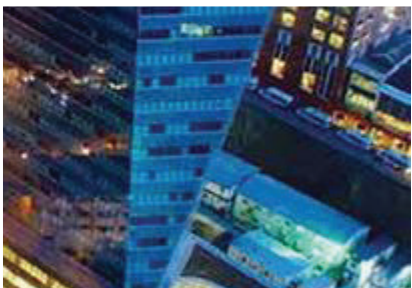
pwc.co.uk/cyber

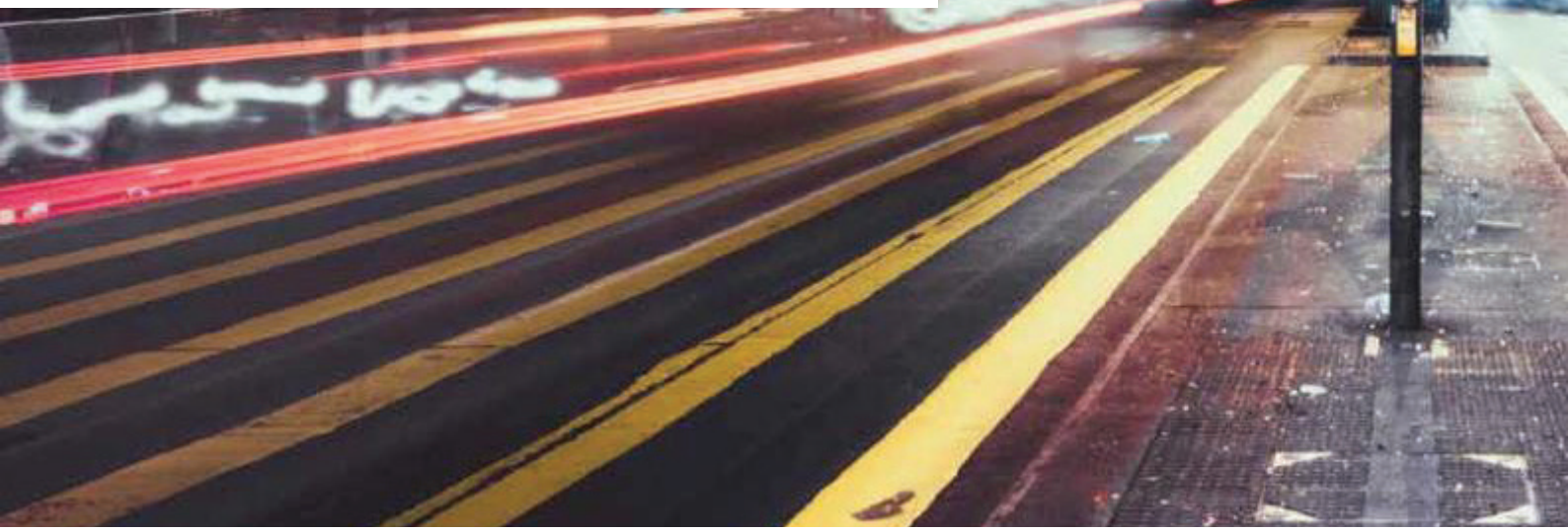
Under the Lens

Threats to the Healthcare Sector - Denmark



pwc

Contents



1 Introduction

Introduction

The healthcare industry, like many others, now operates in an ecosystem where it is heavily reliant on digital business process and technologies. Denmark in particular, is at the forefront of innovative primary healthcare. Its new digital health strategy[1] aims to create a citizen-centric coherent healthcare network. It focusses on both digitisation and better utilisation of health data collected. Whilst this new digital world provides a wealth of opportunities and benefits, it also increases the potential attack surface, leaving organisations open to cyber threats. It is therefore vital for healthcare organisations to not only develop a secure environment but to maintain visibility of the current threat landscape, and develop the means to detect and respond to cyber incidents so that any impact is minimised.

> "There has been a 65% increase in total financial losses for healthcare providers due to cybersecurity incidents."
>
> – The Global State of Information Security Survey 2018, PwC1

The networks of organisations across the healthcare sector have never held as much data as they do today; they harbour access to the personal and medical data of millions, designs for the latest medical technologies and a plethora of other data sources - each valuable in its own way to various threat actors. Given the nature of the sector, the compromise of data confidentiality, integrity or availability could have disastrous ramifications. Cyber security failure could mean devices rendered inoperable, critical patient records being stolen or unavailable, and even facilities being shut down as a precautionary measure.[2] The sector's position in both the supply chain and demand chain for other highly targeted adjacent sectors, such as biotech and life sciences, also heightens the overall risk. As the Danish healthcare market looks to expand its reach internationally, such compromises would likely undermine the initiative as a whole, and tarnish the reputation of associated public and private organisations.

The healthcare sector has been a popular target for espionage threat actors in recent years. Whilst threat actor motivations vary widely, the considerable information held by such organisations is a tempting target. This includes strategy and market data which could be used for corporate espionage; knowledge of specific processes and technologies to aid in the understanding and development of the sector in developing economies; and the theft of personal data by nation-state threat actors for intelligence purposes. In recent years, health insurers in particular have become the focus of several targeted espionage campaigns.

On the cyber crime front, threat actors have focussed on the theft of data, where the sale of medical records is particularly lucrative on the black market, with values often set at ten times higher than credit card information alone.[3] Such data is almost exclusively sold in bulk sets, consisting of thousands of individual records. Its value largely stems from the fact that there are many avenues through which it can be exploited, for example in blackmail, or to illicitly acquire medication which can then be resold. The sector has also been particularly vulnerable to ransomware attacks where, aside from the prevalence of insecure legacy systems, due to the criticality of the data stored, and concerns over patient safety, hospitals and critical health services are considered more likely than other organisations to pay ransoms.[4] The risk of this type of attack is increased where networks

1 'New Danish strategy for digital health 2018 – 2022', Healthcare Denmark, https://www.healthcaredenmark.dk/news/new-danish- strategy-for-digital-health-2018-%E2%80%93-2022.aspx (15th January 2018)

2 'Top health industry issues of 2018', PwC, 2018, https://www.pwc.com/us/en/health-industries/top-health-industry-issues.html

3 'Low risk; high reward – why hospitals are targets for cyber-attacks', CBR, https://www.cbronline.com/business/low-risk-high-reward- why-hospitals-are-targets-for-cyber-attacks-4997648/ (6th September 2016)

4 'Why Hospitals are the Perfect Targets for Ransomware', Wired, https://www.wired.com/2016/03/ransomware-why-hospitals-are-the- perfect-targets/ (30th March 2016)

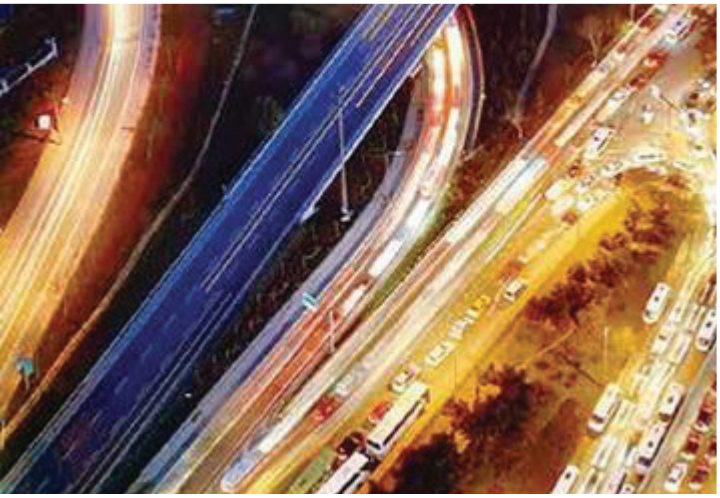
are increasingly shared. An example of this can be seen in the effect of the WannaCry attack on various NHS trusts, where the Eternal Blue vulnerability was leveraged to aid in the spreading of the malware.[5]

New technologies designed to enhance the customer experience, such as web-based services and mobile apps, are positively disrupting the way in which the healthcare sector is working. These include web portals, such as Denmark's e-health portal sundhed[.]dk, and mobile access to healthcare and health data. However, these types of services also broaden the threat landscape, providing new attack vectors for threat actors to exploit. Significant disruption to these services, or the underlying data, would heavily impact an organisation's ability to deliver reliable services. Furthermore, the growing pervasiveness of connected devices in the health sector, including telehealth solutions and medical equipment such as insulin pumps and heart monitors, is increasingly opening the sector up to the risk of sabotage attacks. This includes homecare initiatives to develop technological solutions supporting independence in the home. Such devices add to the growing number of devices forming part of the 'Internet of Things' (IoT). In addition to allowing potential sabotage actors to take remote control of these devices, security flaws within devices could also make healthcare facilities more vulnerable to attack by criminal groups by allowing lateral backdoor access to other networks.

This report aims to highlight some of the most common cyber threats currently facing the healthcare sector in Denmark in order to generate awareness and illustrate the motivations behind such attacks. This will aid organisations within the sector to identify and prevent targeted attacks. We also recommend a set of actions which can be taken to reduce the likelihood of a targeted attack being successful.

5 'SMB Exploited: WannaCry Use of "EternalBlue"', FireEye, https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html (26th May 2017)

2 Methodology



Methodology

Most cyber attacks have an underlying and ultimate motivation. Although attacks by separate threat actors might share objectives, separate threat actors do not always share the same motivation. Examining the motivation of an attack can enable the identification of the category of attacker.

PwC divides the threat landscape according to the motivation of those behind cyber-attacks. These divisions are as follows:

Attacker Category	Motivation	Description
Espionage	**For the nation**	Espionage attackers (often referred to as "Advanced Persistent Threats", or APTs) typically seek to steal information which will provide an economic or political advantage to their benefactor – who is often a nation sate. Usually, the information sought out by espionage attackers is only found at specific organisations, meaning they repeatedly target the same organisation and their suppliers until they have completed their mission.
Criminal	**For the money**	Cyber-criminals are indiscriminate in who they attack, they simply seek to monetise their attacks – and both individuals and organisations have money for the taking. Commonly, these attacks are realised through mass distribution of banking malware (for example ZeuS or Citadel) which surreptitiously steal credentials from users as they type them into their web browser. Some cyber-criminal threats are more focused, including targeted fraud aiming to steal credentials from specific high value individuals or companies. Another example of a more focused cyber-criminal threat is that posed by distributed denial of service (DDoS) attack ransoms, where criminals threaten to disrupt web services until payment is made.
Hacktivist	**For the cause**	Hacktivists conduct attacks to raise awareness of their cause. This is typically done through disruption of services or website defacements. In many cases such attacks can be random, as the attackers' only goal is to increase their visibility and public profile. They can care little how this is done or who is affected. In some cases, however, their targets are deliberately chosen, and the attacks relate to the perceived support of a political issue by an organisation. As with espionage, attacks from hacktivists are sometimes influenced by real world events, meaning the risk of such attacks is subject to change
Sabotage	**For the impact**	This category of attackers are tasked with either modifying or causing significant disruption to normal operations, and in some instances are likely to be state sponsored. Examples include wiping hard drives, causing SCADA systems to malfunction or altering trade data. As with espionage attacks, saboteurs tend to be influenced by real world events, making the risk of attacks specific to geography and company actions in relation to political events/issues.

Equally, we can attribute some typical objectives with each category of attacker. In some cases these objectives are dependent on the presence of certain datasets. For example, point-of-sale data is attractive to a criminal, but not as attractive to most hacktivists. We can therefore form an estimate of the likelihood of an attack from each category of threat actor against a given sector[6] based on common data held by that sector. Knowing which threat actors are relevant to a specific sector and organisation is an important step toward strategically directing investment in appropriate defences.

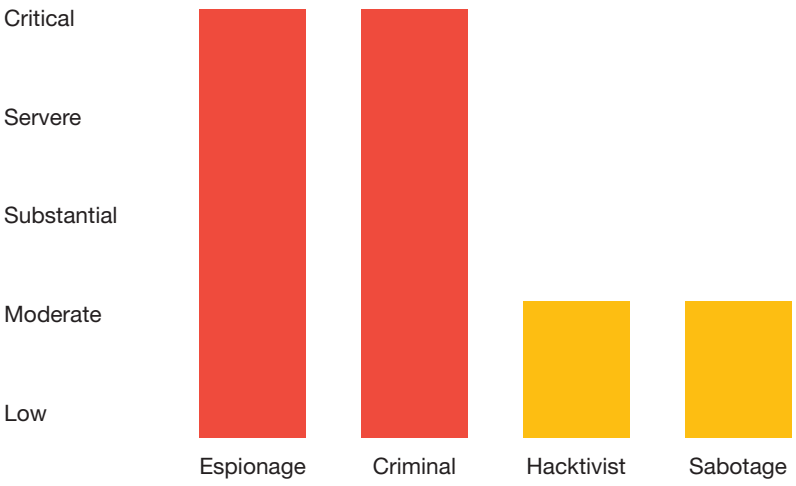
The overall view presented in this report spans an entire sector, and more granular analysis should be done on a per-organisation basis to inform security investment strategies.

When classifying the likelihood of attacks by specific categories of threats, we use the same threat level scale as the UK government:[7]

Threat level	Threat level description
Critical	An attack is imminent, or has occurred
Severe	An attack is highly likely
Substantial	An attack is a strong possibility
Moderate	An attack is possible, but not likely
Low	An attack is unlikely

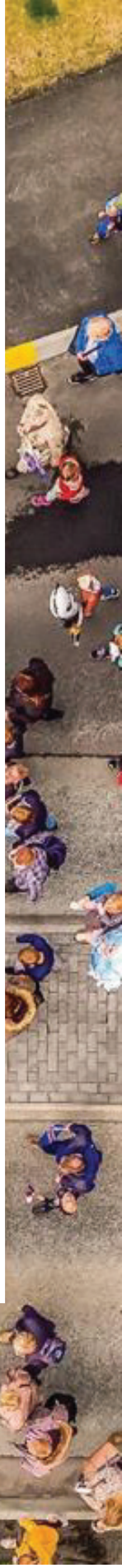
Our views are informed by our in-house intelligence datasets maintained on cyber-attacks and targeting from a variety of threat actors, intelligence gleaned from our incident response engagements around the world, as well as publically available information on attacks against the healthcare sector. The wide-ranging nature of the healthcare sector and the interests of the companies which operate within it means that this report will focus on the threat landscape of a number of key lines which are known to have been the target of malicious cyber activity and the types of actors which could have been behind this activity.

Based on past incidents, we believe that espionage and criminal activity poses the highest risk for the healthcare sector at present. Hacktivist and sabotage both represent a moderate risk at present.



6 Each organisation is different, however, and a number of factors such as political relationships and geographies operated in all play a part in determining the specific threat level to a given organisation.

7 'Terrorism and national emergencies', GOV.UK, https://www.gov.uk/terrorism-national-emergency



3

Threats on the Healthcare Stage

Espionage

Cyber attacks motivated by espionage usually originate from either industry competitors or state-sponsored attackers. The economic activities of some nations will always be of general interest to others where there is either an adversarial scenario or where there is a significant strategic interest in furthering their footprint in specific global markets. Developing economies, for example, may have a strategic interest in furthering their knowledge, technology or market share in a particular sector. As a result, the knowledge and working practices of large healthcare organisations are likely to be of interest to threat actors looking to develop expertise in specialised lines of business.

Attractive intelligence targets for espionage threat actors could include research and development (R&D) teams that are creating new models of healthcare through monitoring and analysing market developments, or identifying unmet consumer needs. Gaining insight into such strategy or market opportunities could provide industry peers with a competitive edge in the market. Similarly, technology innovation – whether through breakthroughs in patient care, diagnostics or in platforms supporting customer interaction – could also be an attractive target for espionage activity. In particular, the vast costs that can be associated with R&D in the healthcare sector means that some nation states will seek to gain inside information in order to cut their own costs and accelerate domestic advancement more swiftly. Denmark, as an innovator of both new technologies and systems in the healthcare sector, could be targeted for these reasons.

In the health insurance sector, China-based threat actors in particular have a prior history of targeting Western institutions.[8] This may in part be due to recent growth in China's domestic insurance market and its healthcare reform strategies which include the 'Healthy China' initiative. This includes objectives to enable improvements and technological advancements to the health insurance system.[9] The healthcare sector in China, including private hospitals, has also witnessed significant investment and is forecast to become a USD 1 trillion a year business by 2020.[10] President Xi Jinping has put health at the centre of the country's entire policy-making machinery, making the need to include health in all policies an official government policy. An example of this type of attack occurred in 2015 where the US health insurance company, Anthem was targeted by the China-based threat actor Deep Panda, which PwC tracks as Red Gargoyle. Further examples of China-based threat actor activity in this sector include Premera Blue Cross and CareFirst, US health insurance companies which also suffered data breaches in 2015.[11]

8 'ThreatConnect Enables "Healthy Networking" for the Biomed and Life Sciences Industry', Threat Connect, https://www.threatconnect.com/threatconnect-enables-healthy-networking-biomed-life-sciences-industry/ (5th May 2014)

9 'Healthy China', WHO, http://www.who.int/healthpromotion/conferences/9gchp/healthy-china/en/, 2016

10 'China's healthcare sector a big draw for private equity investors', South China Morning Post, http://www.scmp.com/business/article/2063273/chinas-healthcare-sector-big-draw-private-equity-investors (18th January 2017)

11 'Cyber security: Attack of the health hackers', Financial Times, https://www.ft.com/content/f3cbda3e-a027-11e5-8613-08e211ea5317 (21st December 2015)

Case study: Premera Blue Cross

Premera Blue Cross health insurance had its systems breached and 11 million applicants' and members' personal, financial and medical information stolen. Details including birthdates, ID numbers, bank accounts and clinical information were believed to have been compromised. The attack, which happened in May 2014 but was not discovered until January 2015, was reported to have been perpetrated by a China-based threat actor, Deep Panda.[1] The attack on Premera Blue Cross appeared to have occurred around the same time as the company's cyber security processes were audited by the Office of Personnel Management (OPM), whose final report highlighted concerns over patch implementation, unsupported software use and insecure server configuration.[2] Deep Panda was also linked to a subsequent data breach at OPM in 2015 which affected millions of people, exposing personal records and national security clearance status.3

1 'Premera Blue Cross Breach Exposes Financial, Medical Records', Krebs on Security, http://krebsonsecurity.com/2015/03/premera- blue-cross-breach-exposes-financial-medical-records/ (17th March 2015)

2 'Report No. I A-10-70-14-007, U.S. OFFICE OF PERSONNEL MANAGEMENT, November 2014, https://www.opm.gov/ourinspector-general/reports/2014/audit-of-inoformation-systems-general-and-application-controls-at-premera-blue-cross.pdf 3 'OPM Breach: Two Waves Of Attacks Likely Connected, Congressional Probe Concludes', Dark Reading, https://www.darkreading.com/endpoint/opm-breach-two-waves-of-attacks-likely-connected-congressional-probe-concludes/d/d- id/1326834 (7th September 2016)

Although the healthcare industry holds a large amount of sensitive data, the ultimate target of a threat actor may not be healthcare related. In recent times, threat actors have been found to adopt an 'island-hopping' approach by targeting varying systems and organisations to gain access to the networks of their affiliates. Attackers will often look for the weakest entry point through which they can target the intended victim. This is particularly relevant for Danish healthcare, where there exists a close network of third party relationships, and public-private partnerships are prevalent. A threat assessment from the Danish Centre for Cyber Security details one such incident occurring between 2014 and 2015, where a Danish company and its service provider were targeted by an unnamed nation-state threat actor. The malware used was able to record sound from computer microphones, create screen dumps and record keystrokes.[12]

Case study: Health South-East RHF[1]

In January 2018, the Norwegian healthcare service was breached by a suspected nation-state APT. The attack was reportedly focussed on patient data and in particular, information pertaining to 'Trident Juncture 18', a NATO exercise scheduled to take place in Norway later in October 2018. The attack put the data of up to 2.8 million people, more than half of Norway's population, at risk.

1 'Norway healthcare cyber-attack could be biggest of its kind', Digital Health, https://www.digitalhealth.net/2018/01/norway-healthcare-cyber-attack-could-be-biggest/ (24th January 2018)

Espionage attacks against healthcare organisations could be categorised in three broad areas:

- **Sensitive data theft** – A primary focus of espionage attacks is the theft of intellectual property and sensitive business data. In contrast to the focus of data stolen by financially focused cyber criminals, data stolen in espionage attacks can often only be monetised by another organisation in the same sector. Examples of assets likely to be targeted include market strategies and data, proprietary technology, patient data including PII (personally identifiable information) and PHI (protected health information) records, and medical research e.g. epidemiological research related to the Danish National Biobank.

12 'The cyber threat against Denmark', Centre for Cyber Security, https://fe-ddis.dk/cfcs/CFCSDocuments/Threat%20Assessment%20-%20The%20cyber%20threat%20against%20Denmark.pdf (January 2016)

- **Event driven attacks** – Some attackers with an espionage focus specialise in short-term intelligence collection requirements. This is typically the case when a real-world event results in a need to gather intelligence. The most common examples of this relate to significant investments, where having inside knowledge of the position or strategy of another party provides a substantial advantage. Access to voicemail and conference call systems is often of particular interest to attackers in this space, providing almost real-time insight into thought processes and planning. Our Threat Intelligence practice has observed case studies of espionage activities with the goal of gaining an advantage over the negotiation table.
- **Knowledge** – Our Threat Intelligence practice has observed several instances where the purpose of an espionage attack is not necessarily to obtain sensitive business data, but to simply understand how high- performing organisations work in order to be able to replicate the model locally, or to gain understanding of critical infrastructure supporting services in order to design attacks to cripple the infrastructure in the event of a conflict.

Espionage attacks can be conducted in a variety of ways. Some threat actors break perimeter systems directly and navigate inwards from there. Others prefer to spear phish individuals, establishing a foothold on user systems and moving laterally until they find the data they want. Watering hole attacks are increasingly prevalent in narrow verticals, since it is possible to identify popular websites for that vertical which, once compromised, can be used to target a wide variety of organisations in it.

At a minimum, we believe the following threat actors have previously, or are currently, targeting the healthcare sector:

APT18

APT 18, also known as Dynamite Panda, which PwC tracks as Red Wraith, is a highly advanced China-based threat actor best known for compromising the security firm RSA before proceeding to compromise more than 700 organisations.[13] In what is now known to be one of the most sophisticated supply chain attacks, the reason for targeting the RSA was to steal the security tokens used for its SecurID products.[14] Armed with those security tokens, the threat actor then proceeded on to targeting specific organisations who used SecurID to secure access to their IT environments. This threat actor remains active and was one of several groups to rapidly repurpose zero-day exploits disclosed in the breach of Italian company Hacking Team.

Red Wraith has consistently run large-scale campaigns against the healthcare and pharmaceutical industries since 2014, when it was linked to the theft of medical and personal data from the US healthcare network, Community Health Systems.

APT19

APT19 or Deep Panda, which PwC tracks as Red Gargoyle, is a China-based threat actor known to have been active since as early as 2012. It has targeted a wide range of sectors including government, universities, defence industrial bases, technology and healthcare. This threat actor has demonstrated a preference to use malware families such as Derusbi and Sakula as well as digital certificates such as DTOPTOOLZ to sign its binaries in an effort to evade security detection mechanisms. It is based on this preference that APT19 has also been associated with the high profile breaches at Anthem, Carefirst and Premera Blue Cross as well as the OPM breach which collectively results in the loss of over 100 million personal records.[15] It also makes extensive use of web shells and has displayed a high level of technical sophistication and is persistent in its attempts to breach targets.

13 'RSA attackers hit over 700 other firms', v3, https://www.v3.co.uk/v3-uk/blog-post/2119598/700-firms-attacked-rsa-security-hackers (24th October 2011)

14 RSA breach leaks data for hacking SecurID tokens, The Register, http://www.theregister.co.uk/2011/03/18/rsa_breach_leaks_securid_data/ (18th March 2011)

15 'OPM vs. APT: How Proper Implementation of Key Controls Could Have Prevented a Disaster', SANS Institute, https://www.sans.org/reading-room/whitepapers/breaches/opm-vs-apt-proper-implementation-key-controls-prevented-disaster-36852 (10th March 2016)

APT37

Also known as Reaper, PwC tracks this threat actor as Black Shoggoth. This threat actor is based in North Korea and is thought to have been active since 2012. It is known to have targeted organisations across several sectors including governments, aerospace, manufacturing, automotive, electronics, chemical and healthcare, with a regional focus on Asia and the Middle East. It has been known to utilise third party infrastructure, including messaging platforms, cloud services and compromised servers as part of its command and control infrastructure.

Criminal

Crimes committed through 'cyber' means often have the same outcome as their equivalent attacks committed through physical means. However, the cyber element of such crimes allows the threat actor to operate with far lower risk, higher reward and a variable modus operandi. Whilst the transition from physical to cyber crime has been well-documented in terms of sensitive data and financial theft, there are also some organised cyber crime groups using techniques which cross both the physical and cyber domains.[16]

Organisations with a prevalence of legacy systems, as is the case with many healthcare institutions, are particularly vulnerable to attack. In 2018, for example, PwC investigated an incident in the sector where poorly managed infrastructure, in use at a national level, had been exploited for several years by a number of different threat actors running automated vulnerability scans. This could have potentially serious implications if access to critical systems were to be disrupted.

Health-related data is a particularly popular target for financially motivated threat actors, with personal identity information (PII), protected health information (PHI) and financial data all easily monetisable. It can also be utilised by criminals to defraud victims in a number of ways and many holders of such data have a traditionally low level of security counter-measures in place. The data can be used to directly target customers to obtain further sensitive information, where stolen information such as a name and membership ID could be used to falsely establish a threat actor as a representative from the insurer or agency. This type of fraud could be performed over a number of channels, e.g. phone, email or post, and be used to trick victims into redirecting payments. Of particular note, the data of high-profile customers, such as high net worth individuals (HNWIs) may be sought after and could be used to blackmail victims with the threat of exposure of sensitive medical details.

Although some of this information may be openly available through other channels, it is important to note that the completeness of this data as a whole and detailed dataset makes it much more valuable. Employee data, which includes a wealth of sensitive data including PII, may also be exploited in a similar fashion.

Case Study: Cyber crime – Medicare Australia patient data for sale[1]

A darkweb trader was exposed for selling Australian Government Medicare details. The threat actor was reportedly able to access the patient details of any Australian citizen on request by exploiting an undisclosed vulnerability in a government system. The threat actor boasted that it had sold more than 75 records since October 2016, where individual records were valued at 0.0089 bitcoins (equivalent to approximately USD 6 at the time).

1 'The Medicare machine: patient details of 'any Australian' for sale on darknet, Guardian, 'https://www.theguardian.com/australia- news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet (3rd July 2017)

One popular attack vector used by cyber criminals is phishing emails. It is common for phishing emails to contain a malicious link which will take the user to a cloned website and then ask for credentials to be entered in order to 'log in'. Other conduits for similar attacks include SMS or fake apps available on legitimate app stores. In particular, cyber criminal attacks can be facilitated by using stolen or compromised credentials. In the case of healthcare organisations, this could comprise attempts to clone portal login webpages, for example.

16 'Francophoned – A Sophisticated Social Engineering Attack', Symantec, http://www.symantec.com/connect/blogs/francophoned-sophisticated-social-engineering-attack (28th August 2013)

A growing number of mobile health apps have also been shown to be vulnerable where sensitive data could be extracted and exploited. A study by application security firm Arxan[17] found that 84% of FDA and 80% of NHS approved apps contained at least two OWASP top ten mobile vulnerabilities and the majority did not have binary code protection, meaning that they can be easily reverse-engineered or modified. Similarly, a report into the security and privacy behind the twenty of the most popular and freely available m-Health apps found that the majority tested did not follow best practices and guidelines, with some not meeting legal restrictions on data handling. The apps tested were found to put user data at risk by disclosing potentially sensitive data to third parties including PHI, location data, photos, emails and passwords. There was also a lack of encryption used in the transmission of sensitive data.[18]

Case study: Under Armour Inc. – MyFitnessPal app[1]

Data from approximately 150 million MyFitnessPal diet and fitness app accounts was compromised in February 2018. The app is owned by Under Armour Inc. and used by customers to monitor calorie intake and exercise regimes. The data stolen included user names, email address, and scrambled passwords, and customers were warned to change their passwords as a result of the breach. Financial and personal data including payment data and social security numbers were not reported to be compromised. Shares of Under Armour Inc. subsequently went down by 3%.

1 'Under Armour says 150 million MyFitnessPal accounts breached', Reuters, https://www.theguardian.com/technology/2018/mar/30/hackers-steal-data-150m-myfitnesspal-app-users-under-armour (30th March 2018)

Threats from cyber crime are not limited to opportunistic actors who strive for high volume and low impact fraud. Ongoing threat intelligence collected by PwC suggests that many cyber criminals are increasingly seeking to adapt their techniques to more closely align with those used by prominent espionage threat actors. These techniques include the targeting of important staff members with well-crafted spear phishing emails, as well as the technical ability to establish persistence and move laterally through victim networks. This comes at an increased cost in terms of time to criminals, meaning that attacks using these techniques are often lower in volume but higher in impact.

Cyber crime attacks against the healthcare sector are likely to fall into the following areas:

- **Personal data** – Medical and other personal data (including billing, payment and insurance information) held by healthcare institutions is likely to be of interest to criminals seeking fresh data to exploit. This data on individuals or families could be targeted by a criminal organisation seeking PII with a view to performing insurance fraud or to gain access to prescription medication and medical devices for resale. The data can also be sold and used to defraud victims of assets through other channels (e.g. banking). The records are specifically targeted from this sector due to the traditionally low level of security counter-measures in place. With the digitisation of more and more sensitive data and added elements of cloud computing and storage, connected devices and m-Health apps, the associated risks and countermeasures should be carefully evaluated.

- **Ransomware** – Attacks using ransomware are becoming increasingly aggressive and popular particularly in the healthcare sector. Ransomware is a type of malware that encrypts a computer's files. Victims are then shown instructions for how to pay the ransom in order to get the decryption key. Ransom demands can range from a few hundred to hundreds of thousands of dollars. The most active ransomware families to date include Cryptowall, a family of file-encrypting ransomware that first appeared in 2014, CryptXXX which encrypts files on all attached data storage after the machine has been infected, Locky,

17 'Dozens of mobile health apps found vulnerable to security risks', Graham Cluley, https://www.grahamcluley.com/dozens-mobile-health- apps-vulnerable-security-risks/, (13th January 2016)

18 'Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice', ACHILLEAS PAPAGEORGIOU et al, IEEE Access, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8272037 (29th January 2018)

more recent strain of ransomware known to target hospitals in the US, Japan and South Korea, and Samas, which has been used to target servers in healthcare environments. The majority of ransomware is primarily distributed through spam messages that try to trick victims into opening attachments and, once executed, the malware encrypts personal files (such as images, documents and videos) on fixed, removable and network drives. These type of attacks are often sent over a wide target range spanning across multiple industries. Given the sensitivity and value of the data stored by healthcare providers and medical institutions, there is an ongoing threat against the sector.

CryptoLocker ransomware has been used to successfully infect the East and North Hertfordshire NHS trust twice. Although the ransom was not paid in this case, it is possible sensitive information could also have been stolen.[19] In such cases, there is also a danger of interruptions to medical appointments or procedures. This strain of ransomware - largely obsolete since 2014 - was typically spread using social engineering techniques for example through infected email attachments which often appeared official, important and/or urgent. When run, the malicious file would then act to encrypt the user's files unless the ransom was paid within a specified time limit.[20] In 2015, phishing emails purporting to be from Post Denmark and PostNord were used to lure Danish targets into downloading this strain of ransomware.[21]

In 2016, Locky is known to have affected US hospitals including Kentucky Methodist Hospital, Chino Valley Medical Center and Desert Valley Hospital, California. Although services were temporarily interrupted, no ransom was reported to have been paid as systems were restored from backups.[22] In the case of Hollywood Presbyterian Medical Center, which was targeted in February 2016, Locky caused significant disruption taking systems relating to the emergency rooms, labs, CT scans and documentation offline. An amount of USD 17,000 was paid in Bitcoins to restore access.[23]

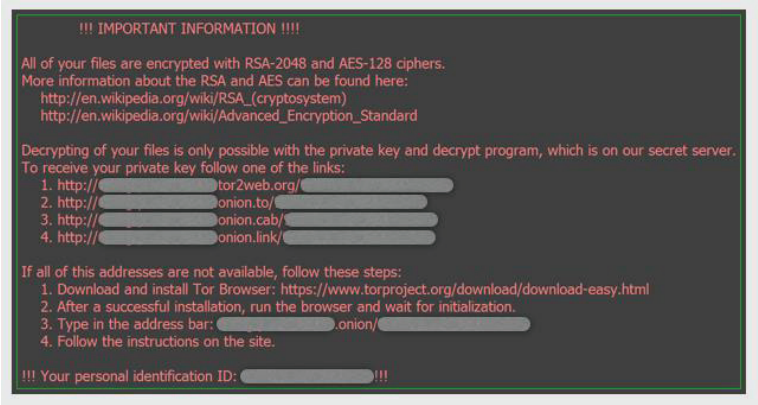


Figure 1: Locky ransom instructions

Samas or Samsam is a ransomware which has been used by a threat actor which bypasses traditional social engineering techniques, instead targeting vulnerable web servers and other perimeter systems. The threat actor has been seen to specifically exploit JBoss application servers. Once compromised, the threat actor strategically deploys the ransomware onto an organisation's network, in many cases targeting highly valuable systems such as file servers.[24] The US-based MedStar Health organisation was thought to

19 'UK hospitals targeted by ransomware but NHS did not pay up', IBT, http://www.ibtimes.co.uk/uk-hospitals-targeted-by-ransomware- nhs-did-not-pay-1578832# (31st August 2016)

20 'CryptoLocker: What Is and How to Avoid it', Panda Security, http://www.pandasecurity.com/mediacenter/malware/cryptolocker/ (14th May 2015)

21 'Post Office Email Scams Target Denmark, Drop Crypt0l0cker Ransomware', Tripwire, https://www.tripwire.com/state-of- security/security-data-protection/cyber-security/post-office-email-scams-target-denmark-drop-crypt0l0cker-ransomware/ (29th September 2015)

22 'Three US hospitals hit by ransomware', BBC, http://www.bbc.co.uk/news/technology-35880610 (23rd March 2016)

23 'Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating', LA Times, http://www.latimes.com/business/technology/la- me-ln-hollywood-hospital-bitcoin-20160217-story.html (18th February 2016)

24 'Samas ransomware enters hospitals through vulnerable servers', HelpNetSecurity, https://www.helpnetsecurity.com/2016/03/31/samas-ransomware-enters-hospitals/ (31st March 2016)

be attacked by the threat actor behind Samas in 2016, where several hospitals on the network were compromised. In 2018, US hospital Hancock Health paid 4 bitcoins, equivalent to approximately USD 55 000, as part of a Samas ransomware attack. The ransom was paid to gain access to a decryption key and restore access to key IT systems.[25]

- Targeted fraud - PwC has observed a significant increase over the past 18 months in targeted fraud cases where criminals send legitimate-looking emails imitating a real persona known to the target. In such attacks, also known as business email compromise (BEC) fraud, the attacker would ask the victim to make bank transfers to accounts under the attacker's control. In one incident of such targeted fraud we have investigated, the total financial loss was in the scale of millions. Unfortunately, this figure is dwarfed by the statistics published by the FBI which shows that global businesses lost a total of USD 12 billion to BEC fraud between 2013 and 2018, with an increase of 136% between December 2016 and May 2018.[26] In 2018, PwC investigated BEC incidents where the fraud losses have totalled more than USD 20 million.

- Back office information or credentials – A significant proportion of opportunistic attacks are conducted with the objective of obtaining access to privileged systems from which credentials or access can be exploited to achieve the end goal - access to cash. This may be as straightforward as seeking the CFO's credentials to approve wire transfers, or it may be more sophisticated, such as obtaining business continuity plans to be able to convince the business telecommunications provider to temporarily redirect the corporate lines in order to intercept a call from the corporate banking provider to authorise a fraudulent transaction.

Case study: WannaCry

WannaCry is believed to have affected over 200,000 systems in at least 150 countries, making it one of the most prevalent ransomware campaigns ever reported. It affected victims across a wide range of different sectors and geographies, via unpatched remote code execution vulnerabilities in the Microsoft Windows implementation of the server message block (SMB) protocol.

Microsoft released a patch for this vulnerability in itsMS17-010 security update in March 2017, suggesting that WannaCry victims either did not have a sufficiently timely patch programme in place, or were running unsupported legacy systems for which a patch was not initially released (e.g.Windows XP, Windows Server 2003). Indeed, once the scale of the campaign became apparent, Microsoft took the unusual step of releasing a patch for unsupported systems.[1] Disrupted organisations included a number of NHS trusts, with at least 6,900 NHS appointments cancelled as a result of the attack.

1 'Customer Guidance for Wanna Crypt attacks', Microsoft TechNet, https://blogs.technet.microsoft.com/msrc/2017/05/12/customerguidance-for-wannacrypt- attacks/ (12th May 2017)

2 'NHS 'could have prevented' WannaCry ransomware attack', BBC News, http://www.bbc.co.uk/news/technology-41753022 (27th October 2017)

At a minimum, we believe the following threat actor has previously, or is currently, targeting the healthcare sector:

25 'US hospital pays $55,000 to hackers after ransomware attack', ZDNet, https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/ (17th January 2018)

26 'BEC Scam Losses Top $12 Billion: FBI', Security Week, https://www.securityweek.com/bec-scam-losses-top-12-billion-fbi (16th July 2018)

FIN4

Like many organisations, it is often the most senior individuals who have access to the most sensitive data. Throughout 2013, and 2014, PwC closely followed the activity of the threat actor known as FIN4, or White Chrysaor, which is a good example of this.

Background
FIN4 was a financially motivated espionage threat actor with a focus on obtaining insider information which could be used to inform its trading positions on specific stocks.

Operational since as early as mid-2013, this threat actor delivered carefully crafted spear phishing lures to senior executives and other individuals likely to be privy to deal or results information in more than 100 organisations, with a particular focus on the pharmaceutical and healthcare sectors.

FIN4 was either based in an English-speaking country, or employed English-speaking individuals with a robust knowledge of deal and investment environments. Its objective was to obtain email account authentication credentials for people of interest, and to use that access to extract sensitive data, such as drug trial results, major procurement and M&A deals. In many cases, the threat actor targeted organisations for inside information on a deal long before the deal activity was publicly known, suggesting it may have already had privileged access to information.

It would be plausible for FIN4 to have been a legitimate fund, or a shadow fund, effectively an organised crime fund holding positions in legitimate funds and using inside information to underpin its investment strategy and front run market movements in specific stocks.

Targeting
FIN4's typical modus operandi was to exploit illegitimate access to corporate email accounts using legitimate, phished credentials. These were obtained via Word or Excel documents with an embedded macro which displayed a dialogue asking the user for credentials, such as the one below, which was indistinguishable from the legitimate Outlook Web App logon dialog. The Word/Excel documents were relevant to the individual and company being targeted, and were likely to have been stolen from other networks.

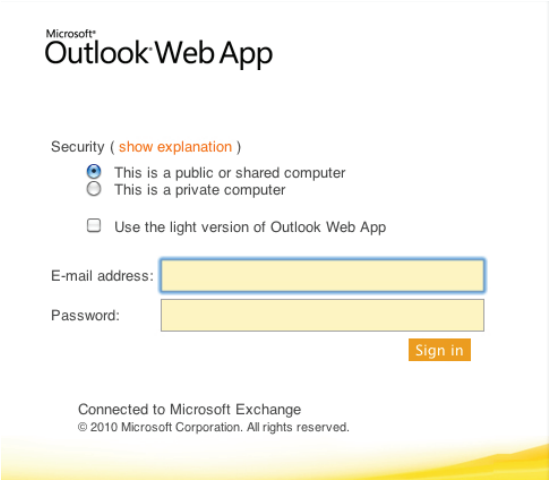


Figure 2: Example dialogue used to phish for login credentials

In many instances, this phishing dialog was tailored to include the legitimate logo of the organisation being targeted. Once it had access to accounts of interest, FIN4's main method of persistence, other than directly accessing mail accounts, which it did via the TOR anonymisation network, demonstrating robust awareness of operational security, was to create an auto-forward rule for specific mailboxes to external email addresses under its control. This technique is something we still observe from many BEC and cybercrime actors.

In addition, FIN4 often sought to broaden its access to other individuals and organisations of interest, by exploiting trust between individuals and injecting itself into existing email threads.

Hacktivist

The targets selected by hacktivists are often selected seemingly at random as the attackers are frequently seeking any avenue through which to gain additional notoriety.

When targets are deliberately selected this usually happens for one of the following reasons:

- The target's website (see below an example of a defaced website) or social media feed attracts a large number of visitors and so defacing it would yield a great deal of coverage of the hacktivists' cause; or

- The target is perceived to support a cause with which the hacktivists disagree. In this case the attackers will seek to harm the target in any way, but typically through defacement of their website or through stealing and then divulging confidential data taken from the target.

Figure 3: Example of a defaced website[27]

Given the relatively limited web presence and low profile of many healthcare organisations, the likelihood of an attack motivated by the first category of threat actors is relatively minimal. However, it is highly likely that the sector will periodically catch the attention of individuals or groups who disagree with a particular method or corporate decision as per the second category described above. This could include medical research facilities with links to controversial lines of research, for example the use of animal testing. For health insurers and hospitals, the risk of an attack will increase where there is media coverage of negative news stories concerning the organisation. This is particularly the case where members of the general public are perceived to have 'lost out' to large corporations or government entities. High-profile coverage of denied insurance claims or malpractice would be pertinent examples of this.

The focus of attacks could include social media account hijacking and website defacements. Whilst mostly superficial in nature, such attacks can impact the reputation of the organisation, where customers subsequently become concerned over the safety of their personal data. More disruptive activities could take the form of denial of service attacks (DoS) rendering data and services unavailable. E-health portals such as Denmark's new sundhed[.]dk service, could be a vulnerable target for such attacks.[28] Given the nature of the sector, a prolonged attack of this kind would cause significant disruption and could indirectly impact patient care. Furthermore, the increase in the use of medical devices forming part of the IoT increases the potential attack surface. In 2014, Boston Children's Hospital website and internet access was taken offline by hacker group Anonymous. The

27 'NHS website defaced by hackers', BBC, https://www.bbc.co.uk/news/technology-43812539 (18th April 2018)

28 'Danish e-health portal sets a new record with high visitor numbers' Healthcare Denmark, http://www.healthcaredenmark.dk/news/danish-e-health-portal-sets-a-new-record-with-high-visitor-numbers.aspx (12th February 2018)

distributed denial of service (DDoS) attack was performed in response to the controversial child custody case with which the hospital was involved.[29]

Case Study: Anonymous defaces AXA Insurance Group website[1]

As part of its #OpGabon campaign, the threat actor known as Anonymous defaced AXA's Gabon website with a message and YouTube video. Anonymous claimed it targeted AXA for its perceived support of the Gabonese President, Ali Bongo. To increase the profile of the attack, it was also promoted by the threat actor on Twitter.[2]

1 '#OpGabon: Anonymous hacks, defaces Axa Insurance Group website against its support for Ali Bongo', HackRead, https://www.hackread.com/opgabon-anonymous-hacks-axa-insurance-group// (25th August 2013)

2 'Anonymous Hackers Hacks and deface AXA, Insurance company website, under #opgabon', TechWorm, https://www.techworm.net/2013/08/anonymous-hackers-hacks-and-deface-axa.html (26th August 2013)

The large amount of sensitive data held by the healthcare sector, including PII and PHI, also makes it a target for data disclosure. In this type of attack, a threat actor would obtain sensitive data, such as business emails or customer databases, and subsequently leak these in the public domain. A high profile example for the sector is the leak of confidential medical data from the World Anti-Doping Agency (WADA) in September 2016. Though attributed to the Russia-based hacking group, APT[28] (informally, the 'fancy bears'), whose activities would normally be considered as an espionage-type threat, the motivation here appears to be retaliation for the independent Pound and McLaren investigations which thoroughly documented a state-sponsored doping programme.[30]

At a minimum, we believe the following threat actor has previously been, or is currently, targeting the healthcare sector.

Grey Ares

Grey Ares (a.k.a. Anonymous) is a hacktivist threat actor who first emerged on an internet forum called 4Chan. It gained global attention through a series of high profile attacks during the WikiLeaks saga. However, due to the ethos of being "anonymous", there have been many unofficial Anonymous factions emerging from different parts of the world, all of which conduct cyber attacks in the name of the Anonymous group. Due to the lack of a distinctive modus operandi, it is difficult to assess the true nature of Anonymous, making this threat actor particularly difficult to track.

Overall, Anonymous consists of a small core of skilled hackers insulated by a large community of low-skilled members. The threat actor's modus operandi usually involves DDoS campaigns and web defacement. There have been past incidents in which it has demonstrated the ability to compromise organisations, such as the HBGary, Stratfor and George K. Baum breaches and the lesser known email compromise of military law firm Puckett & Faraj who represented a US marine court-martialled for an incident in Iraq. It is also worth noting that Anonymous has previously attacked law firm websites and individual lawyers as part of the Operation Payback movement, which protested copyright laws and the prevention of information sharing online.

29 'Anonymous Allegedly Hacked Boston Children's Hospital Over Justina Pelletier', Slate, http://www.slate.com/blogs/future_tense/2014/04/24/anonymous_allegedly_hacked_boston_children_s_hospital_over_justina_pelleti er.html (24th April 2014)

30 PwC Global Cyber Bulletin, 12-26 September 2016

31 Further PwC analysis on Grey Ares is available to Threat Intelligence customers.

Sabotage

Threat actors with the goal of sabotaging businesses and organisations are not uncommon and occasionally appear on the threat radar. This category of cyber threat can be motivated by political, economic or religious ideologies, as well as more formal tasking by nation states. Destructive cyber attacks targeting organisations initially came to prominence in 2011 when the Stuxnet malware was first identified and then linked to targeted attacks on Iranian nuclear plants.[32] Similar attacks have occurred only sporadically since then, with notable instances targeting Saudi Aramco in 2012,[33] South Korean financial services in 2013,[34] and Sony Pictures in 2014.[35]

While the healthcare sector is unlikely to fall victim to an attack on this scale, the vulnerability of connected medical devices provides a possible avenue of attack for both end-users and healthcare institutions. A report by the Royal Academy of Engineering into digitally connected systems highlighted connected health devices as being a particular area of concern.[36] These systems include implantable devices such as pacemakers and drug administrators, and larger hospital equipment such as MRI scanners and X-ray machines. Potential vulnerabilities, inconsistent and out-of-date regulations, and a lack of awareness regarding supply chain risks were identified as some of the main challenges surrounding the use of such devices. Although no direct attacks have been recorded to date, the following examples show that if the motivation exists, the consequences could be fatal.

At the Black Hat 2018 security conference, researchers demonstrated vulnerabilities in a range of medical devices manufactured by Medtronic, which could potentially result in life-threatening scenarios. These included remotely disabling an implantable insulin pump to prevent it from delivering medication. They also demonstrated the control of a pacemaker system where commands could be delivered to either issue or deny a shock.[37]

In August 2018, McAfee researchers described how they manipulated communications between commonly used hospital equipment – a patient monitor device and a central monitoring station. If exploited in a real-life scenario, this could be used to manipulate patient vitals for insidious purposes.[38]

In October 2016, Johnson & Johnson revealed that there were security vulnerabilities in its insulin pumps which could be exploited to alter dosage to its users. In this case a hacker could spoof communications, which are unencrypted, between the wireless remote used to control dosage and the pump itself. This could be used to cause deliberate over dosage which is potentially life threatening.[39]

Similarly, in 2014, Hospira's Symbiq infusion pump, a 'smart pump' used to automate the delivery of drugs and fluids to a patient, was also found to be vulnerable to manipulation. Other examples of vulnerabilities found

32 'Stuxnet attack forced Britain to rethink the cyber war', The Guardian, http://www.theguardian.com/politics/2011/may/30/stuxnet-attack-cyber-war-iran (30th May 2011)

33 'The inside story of the biggest hack in history', CNN, https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html (5th August 2015)

34 'Wiper Malware Threat Analysis', Secureworks, https://www.secureworks.com/research/wiper-malware-analysis-attacking-korean-financial-sector (21st March 2013)

35 'Analysis of wiper malware, implicated in Sony breach, exposes Shamoon-style attacks, SC Magazine, https://www.scmagazine.com/home/news/analysis-of-wiper-malware-implicated-in-sony-breach-exposes-shamoon-style-attacks/ (4th December 2014)

36 'Cyber saftety and resilience', Royal Academy of Engineering, https://www.raeng.org.uk/publications/reports/cyber-safety-and-resilience, March 2018

37 'Hackable implanted medical devices could cause deaths, researchers say', The Guardian, https://www.theguardian.com/technology/2018/aug/09/implanted-medical-devices-hacking-risks-medtronic (9th August 2018)

38 '80 to 0 in Under 5 Seconds: Falsifying a Medical Patient's Vitals', McAfee, https://securingtomorrow.mcafee.com/mcafee-labs/80-to-0- in-under-5-seconds-falsifying-a-medical-patients-vitals/ (11th August 2018)

39 'J&J warns diabetic patients: Insulin pump vulnerable to hacking', Reuters, http://uk.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUKKCN12411L (4th October 2016)

through research on specific medical devices include the Medtronic insulin pump which could be manipulated to provide lethal doses, and the hacking of a pacemaker to deliver dangerous shocks.[40]

Two reports by TrapX[41] highlight the extent to which vulnerabilities in connected medical devices could be exploited where it was shown that an attacker could gain access to an entire hospital network. One of the problems stems from running outdated operating systems which have known insecurities and therefore easily infected by malware. Furthermore medical devices are mostly serviced and maintained by manufacturer's meaning that end users are unable to run periodic security diagnostics. In the case studies highlighted by the report, though attackers could manipulate the entry devices and gain access to critical hospital systems, there is no evidence of this behaviour as yet; instead the motivation appears to be directed towards obtaining medical records and password credentials.

In recent times, several attacks have been carried out by suspected nation-state threat actors as 'distractions' to cover the ultimate purpose of the attack. The July 2017 NotPetya campaign is one example of this. Initially believed to be ransomware, it was later assessed to have been spread for the purposes of sabotage and intelligence collection. The fallout from this attack affected a number of companies on a global scale, resulting in over USD
10 billion in financial impact.[42] The affected organisations included Merck, one of the world's largest pharmaceutical companies, with the incident costing the firm more than USD 300 million in Q3 2017 alone.[43] As part of the same attack, Danish shipping and logistics firm, Maersk, was forced to perform a complete infrastructure overhaul, reinstalling 4000 servers, 45000 PCs and 2500 applications. It is estimated it list up to USD 300 million due to "serious business interruption".[44]

There are currently no specific threat actors known to be targeting the healthcare sector with the motivation of sabotage. However, given the rise in the number of medical devices joining the Internet of Things, and the current vulnerabilities seen, this is an area for which security will become an increasing concern and should not therefore be ignored.

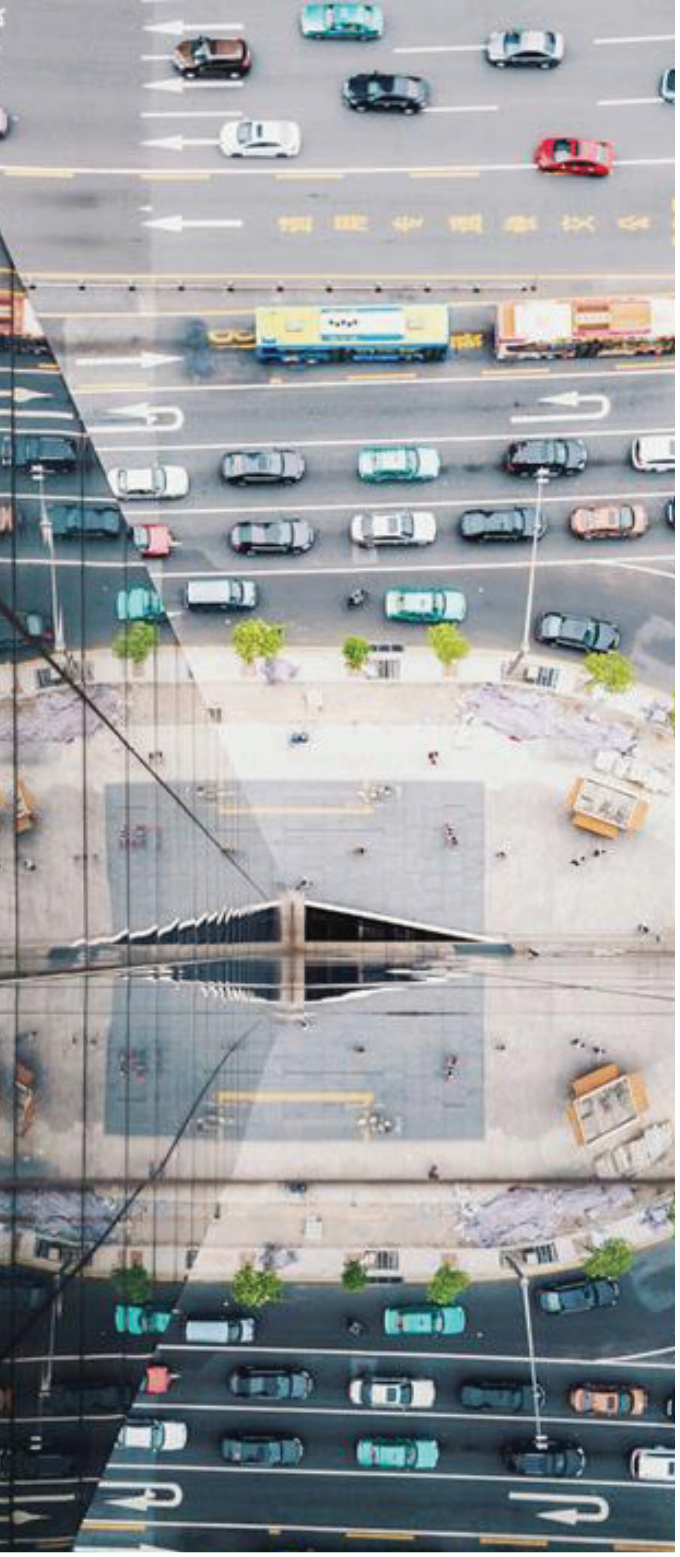
40 'It's Way Too Easy to Hack the Hospital', Bloomberg, http://www.bloomberg.com/features/2015-hospital-hack/ (November 2015)

41 'TRAPX LABS DISCOVERS NEW MEDICAL HIJACK ATTACKS TARGETING HOSPITAL DEVICES', TrapX, https://trapx.com/trapx-labs-discovers-new-medical-hijack-attacks-targeting-hospital-devices-2/ (27th June 2016)

42 'The untold story of NotPetya, the most devastating cyberattack in history', Wired, https://www.wired.com/story/notpetya-cyberattack- ukraine-russia-code-crashed-the-world/ (22nd August 2018)

43 'NotPetya ransomware outbreak cost Merck more than $300M per quarter', TechRepublic, https://www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/ (30th October 2017)

44 'NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs', ZDNet, https://www.zdnet.com/article/maersk-forced-to- reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/ (26th January 2018)



5

PwC Cyber Security

PwC Denmark – local presence with global expertise

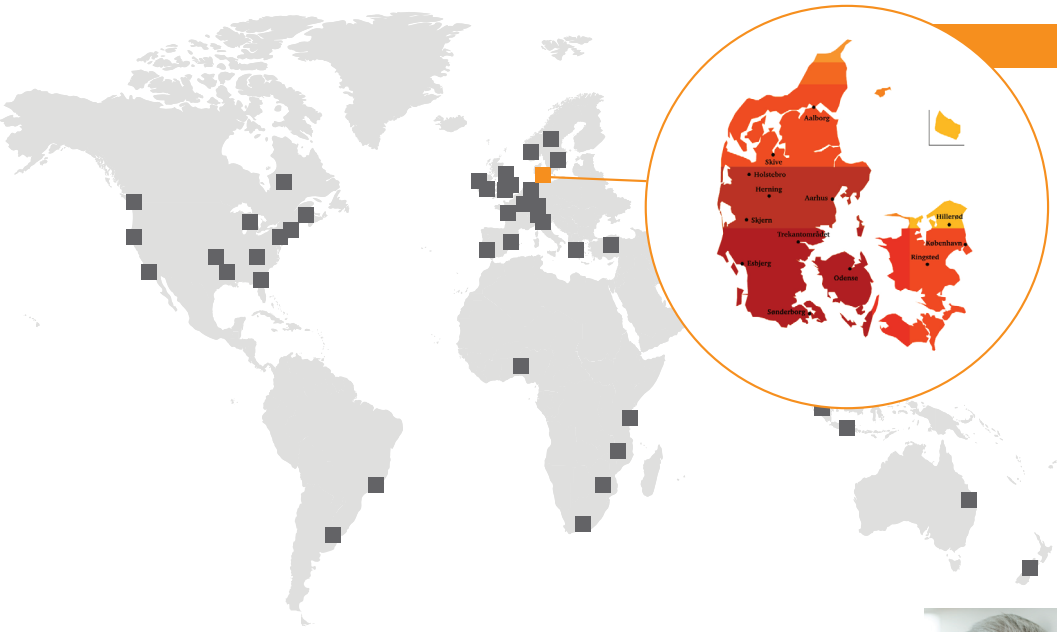
“Informing and enabling strategies for agile and dynamic defence, directed by intelligence, which address real-world, relevant threats.”

PwC is globally recognised by industry analysts as a leader in cyber security and as a firm with strong global delivery capabilities and the ability to address the security and risk challenges our clients face.
We underpin our board-level security strategy and advisory consulting services with expertise gleaned from the front lines of cyber defence across our niche technical expertise in services such as red teaming, incident response and threat intelligence.

We differentiate ourselves with our ability to combine strategic thinking, strong technical capabilities and complex engagement delivery with client service excellence. Our core focus is delivering pragmatic services to our clients, helping them handle some of their most sensitive business issues.

We bring together a team of specialists with expertise in security management, threat detection and monitoring, threat intelligence, security architecture and consulting, behavioural change and regulatory and legal advice, to help our clients protect what matters most to them.

Our rapidly growing threat intelligence team has been described by the Financial Times as one of “the world’s most elite corporate teams of cyber defenders”. We specialise in providing the services required to help clients resist, detect and respond to advanced cyber-attacks. This includes crisis events such as data breaches, economic espionage and targeted intrusions, including those commonly referred to as APTs.



GDPR | Cyper

Danish service desk
T: +45 7022 2444

Security excellence centers in Aarhus and Copenhagen

- 120 dedicated security consultants
- Legal experts
- Forensic investigation experts
- Infrastructure consultants
- Other practice areas: Strategy and Organisation, Digital Transformation, Financial Effectiveness, People and Change

PwC Denmark connects to global knowledge centres.

3,200 security consultants. Partnerships with industry-leading security companies

Mads Nørgaard Madsen
Head of Security & Technology (DK)
T: +45 2811 1592

Jørgen Sørensen
Head of Security (DK)
T: +45 2494 5254