mimecast

The Cyber Threat to UK and RoI Healthcare

This paper is intended to be a high-level, horizon-scanning discussion on the potential threats that could be realised from technology developments, world events, or societal change across the Healthcare and Pharmaceutical sectors.

It is intended to stimulate thought and is a forecast assessment based on analysis of current information and intelligence products.

mimecast

The Cyber Threat to UK and RoI Healthcare

Discussion paper – July 2020

Introduction

National Cyber Security Centre (NCSC) advisories and open source media reporting have identified that APT groups and cybercriminals are targeting individuals, small and medium businesses, and large organisations, including those in the healthcare sector, with ***COVID-19*** related scams and phishing emails.[1]

With the healthcare sector recently having seen a dramatic increase in its reliance on the internet, from connectivity with patients, interconnectivity of an abundance of technical medical / health devices passing confidential date, to provisioning its IT backbone, the ever-expanding threat vector and plethora of research, personal, and confidential data is the key reason it is the subject of cyberattacks.

The evolution of cyber technologies, and the increased drive to mobility and digital transformations, has facilitated threats from cyber threat actors who use these same enablers to gain access to target networks (to identify weaknesses in the architecture, infrastructure, or defences), exfiltrate personally identifiable information (PII) and exploit any potential vulnerabilities. These actors then use these findings to improve their attack methodologies. Healthcare organisations, in addition to sensitive medical information, retain information on insurance and financial information.

But with both healthcare providers and biotechnology / pharmaceutical companies rising in prominence over the last few months owing to their key roles in fighting the ***COVID-19*** battle, why, despite the humanitarian capacity of their roles, are they being targeted by nefarious entities?

Background

Through its fundamental role in supporting a nation, healthcare is considered part of a nation's critical national infrastructure. With such importance alongside water, electricity supply & distribution, and transport networks, the sector becomes an attractive target for those entities intent on causing disruption, chaos, and exploiting times of confusion and uncertainty. By denying services or the efficiency of the healthcare sector, a hostile state actor can be seen as subverting a nation through undermining the healthcare aperture and degrading efficiency, reputation, and trust. There is also a possibility that in attacking a healthcare organisation that is part of a wider network of infrastructure, it may be possible to pivot to other critical facilities.

With many pharmaceutical companies around the globe striving to develop cures and vaccines for ***COVID-19***, an increased reliance on artificial intelligence (AI) within this industry, and the protection of patient, intellectual, and proprietary data. AI has a credible record within medicine.[1] Advances in AI and machine learning technology have dramatically reduced the timeframes necessary to develop, test, and produce medication. The previously labourious drug development regime would typically consist of a review of literature relating to the disease, a study of the DNA and structure of the virus, followed by consideration of the suitability of various drugs. What could have taken 15 years to develop can now be undertaken via algorithmic processes in a matter of days.

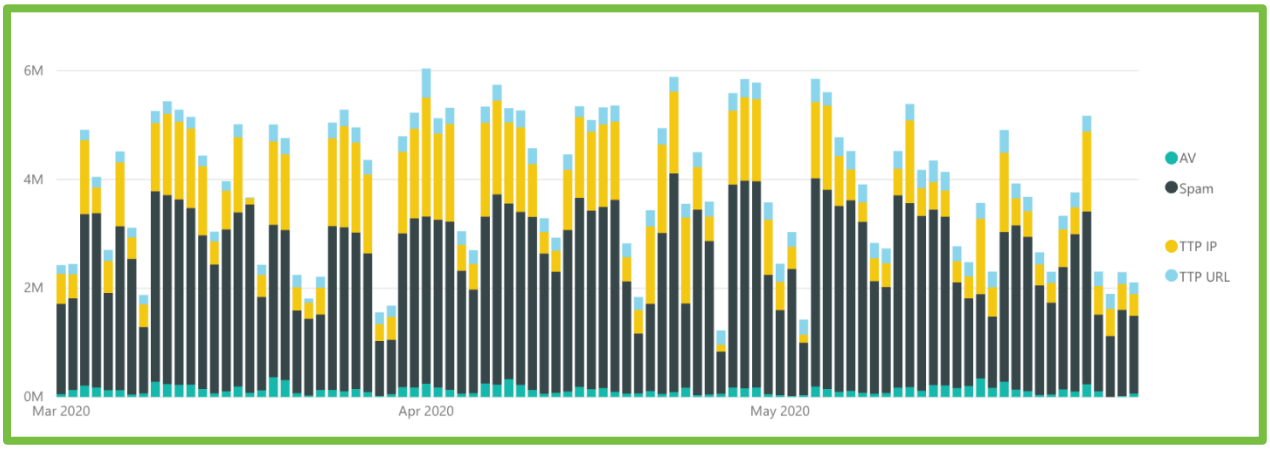

Figure 1: Statistics for the Healthcare Sector since Mar 2020 from Mimecast Data

Medical research and other sensitive intellectual property remain highly attractive to both traditional cyber threat actors and nation state actors; the introduction of progressive, innovative, and technological advancements increases their value. The research and associated intellectual property these organisations hold is extremely valuable,[2] none more so than to hostile states who are keen to advance their own programmes using research and IP obtained from elsewhere. On 05 May 2020, the UK's National Cyber Security Centre (NCSC) issued a joint cyber warning with the United States' Cybersecurity and Infrastructure Security Agency (CISA) to both healthcare and medical research organisations.[3]

With the large number of applications a healthcare provider uses, it can often be very hard for IT managers to keep up-to-date with the diversity of cyber threats, ever-changing legislation, and available platforms to manage

[1] https://www.bbc.com/news/technology-52120747
[2] https://www.bbc.com/news/technology-52551023
[3] https://www.ncsc.gov.uk/news/warning-issued-uk-usa-healthcare-organisations

these. Budget constraints imposed on NHS Trusts' risk appetite mean IT managers are heavily reliant on the advice from cybersecurity vendors to ensure high availability, secure data storage, and legislative practices. This often results in security policies not being able to keep up, or just not considered during the application of digital systems

The security triad of maintaining the confidentiality, integrity, and availability of data resonates thoroughly with this sector. Despite the necessity of drug discovery, there are still malicious entities intent on making financial gain from others suffering. All data has a value, be that reputational, financial, or intellectual

Data collected, consumed, and formulated by pharmaceutical companies, including technological, and patient information are both sensitive and valuable. Should those charged with maintaining the security of this data in either an information technology (IT) or operational technology (OT) environment lose control over that data, this can have catastrophic consequences eroding patient and consumer trust, leaving manufacturing processes at risk of compromise, and jeopardising potentially. A potential result could be the promulgation of fake and spoofed web pages, emails, and advisories promoting counterfeit drugs and the extortion of funds from an unsuspecting populace.[4]

Assessment (So What?): *While health technology tools and organisations are more powerful and impactful than ever before, individuals or organisations within this sector potentially hold the keys to ending the* ***COVID-19*** *pandemic. Consequently, they offer more cyberattack surfaces and options for adversaries.*

Both biotechnology and pharmaceutical companies have seen an increase in targeting by cybercriminals than in previous years. Reports have considered that the pharmaceutical industry is now the number one target of cybercriminals globally, especially for intellectual property theft. As these specialised companies move towards increased digitisation and a reliance on IT and OT for development, storage, and understanding of more valuable data online, they are becoming more attractive targets.

Stolen data can either be sold on the dark web or ransomed back to desperate companies who rely on access to critical documents, such as trial results, patient information, and intellectual property to continue operations.

Recommendation (What Can I Do?): *Networks are only as strong as their weakest vulnerability. Organisations that capture and retain data have a responsibility to ensure that detail in their charge remains confidential, complete, and available only to those with a need to access it. In order to achieve this IT security triad, it needs to be underpinned by a tested, robust, and considered cybersecurity policy. This policy should identify the requirement and process for implementing updates and patches when issued, and policies for software and hardware end-of-life activity.*

What can be evidenced from previous global data breach articles is the need for separation of operational and informational data. This can be achieved through air-gapped systems, a considered layered security approach, encryption, password protection, segregation, access-control, vetting, and application of user access groups / least privilege considerations being implemented.

For those organisations that are subjected to a ransomware attack the consequences stretch beyond the breach, compromise, and financial penalties. A longer lasting outcome is the reputational damage that the brand will be

[4] https://www.bbc.com/news/health-52201077

tarnished with. When a breach has been identified, it requires time and effort to contain the impact and mitigate the damage. This can cause a significant strain on resources, focus, people hours and funding that could have been used elsewhere.

There is no single layer or control that can be implemented which will completely protect an organisation against these attacks. Using a layered approach to fight against ransomware and other campaigns, a tried and tested continuity and recovery plan, and going back to basics is the best method to use when defending against attack.

With the medical sector having an increased reliance on AI, comes an increased number of devices, and objects being reliant and dependant on internet connectivity. This single factor leads to an increased number of potential, and vulnerable, exploitable access points for malicious actors. Unlike the many 'entertainment' devices that aggregate to form our understanding of the IoT, there are multiple connected medical devices that are often unseen, but vital. Connected medical devices have obvious benefits for clinicians, medical staff, and patients. These devices have the ability to instantly exchange data, or instructions on treatment. But this aspect is where some of the greatest dangers lie as the devices are often involved in critical procedures or treatments. Consequently, interference with the signals to a robotic surgical tool, for example, would potentially have devastating consequences.

Regardless of the intended use of systems, networks, and technology, they will typically suffer from the same inherent issues, and vulnerabilities. With a recent rollout of ***Microsoft 365*** across the NHS,[5] it is key that resilience and communication service downtime that directly impact any vital service provisions are understood fully. Any organisations moving to ***Microsoft 365*** security and productivity services, especially those part of CNI, should still be aware of their own business continuity, and resilience, seeking additional provision as necessary.

But when security teams believe that they solved a vulnerability, others will generally appear. Furthermore, with systems designed by humans, for humans, they will be considered, as default, to have numerous vulnerabilities at all levels through human error either from users, administrators, designers, or manufacturers.

Despite best intention, and as evidenced globally, the issue with maintaining an appropriate cybersecurity posture is typically compounded by budgetary constraints. Healthcare and the pharmaceutical industries are typically heavily reliant on the advice from cybersecurity vendors to ensure high availability, secure data storage, and legislative practices. This often results in security policies not being able to keep up, or just not considered during the application, maintenance, and through life support of digital systems.

[5] https://www.mimecast.com/blog/2020/06/critical-it-continuity-planning-for-a-secure-microsoft-365-national-health-service/

Assessment (So What?): *Although healthcare trusts and pharmaceutical companies can initiate a cybersecurity defence in depth policy, all staff within an organisation have a responsibility for maintaining the security profile. Training is essential and should be undertaken every six months by all staff. It only takes one person clicking on a malicious attachment to disrupt a whole system, potentially affecting patients' lives, or disrupting years of research.*

The reputation and trust of healthcare establishments depends on them understanding the extent of the threats they face on a daily basis. They are only as strong as the weakest link,[6] so it is essential that all networked devices, equipment, and access is appropriately secured and registered. Many endpoint devices reliant on internet connectivity, including patient-monitoring equipment or legacy dispersed networks, are often unpatched. The success of the ***WannaCry*** *attack was as a result of the prominence of the outdated* ***Windows 7*** *operating system that was common across the NHS.[7] Appropriate security measures are typically defined as ones that consist of attack prevention, security awareness training, roaming web security tied to email efficacy, brand exploitation protection, threat remediation and business continuity.*

What is Mimecast Seeing?

There has been a significant step change in reputation rejections starting in late February 2020, particularly in the UK. The volume of all threat detections relating to spam, impersonation, malware, blocked clicks and web or domain based threats has increased significantly during the period of report. The most significant increases occurred from March 2020 onwards as threat actors had now clearly pivoted to heavily exploit the pandemic as a key theme of global concern and therefore representing a huge opportunity for exploitation, compromise, fraud, and theft.

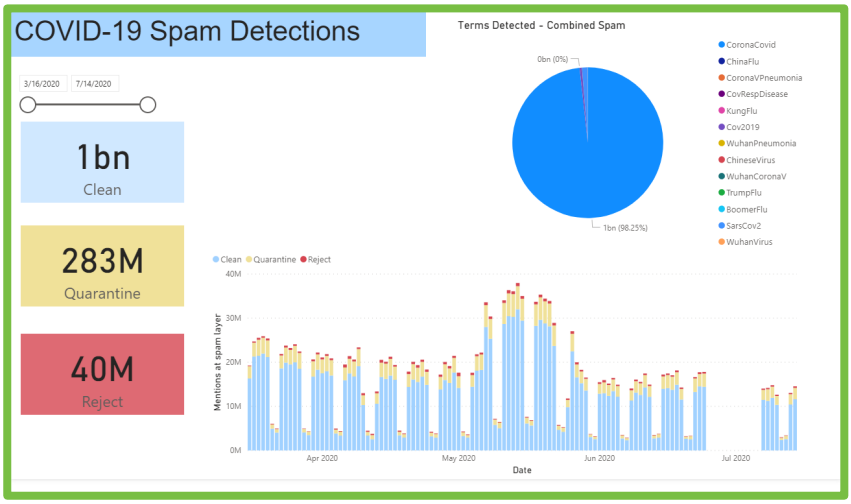

Figure 2: ***COVID-19 Spam Detections Apr to Jul 2020***

Figures 2 to 5 provide an overview of malicious detections (Malicious URL, Attachment Protect, Spam, AV, and Impersonation Protection) observed during the reporting period.

[6] https://www.bbc.com/news/technology-48935111
[7] https://www.bbc.com/news/technology-41753022

UK Healthcare

In examining the UK Healthcare sector, which includes both hospitals and clinics and other facilities, figures have remained at a fairly consistent level throughout the period reviewed. Mimecast's total detection data shows the volume and vector of attack over the course of the reporting period and the attachment type detected and blocked by AV scanners. Spam is the most frequent attack vector, followed by impersonation attacks. Spam campaigns are frequently used to spread other threats and are linked to dangerous malware attacks.

Figure 3: UK Healthcare - malicious detections between 01 January and 25 June 2020

- **Trend Analysis** - Spam remains the preferred method of attack, followed by impersonation, both of which have remained at a fairly constant level over the reporting period. There were five file types detected by attachment protect over the period of interest as illustrated in Figure 4, below.

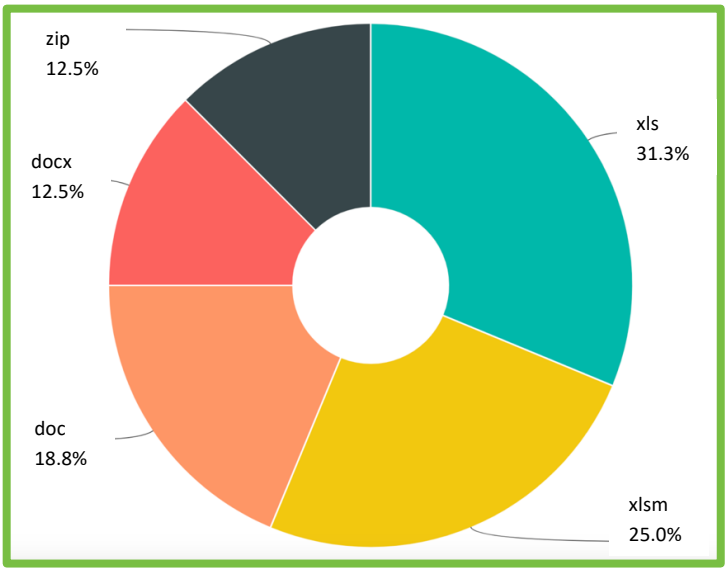

Figure 4: UK Healthcare – attachment types by volume between 01 January and 25 June 2020

- Impersonation detections peaked on the 20 Apr 2020 (2,975) and a low (188) on 29 Mar 2020.

- **AV detections** – The majority of detections were trojans associated with ***RAR, ZIP*** and ***Image*** files. Many trojans will promulgate malicious content via phishing emails, that typically contain links to a spoofed website, or malicious code, that will seek to harvest user credentials, such as username and password details, or secure network access.

UK Pharmaceutical and Biotechnology

Despite a number of significant spikes in February 2020 for the UK pharmaceutical and biotechnology sector, figures have remained at a constant level throughout the reporting period. Spam is the most frequent attack vector, followed by impersonation attacks for this sector.

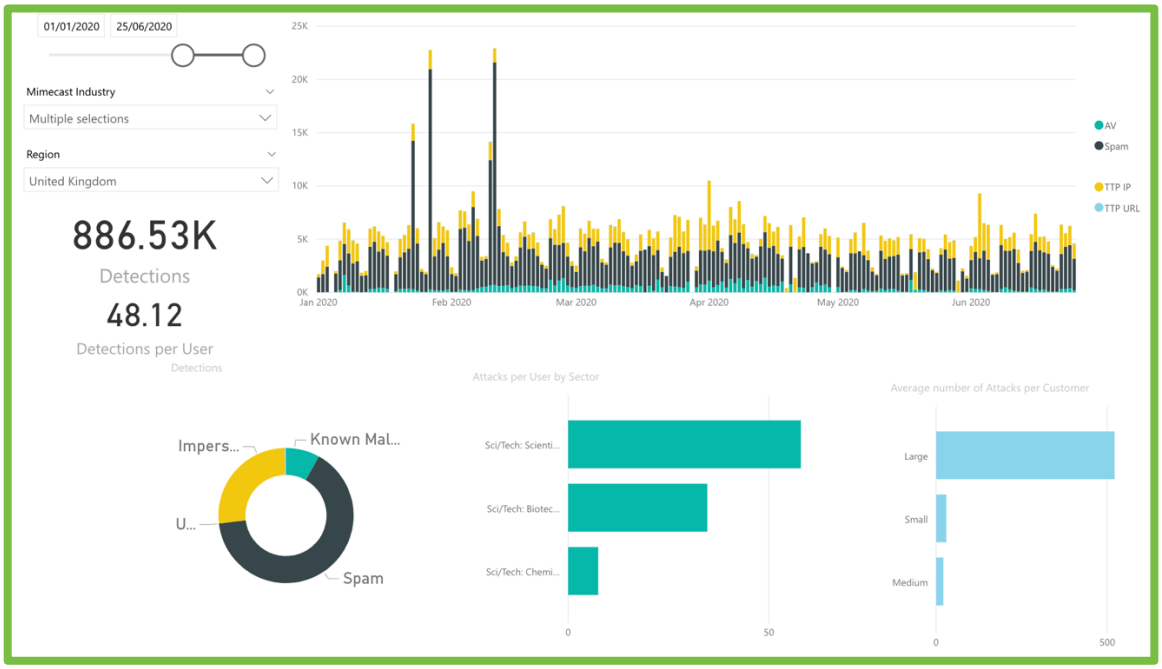

Figure 5*: UK Science & Technology (Pharmaceuticals and Biotechnology) - malicious detections between 01 January and 25 June 2020*

- **Trend Analysis** - Spam was again the preferred method of attack, followed by impersonation, both of which remaining at a fairly constant level over the reporting period. There was only a single file type detected by attachment protect over the period of interest, which was ***.doc***.

- Impersonation detections peaked on the 31 Mar 2020 (663) and exhibited a low (3) on 24 May 2020.

- **AV detections –** In parallel with findings for the UK Healthcare sector, the majority of detections identified were trojans associated with ***RAR***, ***ZIP*** and ***Image*** files.

Republic of Ireland Healthcare

Analysis of the Republic of Ireland (RoI) Healthcare sector, encompassing hospitals and clinics and other facilities, have shown a greater degree of fluctuation across the reporting period when compared to figures for the UK Healthcare sector. This is illustrated in the graph at Figure 6.

Figure 6*: Republic of Ireland Healthcare - malicious detections between 01 January and 25 June 2020*

- **Trend Analysis** – Comparable to the UK sector, spam was again the preferred method of attack, followed by AV, then impersonation attacks.

- **AV detections –** In parallel with findings for the UK Healthcare sector, the majority of detections identified were trojans associated with ***RAR***, ***ZIP*** and ***Image*** files. There were also detections of ***Cryxos*** variants during the reporting period.

Emerging Threats

From reviewing the threat landscape, an important part of assessing the potential for systemic risk from a cyberattack is understanding the mechanisms and pathways that could propagate the effects of an attack. As organisations become more dependent on technology as a business enabler, the security and reliability of their connectivity is inevitability of increasing importance.

Since the ***WannaCry***[8] attack on the NHS in 2017, the healthcare, pharmaceutical, and biotechnology sectors have been conscious of the possibilities of a ransomware attack. In addition to the loss of sensitive data, ransomware attacks are capable of putting the lives of patients at risk, supplementary to causing disruption

[8] https://www.bbc.com/news/technology-39917278

across the entirety of a healthcare network. Ransomware attacks, such as those evidenced by the successful ***WannaCry*** incident, are capable of delivering a significant impact on the sector and its ability for industry professionals to deliver accurate and considered patient car. A successful attack has the ability to access records of patient's drug prescriptions / allergies and/or being able to use vital equipment to keep patients alive.

Ransomware continues to be on the rise; Mimecast has seen healthcare providers targeted in the past as well as a trend of ransomware extracting data and making this available for download if demands aren't met. Healthcare provides an opportunity for more sensitive data to be extracted and higher risk for confidential data to be made publicly available.

Assessment (So What?): *For those organisations that are subjected to a ransomware attack the consequences stretch beyond the breach, compromise, and financial penalties. A longer lasting outcome is the reputational damage that the brand will be tarnished with.*

Global ransomware attacks have increased significantly in number over previous years and have caused millions of dollars of data recovery costs, brand damage recovery costs, operational costs, insurance costs, and other expenses to organisations.

Ransomware is designed to transit a network quickly and covertly. Ransomware attacks are assessed as ***highly likely (≈80% – ≈90%)*** *to continue to increase. As tactics, techniques, and procedures continue to develop, the targets selected and researched by criminal entities are* ***likely (≈55% – 75%)*** *to become more sophisticated with a higher 'risk and reward' for those willing to exploit.*

Recommendation (What Can I Do?): *These attacks may manifest through email, URL link, BEC, or malicious website. Protecting an orgnisation's 'electronic and network' perimeter is no longer considered as adequate. Protection needs to move beyond the perimeter, to the pervasive environment that is beyond the control of an organisation's security team. This protection, however robust, will need to be enhanced with implementation of a considered cyber resilience plan which should deliberate business continuity, and how an organisation will be able to continue with its critical dependencies should it be targeted by a successful ransomware campaign.*

Given the prevalence of ransomware, apparent in the most recent campaigns, likely representative of wider use generally, and the potential for ***Emotet*** *campaigns being primarily intended to insert this threat, it should be considered an unacceptable risk at this time for any organization to utilize* ***Internet Explorer (IE)*** *as an internet browser. The same should be considered for Flash Plugin software. Ransomware threat actors are specifically making increased use of exploit kits at this time as an additional means to compromise networks and both* ***IE*** *and* ***Flash*** *are specifically vulnerable to exploitation via this means; they are* ***highly likely (≈80% – ≈90%)*** *to be compromised if used to visit an infected or threat actor controlled website. A review of cyber resiliency in the face of this threat should ensure that non-networked backups are undertaken and that the organisation has the facility to utilise fallback email and file archiving capabilities.*

There are also a huge number of opportunities for attacks on healthcare systems simply due to the extent to which they rely on technology. Modern healthcare makes use of, and is to a degree reliant on, the ever-expanding propensity for technology. This technology though does not consider just computer systems and hospital equipment, but also devices attached to and even embedded in the human body, such as fitness monitors, blood pressure monitors, blood glucose monitors, or digital pacemakers. If they are capable of sending data from one device to another or between users, vulnerabilities are likely to be exploited, provisioning many ways in for a cyber threat actor, be that from data networks to mobile applications and even non-medical systems such as CCTV.

With funding always a topical / political discussion point for government and NHS Trusts, there are always copeting priorities for how funds are spent. Is it prioritised on patient care, medical equipment, salaries, or cybersecurity? The response to the ***COVID-19*** pandemic will have seen an extensive and unforeseen impact on healthcare budgets. This will be as a result of both the staff who have received negligible pay increases for many years will have been tested. But should funding reward the staff for their loyalty or bolster cyber defences against the widening threat aperture?

Mimecast's Emerging Threats team, considers that following the ***COVID-19*** pandemic, there will be an increased investment in healthcare technology in order to advance, but also reduce running costs in the long term. As an example the UK healthcare sector appears to be making advances in embracing mobile technology, and associated mobile applications to connect with patients. With surgeries having closed their doors to reduce the ability for the coronavirus to transmit, online consulting, has become the norm. This makes life much easier for the patients and cuts time and costs of GPs and hospitals. However, once the wider population start using electronic and technological devices for these personal and confidential encounters , we should expect to see a rise of phishing/malware emails exploiting fear and ignorance of the end users, malicious mobile apps, and also attacks to unprotected databases in order to gain access to healthcare data. Another worrying aspect could be user privacy, as many mobile apps for any reason could require location data amongst personal data.

Healthcare organisations are reliant on the Internet and networks to function. However, the evolution of technology, and the increased drive towards mobility, has facilitated threats from cybercriminals who use this same enabler to gain access to organisational networks, exfiltrate PII, intellectual property (IP), and take advantage of any potential vulnerabilities. With the introduction of social distancing and requirement for medical staff to support the demand placed on hospitals, many GP surgeries moved to a remote working practice. This would see GPs' work remotely undertaking phone triage and video consultations through computers and smart phones. With links being sent by the GP to the patient to initiate the consultation, the threat vector could be seen as becoming more vulnerable, with an increased opportunity for exploitation becoming apparent with a lack of verification and authentication.

The threat vector is continued to be seen as an expanding surface, more so with the propagation of:

5G

Fifth-generation mobile technology is opening us to a period of increased vulnerability of disruption. Various joint risk assessment reports have highlighted increased security risks that will require a new approach to securing telecoms infrastructure. 5G will also present an increased exposure platform for attacks, offering more potential entry points for attackers to utilise.

5G topology will be increasingly based on software, and the associated risk and security flaws resultant from poor software development processes by suppliers, will gain importance. Insufficient process could make it easier for threat actors to insert backdoors into products and make malicious code harder to detect.

Internet of Things (IoT) and Industrial Internet of Things (IIoT)

State-sponsored, hacktivist-driven, and other adversary-driven attacks on IIoT systems are increasing, especially in the CNI sector, and manufacturing industries. Adversaries are taking advantage of the fact that various industries are slowly moving to digitise its own IIoT systems.

Assessment (So What?): *Cybersecurity professionals have, for some time, warned of poor practices and implementation associated with IoT security and these are now becoming realised. The risks are compounded with historic weaknesses in the cybersecurity regimes of energy companies, often dated ICS platforms, convergence of IT and OT, and a 24/7/365 requirements for service fulfilment.*

Medical equipment is costly to update, upgrade, and reconfigure. As with more traditional industrial control systems there is often the belief that because it is operational 24/7/365 and it works, it cannot be turned off, updated, or reconfigured.

*With the convergence of the IoT, IT systems, and Operational Technology (OT) systems, it is **almost certain (>95%)** that data and networks are at heightened risk of both ransomware & data compromise attacks, and a danger that IoT devices may be as steppingstones for lateral movement within a network.*

*Organisations key to the UK's CNI have been on high alert throughout the **COVID-19** pandemic, with the NCSC having issued warnings over the proceeding weeks of malicious cyber threat actor groups targeting UK bodies critical to the countries infrastructure through password spraying attacks and other campaign vectors.[9]*

The consequences of targeted attacks against key players in the energy supply chain could range from minor disruption of day-to-day operations, to massive energy blackouts that could, in turn, hamper other critical organisations, like hospitals. This could also affect a healthcare provider's own generation sources or UPS.

Research[10] has uncovered numerous bugs and exploitable vulnerabilities in the control code for some SCADA systems that could be potentially more serious than Stuxnet. Similarly, a number of flaws have also been identified in the most commonly used SCADA systems, where vulnerabilities could potentially give an attacker complete control over a targeted system. The three predominate weaknesses in any OCS is considered as people, process, and technology.

There is a push to move more and more operational technology (OT) systems into the IP world, however, the dated ICS operating systems will continue to present a significant vector for online exploitation.

With the footprint for attack vectors ever increasing with the proliferation of 5G and the IoT, the potential risk to ICS Is one that needs to remain at the forefront of security thinking in 2020. ICS represents a grey space that often falls between the IT and OT space. Cybersecurity in the ICS environment is concerned with more than the protection of data. It is focussed on ensuring the safe and reliable operation of plant infrastructure, and the protection of people, and the environment. With traditional cybersecurity aligned to maintaining the confidentiality of data, ICS security is more aligned to maintenance of the integrity and availability of systems and processes.[11]

[9] https://www.ncsc.gov.uk/files/Joint%20NCSC%20and%20CISA%20Advisory%20APT%20groups%20target%20healthcare%20and%20essential%20services.pdf
[10] https://www.bbc.com/news/technology-47812479
[11] Tim Harwood, Director Siker, ICS Practitioners Security

Case Study 1 – *COVID-19* campaigns

In cyber threat terms, there has been a dramatic step change in reputation rejections starting in late February 2020, which was particularly evident in the UK.[12] Since the outbreak of the ***COVID-19*** pandemic, researchers at Mimecast uncovered a number of different campaigns – including emails targeting healthcare professionals regarding a staff seminar on the virus (where they are encouraged to enter their credentials in an Outlook application) or emails containing a link that directs recipients to a fake website bearing an HMRC logo offering a tax refund (where they are encouraged to enter bank account details):

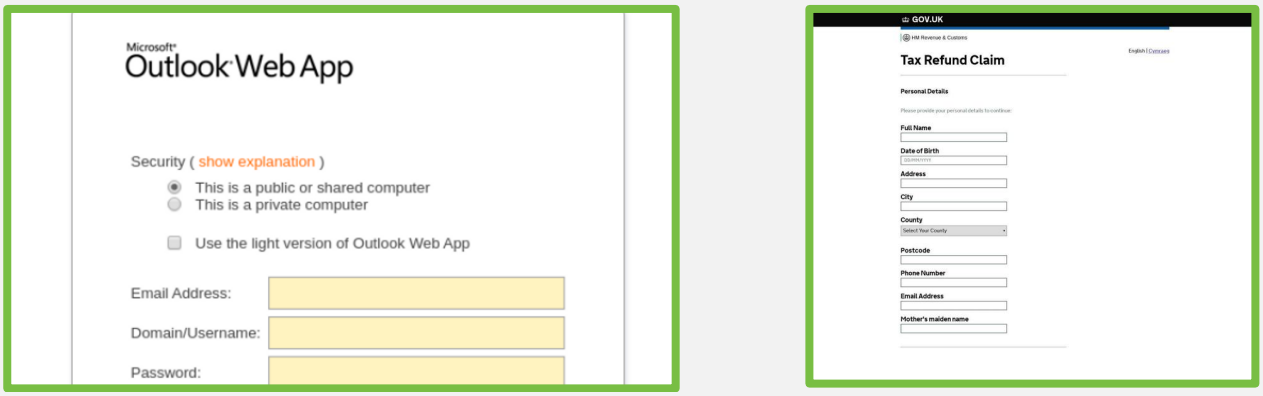

Figure 7*: Screenshots of Coronavirus Campaigns – Healthcare Professionals (left) and HMRC (right)*

Numerous emails have illustrated the diverse and changing nature of the campaigns undertaken during the first 100 days of ***COVID-19***. The following example is representative of campaigns identified, focussing on the healthcare sector. The example provided at Figure 8, below, is an example of such emails. As with all examples provided by our researchers, the emails are primarily spam and phishing samples which sought to steal credentials and/or personal details from their intended target.

09 April 2020 – *COVID-19* Healthcare Welcome Email

This sample is also a message that was apparent in volume from this date and purported to represent a virus specific healthcare scheme in an attempt to lure clicks and credential theft. The group and policy IDs were the same in all noted cases:

[12] https://www.mimecast.com/globalassets/cyber-resilience-content/100-days-of-coronavirus-threat-intelligence.pdf

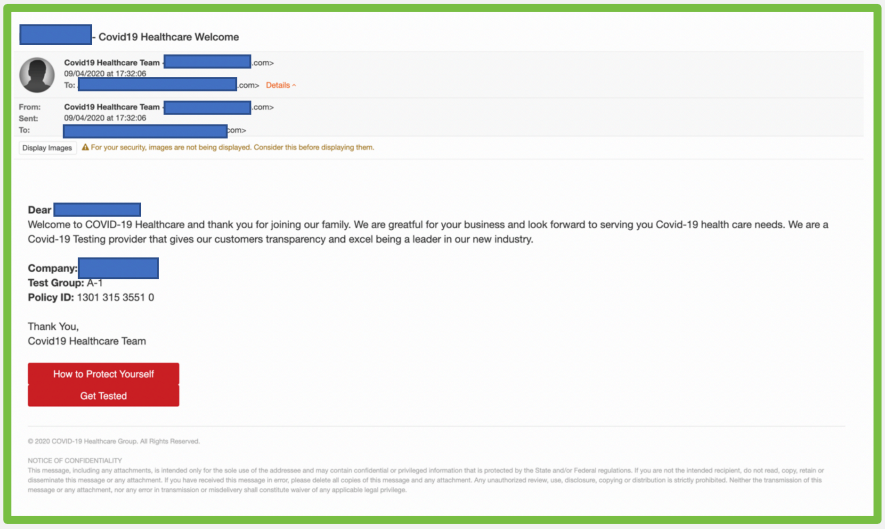

Figure 8: Healthcare Welcome Email

The following articles are representative of a cross-section of publicly available open source media reporting, that identifies and confirms the ever-present threat to the healthcare, biotechnology and pharmaceutical industries at this time.

Case Study 2 – *US Accuses China of Hacking Vaccine Development*

The federal government's top cybersecurity agencies have accused China of undertaking a cybercampaign intended to undermine the US response to the ***COVID-19*** pandemic and development of a vaccine. A joint warning was issued by the US Cybersecurity and Infrastructure Security Agency (CISA) and UK National Cyber Security Centre (NCSC) regarding this activity.[13]

The joint advice issued, was designed to warn US and UK organisations researching the effects of the virus of the "likely targeting and network compromise" by those intent on effecting the critical response to this global pandemic. However, China is now not alone in seeking to exfiltrate research data, with Russian attacks now having been identified against organisations involved in ***COVID-19*** vaccine research and development.[14]

Activity likely targeting healthcare, biotechnology, and pharmaceutical organisations and their work in developing a vaccine will be intent on bolstering identical work being undertaken in hostile states, rather than undermining any target.

[13] https://www.ncsc.gov.uk/news/warning-issued-uk-usa-healthcare-organisations
[14] https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development

Assessment (So What?): *While health technology tools and companies are more powerful and impactful than ever before, individuals or organisations within this sector potentially hold the keys to ending the **COVID-19** pandemic. Consequently, they offer more cyberattack surfaces and options for adversaries.*

Both biotechnology and pharmaceutical companies have seen an increase in targeting by cybercriminals than in previous years. Reports have considered that the pharmaceutical industry is now the number one target of cybercriminals globally, especially for intellectual property theft. As these specialised companies move towards increased digitisation and a reliance on IT and OT for development, storage, and understanding of more valuable data online, they are becoming more attractive targets. Stolen data can either be sold on the dark web or ransomed back to desperate companies who rely on access to critical documents, such as trial results, patient information, and intellectual property to continue operations.

Recommendation (What Can I Do?): *Networks are only as strong as their weakest vulnerability. Organisations that capture and retain data have a responsibility to ensure that detail in their charge remains confidential, complete, and available only to those with a need to access it. In order to achieve this IT security triad, it needs to be underpinned by a tested, robust, and considered cybersecurity policy. This policy should identify the requirement and process for implementing updates and patches when issued, and policies for software and hardware end-of-life activity.*

All organisations should have an appreciation of the wider supply chain and joint research institutes that they are in collaboration with. Exploitation and compromise of less security conscious organisations that work alongside key research entities has the potential to allow pivoting by cyber threat actors on to more secure networks. An understanding of the entire collaborative environment should therefore be undertaken to ensure that adequate cybersecurity defensive measures are in place. A regular review of those in the supply chain should also be undertaken, with those no longer in contract, having any access or authentication means removed.

What can be evidenced from previous global data breach articles is the need for separation of operational and informational data. This can be achieved through air-gapped systems, a considered layered security approach, encryption, password protection, segregation, access-control, vetting, and application of user access groups / least privilege considerations being implemented.

For those organisations that are subjected to a ransomware attack the, consequences stretch beyond the breach, compromise, and financial penalties. A longer lasting outcome is the reputational damage that the brand will be tarnished with. When a breach has been identified, it requires time and effort to contain the impact and mitigate the damage. This can cause a significant strain on resources, focus, people hours and funding that could have been utilised elsewhere.

There is no single layer or control that can be implemented which will completely protect an organisation against these attacks. Using a layered approach to fight against ransomware and other campaigns, a tried and tested continuity and recovery plan, and going back to basics is the best method to use when defending against attack.

Case Study 3 – *Heightened Risk Consideration to the Pharmaceutical and Biotechnology Industry*

In these unprecedented times, there has been an observable escalation in potential malware instances, as malicious entities seek to capitalise and exploit the times of confusion and vulnerability that has resulted from the ***COVID-19*** pandemic.

The cyber environment is one that is continually evolving in both the offensive and defensive spheres. The constant game of 'cat and mouse' is interspersed with the advantage and successes alternating between the hunter and the gamekeeper. But despite the global pandemic and associated fallout, malicious entities are intent on increasing suffering by targeting the retail and healthcare sectors. Although the effects of any cyberattack can be catastrophic, the pharmaceutical sector can be considered as a multi-faceted opportunistic target facing particularly significant implications to any potential breach.

Cybersecurity is typically bound by the security triad of ensuring data remains confidential, complete, and available. With many pharmaceutical companies around the globe striving to develop cures and vaccines for ***COVID-19***, an increased reliance on AI within this industry, and the protection of patient, intellectual and proprietary data.

Video conferencing and collaborative workspace software have seen a monumental increase in both usability and popularity during the pandemic. These technological spaces are considered as ***highly likely (≈80% – ≈90%)*** as representative of the new working paradigm , once a return to 'the new normal' is underway.

Assessment (So What?): *Both biotechnology and pharmaceutical companies have seen an increase in targeting by cybercriminals than in previous years. Reports have considered that the pharmaceutical industry is now the number one target of cybercriminals globally, especially for intellectual property theft. As these specialised companies move towards increased digitisation and a reliance on IT and OT for development, storage, and understanding of more valuable data online, they are becoming more attractive targets. Stolen data can either be sold on the dark web or ransomed back to desperate companies who rely on access to critical documents, such as trial results, patient information, and intellectual property to continue operations.*

Recommendation (What Can I Do?): *Networks are only as strong as their weakest vulnerability. Organisations that capture and retain data have a responsibility to ensure that detail in their charge remains confidential, complete, and available only to those with a need to access it. In order to achieve this IT security triad, it needs to be underpinned by a tested, robust, and considered cybersecurity policy. This policy should identify the requirement and process for implementing updates and patches when issued, and policies for software and hardware end-of-life activity.*

What can be evidenced from previous global data breach articles is the need for separation of operational and informational data. This can be achieved through air-gapped systems, a considered layered security approach, encryption, password protection, segregation, access-control, vetting, and application of user access groups / least privilege considerations being implemented.

For those organisations that are subjected to a ransomware attack the, consequences stretch beyond the breach, compromise, and financial penalties. A longer lasting outcome is the reputational damage that the brand will be tarnished with. When a breach has been identified, it requires time and effort to contain the impact and mitigate the damage. This can cause a significant strain on resources, focus, people hours and funding that could have been utilised elsewhere.

Ransomware is designed to transit a network quickly, and covertly. There is no single layer or control that can be implemented which will completely protect an organisation against these attacks. Using a layered approach to fight against ransomware, a tried and tested continuity and recovery plan, and going back-to-basics is the best method to use when defending against attack.

Case Study 4 – Internet of Things a Potential Security Nightmare

Recent analysis has identified that an estimated 98% of traffic transmitted throughout the Internet of Things (IoT) is unencrypted. This has the potential to expose significant quantities of both personal and confidential data to a plethora of attackers and cybercriminal entities.[15] However, this risk is significantly enhanced by most networks having a mix of IoT devices and traditional IT equipment such as laptops and mobile devices. This consolidation of devices has the increased potential to expose networks to attack with unpatched laptops facilitating access to IoT devices, or vulnerable IoT devices infecting PC's. Each scenario would permit access to vast quantities of saleable data or expose an organisation to the heightened risk of ransomware.

The research undertaken, focussed heavily on the healthcare sector where it established that approximately 83% medical imaging devices run on unsupported operating systems (OS) such as ***Windows 7***. With the prevalence of unsupported OS and a high proportion of healthcare LAN's mixing IoT and traditional assets, the potential for ransomware attacks and for hackers to access personal data is immense.

Assessment (So What?): *Cybersecurity professionals have, for some time, warned of poor practices and implementation associated with IoT security and these are now becoming realised.*

Medical equipment is costly to update, upgrade, and reconfigure. As with more traditional industrial control systems there is often the belief that because it is operational 24/7/365 and it works, it cannot be turned off, updated, or reconfigured.

*With the convergence of the IoT, IT systems, and operational technology (OT) systems, it is **almost certain (>95%)** that data and networks are at heightened risk of both ransomware & data compromise attacks, and a danger that IoT devices may be as steppingstones for lateral movement within a network.*

Recommendation (What Can I Do?): *With the increased convergence of devices on networks and the inherent vulnerability of IoT devices, they are perceived as an easy target for hackers and cybercriminals. It is recommended that IoT devices are password protected, with each device having a unique password.*

Although likely costly, consideration should be given to replacing outdated equipment and unsupported OS. Password protected IoT devices should have the factory set password changed on setup, every 90 days, and when staff who have access to the device leave or no longer require access. Employing a 'defence in depth' methodology throughout any organisation is considered an essential and effective requirement.

[15] https://my.silobreaker.com/v2/tool/search?q=%22The%20Internet%20of%20Things%20is%20a%20security%20nightmare%20reveals%20latest%20real-world%20analysis:%20unencrypted%20traffic,%20network%20crossover,%20vulnerable%20OSes%22

Summary

Healthcare, medical research, and personal data are considered as the most sensitive data types requiring constant protection of its confidentiality, integrity, and availability. The targeting of healthcare providers, and pharmaceutical entities, is becoming a global issue. With the 2017 ***WannaCry*** attacks still at the forefront of the industry, ransomware attacks are assessed as ***highly likely (≈80% – ≈90%)*** to continue to increase. As tactics, techniques and procedures continue to develop the targets selected and researched by criminal entities are ***likely (≈55% – 75%)*** to become more sophisticated with a significantly higher 'risk and reward' for those willing to exploit an expansive vulnerability aperture.

The determination of threat actors to take advantage of the unique circumstances, and therefore opportunities the current pandemic and its associated fear and uncertainty present, should not be underestimated. Threat actors, and likely also those criminals who have committed other offences, are almost certainly focussed on taking maximum advantage of the once-in-a-lifetime opportunity to scam and defraud both individuals and businesses that the current situation of varying national "lockdowns", supply demand, and stretch of healthcare resource presents.

Threat actors will always seek opportunities for exploiting chaos, confusion, and uncertainty to their advantage. Through utilising deception, feigns, and guile they seek to deliver malicious effects. It is considered ***highly likely*** **(≈80% – ≈90%)** that threat actors will utilise the period of uncertainty, stress, and confusion, to exploit those who are most vulnerable. The current situation of uncertainty and fear will almost certainly lend itself to increased incidents of human error due to stress and the difficulties of working in an environment that may be further deteriorated by a lack of workspace or additional caring issues. This will inevitably increase stress and tiredness and therefore the odds of human error playing a part in any compromise are likely to be increased, and to increase further over time.

During the current environment of significant uncertainty, and with the realistic probability of significant disruption continuing, successive waves of the virus, and the potential for further future geographical or national "lockdown" periods, cyber resiliency will be key to exiting this current crisis, intact. Cybersecurity should be considered a multi-layer, multi-discipline, and collaborative environment. Companies and sectors should be encouraged to share information and adopt a proactive, rather than reactive, approach to securing networks, devices, information, research, finances, and PII. At the same time, with many employees increasingly working alone or in isolation, there is likely to be a greater burden of judgment placed upon them, as threat actors continue to attempt every means possible to compromise organisational networks.

Threat actors are opportunistic and inventive – often taking advantage of an organisation's own information to use it against them. They assess how well it secures its networks to identify vulnerabilities in the infrastructure and defences, which they then use to improve their attack methodologies. If an organisation is well protected, these threat actors may pursue third-party stakeholders or those in the 'supply chain' – such as business partners, collaborative research organisations, or suppliers, whose defences may not be as robust, and use these external networks as an alternate way to gain access.

Additional Resources

The following is a list of recommendations, advice, and guidance issued recently by the UK's National Cyber Security Centre (NCSC) and deemed pertinent to the healthcare, biotechnology, and pharmaceutical sectors:

16 July 2020
NCSC
UK and allies expose Russian attacks on coronavirus vaccine development
https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development

19 May 2020
NCSC
NHS Covid-19 app security: two weeks on
https://www.ncsc.gov.uk/blog-post/nhs-covid-19-app-security-two-weeks-on

15 May 2020
NCSC
Cyber attacks target organisations supporting COVID-19 response
https://www.ncsc.gov.uk/report/weekly-threat-report-15th-may-2020

05 May 2020
NCSC
Cyber warning issued for key healthcare organisations in UK and USA:
https://www.ncsc.gov.uk/news/warning-issued-uk-usa-healthcare-organisations

05 May 2020
NCSC
Advisory: APT groups target healthcare and essential services
https://www.ncsc.gov.uk/news/apt-groups-target-healthcare-essential-services-advisory

03 April 2020
NCSC
Microsoft warns coronavirus-hit hospitals of ransomware threat
https://www.ncsc.gov.uk/report/weekly-threat-report-3rd-april-2020

13 February 2020
NCSC
Mitigating malware and ransomware attacks
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

22 January 2020
NCSC
Virtual Private Networks (VPNs)
https://www.ncsc.gov.uk/collection/mobile-device-guidance/virtual-private-networks

30 September 2019
NCSC
NCSC CAF Guidance
https://www.ncsc.gov.uk/collection/caf/introduction

18 September 2019
NCSC
Trusted Research - protecting your research
https://www.ncsc.gov.uk/blog-post/trusted-research

22 March 2019
NCSC
Policy Paper - CNI Sector Security and Resilience Plans 2018: summary
https://www.gov.uk/government/publications/sector-security-and-resilience-plans-2018-summary

20 December 2018
NCSC
APT10 continuing to target UK organisations
https://www.ncsc.gov.uk/news/apt10-continuing-target-uk-organisations

10 May 2018
NCSC
NIS Guidance - The Network and Information Systems Regulations 2018
https://www.legislation.gov.uk/uksi/2018/506/contents/made

How Mimecast Mitgates the Threat:

- **Multiple anti-virus engines** and continually updated global signature database stop known malware.
- **Multi-layered attachment scanning** including static file analysis, sandboxing and safe file conversion blocks unknown malware
- **URL re-writing** with time-of-click analysis protects against links leading to malicious sites and content.
- **Internal and outbound threat protection** monitors, detects, and remediates security threats that originate internally as a result of compromise, careless or malicious action.
- **Web security** prevents access to malicious sites and analyses suspicious file downloads.
- **Data recovery** restores lost or corrupted email content to a known good state.
- **Awareness training** improves employee security knowledge and vigilance to improve the human firewall.

Contact:

For further details, please contact: customer.advocacy.gb@mimecast.com

mimecast®