects devices running on Windows OS, the fraudulent messages were received on all types of devices, including those running on iOS, macOS, Android, or Linux.[14]

8 https://www.infosecurity-magazine.com/news/major-take-down-of-site-selling/

9 https://www.itgovernance.co.uk/blog/ddos-as-a-service-providers-offer-customer-loyalty-programmes/

10 https://www.bankinfosecurity.com/rex-mundi-hacker-extortion-group-busted-a-11093

11 https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce

12 https://www.infosecurity-magazine.com/news/europol-disrupts-rex-mundi/

13 https://www.actionfraud.police.uk/news/fake-wannacry-emails-demanding-payment-jun18

14 https://www.scmagazine.com/fake-wannacry-sent-via-phishing-emails/article/776321/

Read more ▶

Notable or New Attack Tools, Techniques and Malware

RUSSIAN THREAT GROUP APT28 CHANGES TACTICS

On June 8, 2018, Palo Alto's Unit 42 released a report[15] analyzing the activity of Russian APT group Sofacy, also known as Fancy Bear and APT28, during the first half of 2018. As part of its regular monitoring of the threat actor, Unit 42 uncovered new "parallel" attack campaigns. In other words, the threat actor targeted similar types of victims with different types of toolsets. Most recently, the group was seen leveraging Zebrocy, a tool widely attributed to the group, as well as the Dynamic Data Exchange (DDE) exploit technique, which allows an attacker to execute code on a target system regardless of whether macros are enabled.

Zebrocy is delivered primarily via malicious Microsoft Office documents embedded with macros, or an executable attachment sent within phishing emails. In this latest campaign, the threat actor appeared to have slightly changed its tactics – instead of targeting a handful of victims within a single organization, APT28 targeted a wider set of victims across different geopolitical regions. The attackers sent phishing emails to a larger number of targets that did not follow any specific pattern; these email addresses could be easily found using online search engines.

APT28 also put its use of the DDE exploit technique to new use, leveraging it to deliver different types of payloads. For example, Unit 42 found one instance where the DDE exploit was used to deliver and install Zebrocy. In another instance, it was used to deliver an open-source penetration testing toolkit called Koadic, a tool that was not previously used by the threat actor.

CHINESE APT LEVERAGED USB DRIVES TO TARGET AIR-GAPPED SYSTEMS

Tick, sometimes referred to as Bronze Butler, is a threat actor that primarily targets organizations in South Korea and Japan. The group is likely based in China and has been active for several years. It primarily focuses on cyber espionage, targeting organizations that possess intellectual property or sensitive information, such as those in the defense sector and high tech industries.

According to a June 22 report by Palo Alto's Unit 42, [16] Tick succeeded in compromising a specific type of USB drive that was created by a South Korean defense company and was certified as secure by the South Korean IT Security Certification Center (ITSCC).

15 https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/

16 https://researchcenter.paloaltonetworks.com/2018/06/unit42-tick-group-weaponized-secure-usb-drives-target-air-gapped-critical-systems/

Read more ▶

SPECIAL FOCUS

Recent Cyber Events in the Healthcare Industry

This report provides an overview of healthcare cyber events and attacks during the first half of 2018. Following the trend of the last couple of years, most of the reported attacks are based on ransomware; either spear-targeted attacks or "scattershot attacks" (i.e. unfocused, and often generic attacks). The vast majority of malware attacks in the healthcare sector are delivered via file attachments or URLs that link the user to malicious code. In Q1 2018, malicious URLs were the preferred vehicle.

Malware is a concern that plagues numerous industry sectors. However, healthcare organizations have experienced a relatively large number of successful attacks in comparison to other sectors, such as the financial services industry, indicating that the sector's computer systems are systematically ill-protected.

This matter is further compounded by continual developments and adoption of artificial intelligence (AI) and IoT systems. According to International Data Corporation (IDC), AI investments were projected to reach U.S. $12.5 billion in 2017 alone. Still, it pales in comparison to IoT investments, which were expected to exceed U.S. $800 billion and are forecasted to reach U.S. $1.4 trillion in 2021. The number of connected medical devices is currently estimated at 10 billion, and is expected to reach 50 billion within the next 10 years, according to healthcare cybersecurity firm Cynerio.

The industry is currently in the early stages of re-evaluating operations with regards to new cyber threats and the integration of AI and IoT systems with life supporting technologies. It will be imperative to ensure new medical devices are well-deployed and operated properly, as any disruption, failure or security breach may result in loss of life. It will likely take several years for the healthcare industry to fully address this matter.

Read more ▶

"ORANGEWORM" THREAT GROUP LAUNCHES CAMPAIGN AGAINST HEALTHCARE SECTOR

A new threat actor known as Orangeworm has been deploying malware in a campaign targeting the healthcare sector and its supply chain in the United States, Europe and Asia, according to a report by Symantec from April 23, 2018.[17]

Orangeworm has been observed installing a custom-made backdoor called Trojan.Kwampirs across the healthcare sector, including pharmaceutical companies, IT solution providers for the healthcare industry and medical equipment manufacturers. The backdoor has been deployed on medical imaging devices such as X-ray and MRI machines, as well as machines used to assist patients in completing consent forms. The supply chain attack is designed to deliberately and meticulously reach chosen targets within the health sector, likely for espionage purposes.

Once deployed, Trojan.Kwampirs allows the attackers to remotely access the compromised host. After ensuring its persistence, the malware collects initial information on its victim to determine whether the target is of high-value. If the victim proves to be of interest to the threat actor, Kwampirs then collects additional network information to facilitate its propagation, which the malware carries out by copying itself over network shares. This method is suitable for older operating systems such as Windows XP, which are in prevalent use across the healthcare industry. Despite slightly modifying itself while moving across a network to evade detection, Orangeworm does not appear too concerned about being discovered and uses "aggressive" and "loud" methods to propagate the malware and communicate with C2 servers.

The origin of Orangeworm is currently unknown. The group is more likely an individual or a small number of individuals, as opposed to a nation-state actor. It appears to conduct well-planned strikes on its targets. According to Symantec, almost 40 percent of Orangeworm's confirmed victims operate within the healthcare industry, while attacks on other industries, such as manufacturing, information technology, agriculture and logistics, were also intended to reach targets in healthcare.

MEDICAL DEVICE RECALLS INCREASE BY 126% IN Q1, PREDOMINANTLY DUE TO SOFTWARE ISSUES

According to the Stericycle Recall Index, recalls of medical devices increased 126 percent in the first quarter of 2018, primarily due to software that is often run on vulnerable legacy systems.[18] This is the highest level of recalls since 2005. Software issues caused 22.7 percent of recalls, higher than any other cause.

To demonstrate the impact of compromised medical devices on patient care, researchers at the University of California - San Diego and the University of California - Davis studied breaches of various medical devices, including pacemakers, light scopes and insulin pumps. They simulated medical emergencies and provided the doctors in the experiment with the breached devices.

The hacked devices significantly hindered the ability of the physicians in the experiment to provide medical care. At the end of the test, the researchers asked the doctors whether they thought the devices were hacked; none of the doctors thought they were. The research team believes this indicates an implicit trust in medical infrastructure, as well as a lack of awareness at the inherit risk of using digital devices.

HEALTHEQUITY DATA BREACH COMPROMISES 23,000 INDIVIDUAL RECORDS

On June 13, 2018, HealthEquity, which manages millions of health savings accounts (HSAs), reported a data breach occurred in April, affecting 23,000 individuals.

According to reports, a HealthEquity employee's email account was unlawfully accessed, compromising clients' full names, their HealthEquity member IDs, as well as their employers' HealthEquity IDs. The stolen data also contained various types of healthcare accounts, payment records and Social Security numbers for some employees.

17 https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

18 http://www.healthcareitnews.com/news/when-medical-devices-get-hacked-hospitals-often-dont-know-it

Read more ▶

MASSIVE DATA BREACH AFFECTS AUSTRALIAN SOFTWARE PROVIDER PAGEUP

A multinational HR software provider in Australia, PageUp, announced that the personal data of thousands of its clients was potentially compromised. PageUp has roughly two million active users spread across 190 countries. It provides services to organizations across multiple sectors, including Australian institutions such as Telstra, NAB, Coles, Australia Post, Aldi and Medibank.

On May 23, 2018, PageUp detected "unusual activity," discovering that an unauthorized entity had accessed its system. [19] The company immediately launched an investigation to determine what had occurred. Five days later, PageUp found that client data may have been compromised in this event, including client names, street addresses, email addresses and telephone numbers. The company also said it believes certain data such as placement agencies, applicants, references and lists of employees was accessed. Resumes and financial details were not affected.

PageUp said it is confident that the incident has been successfully contained and the threat has been removed. Meanwhile, it is employing the services of third-party security teams and the Australian Cyber Security Center (ACSC) for assistance in its investigation. While speaking to reporters on June 6, 2018, the head of ACSC, Alastair MacGibbon, claimed that "malicious code" was executed inside PageUp's systems, although he did not provide any additional details on this matter.

As the investigation progresses, organizations using PageUp's services are notifying employees and customers about the incident.[20] Australia Post warned its employees that their personal information may have been compromised, and Telstra suspended the use of PageUp services while the investigations are ongoing. Medibank, a national private health insurer in Australia, likewise suspended its PageUp-powered recruitment site during the investigation process, and claimed that the amount of compromised data was greater than what was disclosed by the HR company. According to the health insurer, the compromised information may also include financial details, tax file numbers, diversity and health information, and emergency contact information.[21]

TWO DATA BREACH INCIDENTS HIT ARIZONA'S DIGNITY HEALTH GROUP

Dignity Health, a nonprofit healthcare corporation that operates medical facilities in three U.S. states, recently experienced two data security incidents impacting certain patient information.[22]

On June 2, 2018, Dignity Health's St. Joseph's Hospital and Medical Center in Phoenix, Arizona, announced it experienced a data security incident compromising 229 patient medical records. The records, which were accessed in an unauthorized manner by a hospital employee from October 13, 2017 through March 29, 2018, contained sensitive information, including patient names, dates of birth, and clinical data, such as nurses' or doctors' notes and diagnostic information. The compromised data did not include Social Security numbers, billing or credit card information. The hospital clarified that impacted patients did not need to take further action to protect themselves against identity theft.

On April 24, 2018, Dignity Health and its affiliates Dignity Health Medical Group Nevada, LLC, and Dignity Health Medical Foundation, discovered another issue. An email list formatted by Healthgrades, one of its business associates, contained a sorting error that resulted in Dignity Health inadvertently sending misaddressed emails to a group of 55,947 patients. The emails contained the wrong patient's name and, in some cases, his or her physician's name. No other information was included in the email. There was no financial, insurance or medical information included. Upon learning of the incident on April 25, 2018, Dignity Health and Healthgrades launched an investigation to determine what had occurred, and the companies said they are implementing appropriate measures to prevent a reoccurrence.

19 https://www.pageuppeople.com/unauthorised-activity-on-it-system/

20 https://www.bleepingcomputer.com/news/security/malware-infection-at-hr-company-triggers-flurry-of-data-breach-notifications/

21 https://careers.medibank.com.au/data-security-incident/

22 https://prod.cms.dignityhealth.org/arizona/locations/stjosephs/about-us/press-center/press-releases/2018-06-02-data-breach

Read more ▶

LIFEBRIDGE HEALTH BREACH EXPOSES DATA OF 500,000 PATIENTS

LifeBridge Health, a nonprofit healthcare corporation based in Baltimore, Maryland, experienced a security breach potentially impacting the personal information of over 500,000 patients.[23]

LifeBridge Health operates four hospitals in the greater Baltimore area. On March 18, 2018, LifeBridge Health detected malware on a server that hosts electronic medical records of Potomac Physicians, one of its physician practices, as well as on a shared registration and billing platform that is used by other LifeBridge Health providers. After the discovery, LifeBridge promptly launched an investigation into the incident and engaged the services of a forensic firm. The probe revealed that an unauthorized third-party gained access to the organization's network on September 27, 2016.

On May 16, 2018, LifeBridge Health issued a press release about the incident and said it was notifying all potentially affected patients. The organization did not disclose the type of malware found on its systems, or the nature of the 2016 breach. However, it said the incident compromised certain sensitive information, including patient names, addresses, dates of birth, diagnoses, medications, clinical and treatment information, insurance information, and in some instances, Social Security numbers.

LifeBridge Health and LifeBridge Potomac Professionals said they have no reason to believe that the patient information has been misused in any way, and established a dedicated call center to answer patient questions about the incident.

ALLIED PHYSICIANS OF MICHIANA HIT BY SAMSAM RANSOMWARE

On May 17, 2018, the Allied Physicians of Michiana in South Bend, Indiana, was hit by a variant of the SamSam ransomware, a prolific strain of malware known to target the healthcare sector. The practice immediately took steps to shut down the network and successfully restored its data in a secure format without causing significant disruption to patients or daily operations.[24]

The Allied Physicians practice did not disclose whether attackers demanded a ransom, or if any sum was ultimately paid. It simply stated that the incident was contained with the help of internal IT staff, its incident responder, outside assistance and other professionals. The company would not disclose any additional information.

SamSam is a ransomware strain that exploits vulnerable systems to gain access to a victim's network, or uses brute-force tactics against weak passwords of the Remote Desktop Protocol (RDP). Upon gaining access to a system, the malware holds the victim's data hostage using RSA-2048 encryption. It first appeared in 2016. The Bitcoin addresses associated with SamSam have received over $1 million in ransom payments just this year, making it a highly prolific ransomware strain.[25]

23 https://www.prnewswire.com/news-releases/lifebridge-health-and-lifebridge-potomac-professionals-notify-patients-of-a-recent-security-incident-300649922.html

24 https://www.apom.com/content/uploads/2018/05/FINAL_Allied-Physicians-News-Release_May-21-2018-C2-1-e1526932385481.jpg

25 https://healthitsecurity.com/news/samsam-ransomware-attacks-focus-on-victims-who-will-pay-up

Read more ▶

MISCONFIGURED FTP SERVER COMPROMISES DATA OF 205,000 PATIENTS

A misconfiguration of a public FTP server maintained by the Arkansas-based MedEvolve, a practice management software provider, exposed the protected information of 205,000 patients from two separate healthcare providers. While a number of clients had files on the FTP server, two had stored the medical files without password-protection.[26]

One of the clients, Premier Urgent Care in Pennsylvania, had an SQL database with 205,000 patient records that were not secured. Around 11,000 of those records contained Social Security numbers. The second client was Texas-based dermatologist Dr. Beverly Held, who compromised an estimated 12,000 Social Security numbers that were stored in three .dat files. On May 3, 2018, DataBreaches.net notified the two medical practices and MedEvolve, and the files were consequently removed that same day.

Responding to the questions of DataBreaches.net researchers, the President and CEO of MedEvolve, Matthew Rolfes, said:

"Our IT team, along with our healthcare lawyers, are aggressively investigating the situation. We have, and will take any necessary steps in order to mitigate any adverse effects to the extent within our control. We are also aware of HIPAA requirements applicable to Covered Entities and Business Associates in the event of a breach. Our company will comply accordingly. I know you will understand that we cannot, on the advice of counsel disclose to you all aspects of the investigation."

RANSOMWARE HITS ASSOCIATES IN PSYCHIATRY AND PSYCHOLOGY

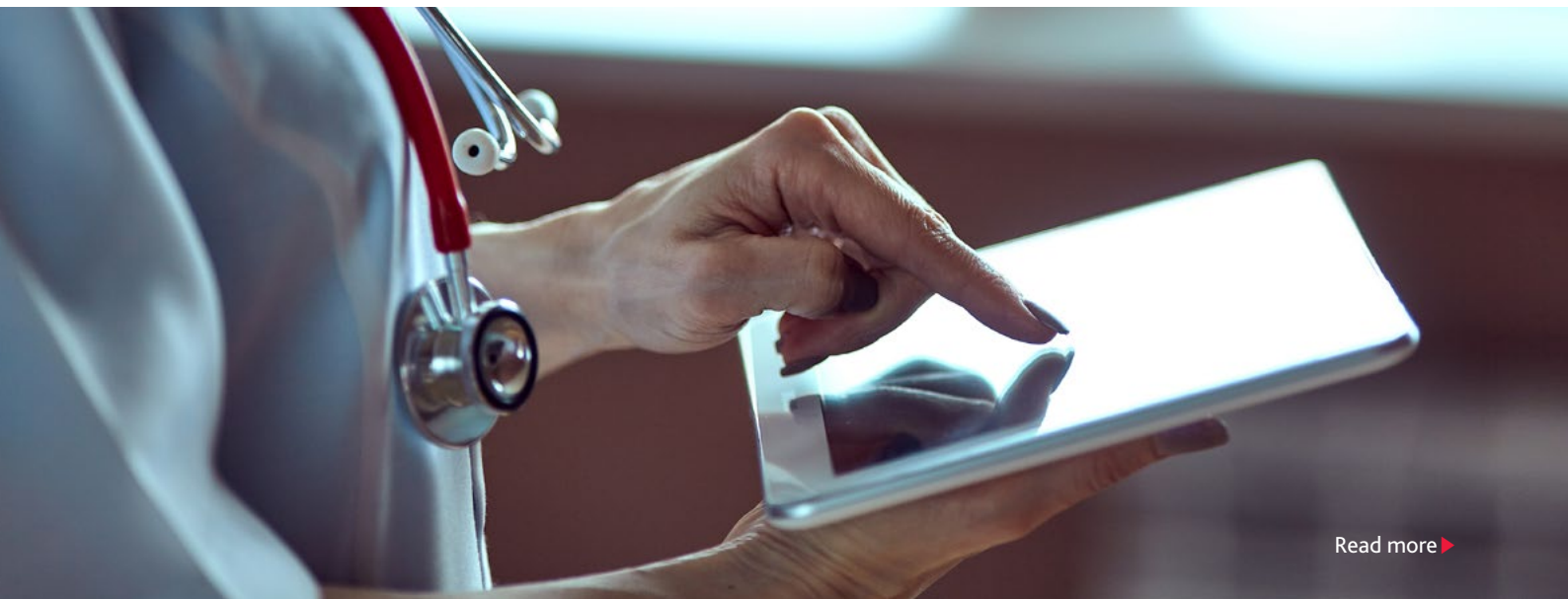
Between the evening of March 30 and the morning of March 31, 2018, threat actors breached the servers of Minnesota-based Associates in Psychiatry and Psychology (APP), encrypting all data files and disabling all system functions. The attackers demanded ransom in exchange for system restoration.[27]

The attackers, who are believed to be located in Eastern Europe, infected several of APP's computers with a TripleM ransomware variant that encrypted the files with an RSA-2048 encryption protocol. They also disabled the system restore function on all affected computers and reformatted the network storage device where the practice maintained its local backups.

After the discovery of the attack, APP's servers were taken offline for four days so that the practice could assess the situation. The attackers initially demanded four Bitcoin, but APP successfully negotiated the sum down to 0.5 Bitcoin, which was paid to the threat actors. The compromised server stored certain demographic information, such as insurance claim processing data and medical details. Credit card information was stored in a separate cloud-based bucket and was not part of the breach. APP said it had found no evidence that any patient information was accessed or copied.

26 https://www.databreaches.net/more-than-200000-patients-records-were-exposed-on-medevolves-public-ftp-server-researcher/

27 https://www.appmn.com/faq/



MISCONFIGURED S3 BUCKET EXPOSES PERSONAL AND MEDICAL DATA

AgentRun, a Chicago-based software startup that provides customer management software to independent insurance brokers, inadvertently compromised sensitive client information after it had stored files in a misconfigured Amazon S3 storage bucket.[28]

Compromised information included client data belonging to companies such as Cigna, Transamerica, SafeCo Insurance, Schneider Insurance, Manhattan Life and Everest, as well as the medical information of thousands of insurance policyholders. In addition, the breached bucket contained scans of customer identification documents such as Social Security cards and numbers, Medicare cards, driver's licenses, and armed forces and voter identification cards.

According to Andrew Lech, the company's founder, the permissions on the bucket were erroneously flipped during an application upgrade, leaving the bucket unprotected and accessible to anyone during the migration. The bucket was secured one hour after disclosure of the breach. The company said it is notifying all potentially impacted individuals and contacted the relevant authorities.

PHISHING ATTACK COMPROMISES MEDICAL DATA OF 42,600 AULTMAN HOSPITAL PATIENTS

Attackers used credentials gained from a phishing attack to access several email accounts belonging to Aultman Health Foundation, including its Ohio-based Aultman Hospital, its occupational medicine division AultWorks, and 25 of its physician practices.[29]

Aultman Health Foundation notified about 42,600 patients of a data breach potentially affecting their medical information after several employee email accounts were accessed by unauthorized individuals. The unknown attackers gained access to the accounts via a phishing attack that occurred earlier this year.

The breach was first detected on March 28, 2018, after which Aultman launched an investigation to determine how the incident occurred and what information was impacted. The probe revealed that access to the email accounts occurred on several occasions starting mid-February 2018 and continued until the breach was detected in late March 2018.

The system that stores electronic medical records was not compromised in this incident, as the breach was limited to the hacked email accounts. Compromised accounts belonging to Aultman Hospital and several practices contained various types of patient data, including names, addresses, clinical information, medical record numbers and names of physicians. The accounts belonging to AultWorks Occupational Medicine had a greater range of information exposed, including names, addresses, dates of birth, patient medical history, reports on physical examinations, results of drug, hearing, and breathing tests, and other lab test results.

Aultman Health Foundation reset and strengthened the passwords used across its practices after discovering it was hit by a phishing attack. Security protocols were hardened to prevent future incidents, and employees were provided with training on the detection of phishing attempts. Aultman Health Foundation said there have been no reports suggesting that compromised information was misused in any way. However, it's unclear whether any sensitive information was viewed or accessed. The Foundation advised patients to monitor their credit reports.

28 https://www.zdnet.com/article/insurance-startup-leaks-sensitive-customer-health-data/

29 https://www.healthdatamanagement.com/news/hackers-access-email-of-aultman-hospital-occupational-medicine-branch?brief=00000157-c311-d2b6-af57-cb9929c60000

Read more ▶

HEALTHCARE ORGANIZATIONS FAIL TO ADOPT DMARC STANDARD TO PREVENT IMPERSONATION

Despite the prevalence of email-based cyber-attacks across all industries, a recent study by mail authentication vendor Valimail found that the majority of healthcare organizations are not sufficiently protected against impersonation and phishing attacks.[30]

The Domain-based Message Authentication, Reporting and Conformance (DMARC) standard, an email-validation system that is designed to detect and prevent email spoofing and domain abuse, was rarely used in any capacity across the health sector, according to the report. Valimail discovered that 98.3 percent of the healthcare companies analyzed were susceptible to being impersonated by phishing attacks directed at employees, partners, patients or others.

DMARC is designed to fit into an organization's existing inbound email authentication process. When a DMARC record is created for a domain, the receiving server checks to determine whether the sender of the message is authorized to use the domain.

For the study, the vendor analyzed the domains of 928 healthcare companies around the world (with annual revenues of more than U.S. $300 million) including hospitals, medical equipment suppliers, pharmacies, physicians and health practitioners. Only 121 companies (13%) had adopted DMARC to secure their domains and prevent email spoofing.

These findings are concerning, considering that phishing emails are responsible for more than 91 percent of all cyber-attacks.[31] The majority of successful phishing attacks employ email impersonation techniques that can be more easily prevented by incorporating DMARC.

MEDICAL TRANSCRIPTION SERVICE SUFFERS BREACH AFFECTING 45,000 PATIENTS

Nuance Communications, a Massachusetts-based software company that provides medical transcription platforms to hospitals, experienced a security incident potentially affecting the medical records of 45,000 individuals.[32]

The compromise occurred from November 20 to December 9, 2017, when a former employee successfully breached Nuance's servers and accessed the personal information of thousands of individuals from several of the company's clients. After discovering the breach, Nuance Communications promptly shut down the affected platforms and notified law enforcement of the incident.

The company said it notified clients of the breach and moved them to an alternative platform while it resolved the issue. So far, the San Francisco Department of Public Health is the only one of Nuance's clients to notify impacted patients. The department sent letters to 895 individuals whose personal information was compromised; this information includes patient names, dates of birth, medical record numbers, patient numbers and medical information such as patient condition, assessment, diagnosis, treatment, care plan and date of service. Impacted patients visited the Zuckerberg General Hospital and Laguna Honda Hospital in San Francisco.

In a press release,[33] the Health Department said that it delayed notifying patients at the request of the FBI and Justice Department, which have been investigating the breach. The U.S. Department of Justice said the data had been recovered from the former employee and there was no evidence that the compromised information was used or sold.

30 http://www.healthcareitnews.com/news/despite-email-attacks-healthcare-still-not-using-dmarc-protect-against-spoofing

31 https://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704

32 https://www.bankinfosecurity.com/nuance-communications-breach-affected-45000-patients-a-11002

33 https://www.sfdph.org/dph/alerts/files/DPH_Release_notification_of_security_incident_5_11_18.pdf

Read more ▶

THE OREGON CLINIC NOTIFIES PATIENTS OF DATA SECURITY INCIDENT

The Oregon Clinic disclosed that on March 9, 2018, it learned that an unauthorized third party accessed an email account that contained certain protected health information.[34] [35]

The Oregon Clinic, a private specialty physician practice in Oregon, has been notifying patients about the company email account breach that may have compromised personal identifying information. A press release noted that the account was disabled immediately after the breach was discovered, but did not disclose the number of patients affected or the exact method used by the third-party to gain access to the account.

The clinic said it launched an investigation, using a digital forensics firm and other cybersecurity experts to determine what occurred. The investigation revealed that the exposed information included patient names, dates of birth, medical record numbers, diagnosis information, medical condition, diagnostic tests performed, prescription information and/or health insurance information. Social Security numbers may also have been affected for a small subset of patients.

The Oregon Clinic clarified that the breach was restricted to a single email account and did not affect any of the practice's infrastructure. The Oregon Clinic is providing impacted patients with information about how they can protect their personal information, along with 12 months of free credit and/or identity monitoring services.

34 http://www.oregonclinic.com/dataincident

35 https://www.healthdatamanagement.com/news/the-oregon-clinic-notifies-patients-after-data-breach

Read more ▶

MALWARE HITS THREE FLORIDA HOSPITAL WEBSITES

Malware was recently discovered on three websites belonging to Florida Hospital. The incident potentially compromised certain patient information to malicious actors. The hospital is notifying all impacted individuals.[36] [37]

In a statement released on May 2, 2018, Florida Hospital said the impacted websites - FloridaBariatric.com, FHOrthoInstitute.com and FHExecutiveHealth.com – potentially exposed patient names, email addresses, phone numbers, birthdates, height, weight, insurance carriers and the last four digits of individuals' Social Security numbers. No financial information was compromised and it did not affect
any other hospital infrastructure.

The hospital found no evidence that patient information was misused. All three websites were taken down while the malware was removed. It is unclear how long the malware was present on the hospital's websites and what type of malware was involved. Florida Hospital did not disclose the number of affected patients but clarified that it is implementing the appropriate measures to ensure similar breaches are prevented.

MEDICAL TRANSCRIPTION SERVICE COMPROMISES MEDICAL RECORDS

MEDantex, a Kansas-based medical transcription service, removed its web portal after it exposed thousands of patient medical records that were not password protected.[38]

KrebsOnSecurity, a security blog run by journalist Brian Krebs, notified the company on April 20, 2018, that the portion of its website reserved for physicians was completely accessible online. Visitors could add and delete user information and search for records by patient or physician name.

After being notified of the breach, MEDantex confirmed that it recently rebuilt its online servers after being hit by ransomware that was suspected to be a variant of WhiteRose malware.[39] According to the company's founder and chief executive Sreeram Pydah, the exposed pages were inadvertently incorporated into the rebuild after the attack.

The exact number of compromised documents remains unclear. In some cases, records date as far back as 2007, but the majority of them are recent. Among the clients receiving MEDantex services are New York University Medical Center, San Francisco Multi-Specialty Medical Group and Jackson Hospital in Montgomery, Alabama.

36 https://www.hipaajournal.com/malware-installed-on-florida-hospital-websites-may-have-provided-access-to-phi/

37 https://www.beckershospitalreview.com/cybersecurity/malware-attack-at-florida-hospital-may-have-compromised-patient-data.html

38 https://krebsonsecurity.com/2018/04/transcription-service-leaked-medical-records/

39 https://www.bleepingcomputer.com/news/security/the-whiterose-ransomware-is-decryptable-and-tells-a-strange-story/

Read more ▶

TEXAS HEALTH BREACH IMPACTS NEARLY 4,000 PATIENTS

On January 17, 2018, Texas Health Physicians Group was informed by law enforcement that an unauthorized third party may have gained access to a number of Texas Health email accounts in October 2017.[40]

The organization refrained from immediately contacting patients at the request of law enforcement, which was investigating the incident as part of a wider cyber event affecting multiple U.S. entities. Meanwhile, the organization launched its own internal investigation with the help of a forensic security firm. The investigation revealed that the affected email accounts may have included information such as patient names, medical record numbers, birth dates, addresses, Social Security and driver's license numbers, and insurance and medical information.

According to Texas Health, the breach affected around 3,808 patients that received treatment in 2017, but there are no indications that the exposed information has been misused in any way.

CALIFORNIA CENTER FOR ORTHOPEDIC SPECIALISTS HIT BY RANSOMWARE

The Center for Orthopedic Specialists (COS) in California announced that a ransomware attack affected three of its facilities across the state. The attackers succeeded in encrypting the medical records of 85,000 former and current patients that were stored on the system of a third-party IT vendor.[41]

The encrypted patient data potentially included patient names, birth dates, medical record information and Social Security numbers. COS clarified that all the information was taken offline before the threat actors could remove it from the system, but did not indicate whether it paid the demanded ransom or what strain of ransomware infected its systems.

The investigation with the affected IT vendor revealed that the attackers began attempts to access its systems on February 18, 2018. Consequently, the compromised system was permanently taken offline and all potentially affected patients were notified.

40 https://www.thpg.org/Pages/A-Notice-to-Our-Patients.aspx

41 http://www.cos-orthopaedics.com/web-notice/

BDO Cybersecurity Services

PAYMENT CARD INDUSTRY (PCI)

- PCI assessment and remediation
- Third-party assessments

INFORMATION GOVERNANCE AND DATA PRIVACY

- Data mapping
- Data privacy assessments
- Data privacy strategy and implementation
- Privacy officer consulting
- Information governance assessments

CYBER INSURANCE

- Cyber insurance claim preparation
- Coverage adequacy evaluation

INCIDENT RESPONSE

- Data breach investigations
- Network/host active threat monitoring
- Threat hunting - exec, enterprise, nation state, insider
- Threat intelligence - deep/dark web, social media analysis
- Training & testing - 1st responder, table top, RED team, simulations
- IR data analytics

CYBER RISK ASSESSMENTS

- Level 1- 3 risk assessments against multiple frameworks
- Cyber risk remediation

CYBERSECURITY STRATEGY, POLICY AND PROGRAM DESIGN

- CIO & CISO advisory services
- Cyber strategy consulting
- Regulatory compliance
- Government relations consulting

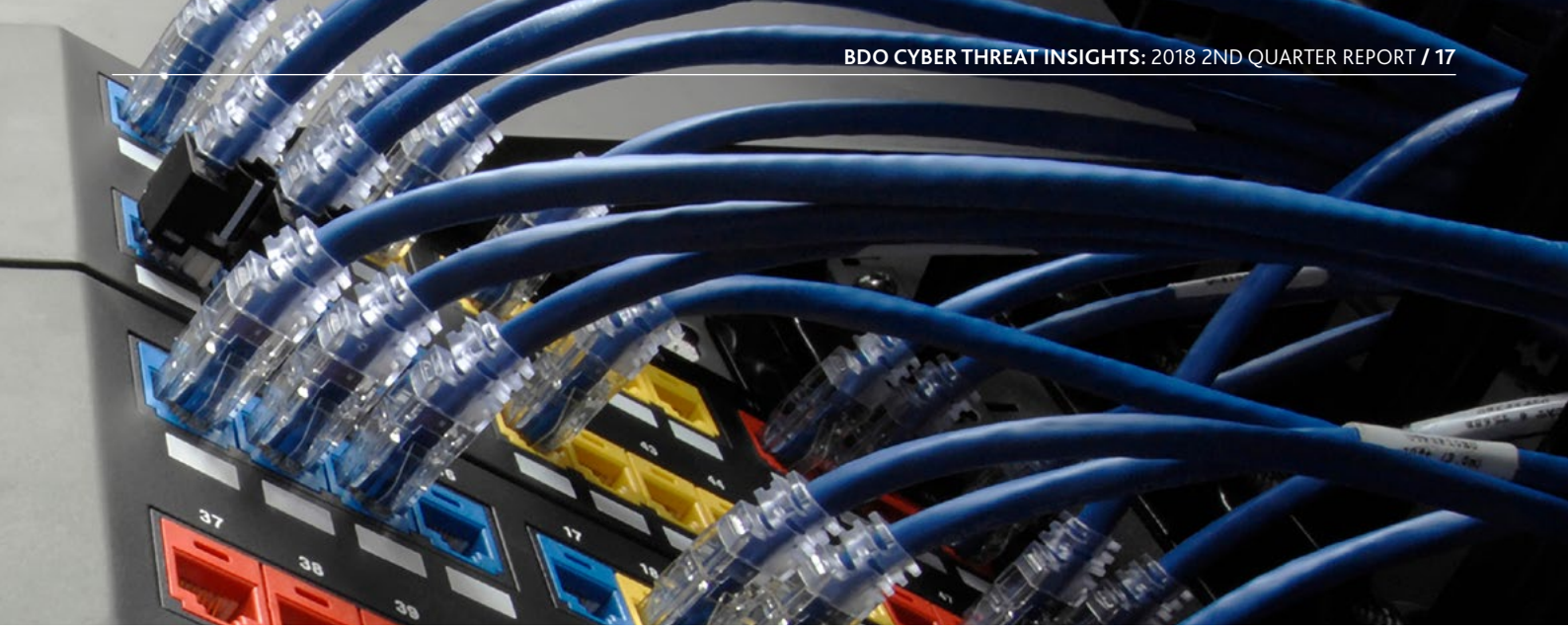
CYBER THREAT INTELLIGENCE

- Dark web recon
- Dark web analysis
- Social media

MANAGED SECURITY SERVICES

- Email and Network Attack Threat Assessments
- Security Operations Center (SOC)
- Penetration testing
- Vulnerability assessments
- Cloud migration & security
- Virtual desk-top services
- Cybersecurity education, training, & simulations
- Security Incident & Event Management (SIEM)

Read more ▶



Cybersecurity Leadership Team

GREGORY GARRETT
Head of U.S. & International Cybersecurity
Tel: +1 703-770-1019
ggarrett@bdo.com
Resident Country: USA

GRAHAM CROOCK
Director, IT Audit, Risk & Cyber Laboratory
Tel: +27826067570 or +27824654539
gcroock@bdo.co.za
Resident Country: South Africa

JASON GOTTSCHALK
Partner, Cybersecurity Practice Leader
Tel: +44 (0)79 7659 7979
jason.gottschalk@bdo.co.uk
Resident Country: UK

STEPHAN HALDER
Senior Manager, Forensic, Risk and Compliance
Tel: +49 40 30293 169
stephan.halder@bdo.de
Resident Country: Germany

LEON FOUCHE
Partner and National Cybersecurity Lead
Tel: +61 7 3237 5688
leon.fouche@bdo.com.au
Resident Country: Australia

SANDRA KONINGS
Partner, Cybersecurity Practice Leader
Tel: +31 (0) 6 5150 8151
sandra.konings@bdo.nl
Resident Country: Netherlands

ANDREAS VOGT, PH.D.
Partner, Head of Section BDO Security & Emergency Services
Tel: +47 48171714
andreas.vogt@bdo.no
Resident Country: Norway

OPHIR ZILBIGER, CISSP, CRISC
Partner, Head of Cybersecurity Centre
Tel: +972-52-6755544
OphirZ@bdo.co.il
Resident Country: Israel

Read more ▶

FOR MORE INFORMATION:

CYBERSECURITY.BDO.GLOBAL

Twitter:
@BDOglobal

Email:
Marketing@bdo.global

Editorial: BDO Cybersecurity Leadership Team

www.bdo.global

MKT0272