KnowBe4
Human error. Conquered.

Rising Threat Of Malware Attacks In Ireland And United Kingdom Healthcare Sectors

INTRODUCTION

Healthcare institutions are responsible for safeguarding some of the most vital and confidential data in the world. Criminal hackers are keenly aware of this fact and may exploit it by demanding ransom in exchange for protection of the patients' information. When health information is centralised, as it is in the United Kingdom and Ireland, the sector becomes a lucrative business model for international cybercriminals.

The sector's vulnerability was on display in 2021, when Ireland's Health Service Executive (HSE) was subjected to the largest known attack against a health service computer system in history, paralysing crucial aspects of hospital care including surgery scheduling, diagnostics, and cancer treatments.

This was not the first attack in the region. In 2017 England's NHS was crippled by a WannaCry ransomware attack that encrypted 230,000 computers on the system. The attack affected 80 service providers, 603 primary care and other NHS organisations, and 595 General Practitioner offices, and caused cancellation of 19,000 appointments. Critical equipment and systems became inoperable or unavailable, which led to the closure of emergency rooms. The costs to the NHS from the attack are estimated at £92 million.

Since that time, the threat has only increased. A 2022 report by the government of Ireland notes that "the reality is that critical systems in Ireland's health, energy, communications, transport and other key sectors are under constant threat of ransomware and other malicious cyber activity." The United Kingdom's National Cyber Security Centre (NCSC) CEO Lindy Cameron has called for increased UK-Ireland cooperation to prevent attacks and improve shared responses.

In recent years, four nation states – China, Russia, North Korea and Iran – have had a near constant presence in the cybercrime landscape in the UK, Europe, and globally. In April 2023, the NCSC issued an alert, warning of the emergence of a new class of attacks over the previous 18 months, from state-aligned groups sympathetic to Russia's invasion of Ukraine. As the groups are not motivated by financial gain but by the "desire to achieve a more destructive impact against Western civilization," they have become less predictable.

In all cases, keeping in mind that social engineering and phishing account for 70 to 90% of all malicious data breaches, security awareness training provides a critical last line of defence against the growing level of threat.

THE COST OF ONE WRONG CLICK

The 2021 attack against Ireland's HSE began on 18 March, when an employee opened a phishing email and clicked on an attachment, an Excel file. The file used Conti ransomware-as-a-service (RaaS), executed by a Russian criminal gang known as Wizard Spider. The malware roamed the HSE IT system for eight weeks, looking at files and planting more malware before acting. On 18 May, they struck.

The HSE is Ireland's publicly-funded healthcare system under the Irish Department of Health. It consists of 54 public hospitals directly under HSE authority, and voluntary hospitals that utilized the national IT infrastructure. In one stroke, the Conti malware encrypted and effectively shut down 80% of the HSE IT environment. Hospital staff were forced to revert to pen and paper, with no access to diagnostics, medical records, or email. This in turn forced cancellations of critical medical procedures, including hospital care, imaging services, gynaecology and maternity, children’s care, cancer treatments, psychiatric, and community health services.

The ransomware allowed the hackers to exfiltrate 700GB of sensitive data, including protected health information (PHI). Stolen medical and personal data of more than 100,000 patients was then sold on the dark web.

No ransom was paid, and on 21 May, the hackers dropped a decryption key. Even with the key, it was six months after the initial attack before the servers were declared fully decrypted, on 21 September with 99% of applications restored.

The costs were staggering. The HSE attack is estimated to have cost more than €100 million to date. Another €650 million was required to overhaul and fortify the HSE’s IT system. This does not include the staff time to restore or fortify the system, or the costs to affiliated independent hospitals.

Hackers have continued to sell data stolen from the attack on the dark web.

A REGION-WIDE WEAKNESS

While Ireland’s HSE attack was the largest and most severe for the region, it was far from an isolated incident.

A quarterly Digital Universe study by Obrela Security Industries found that in the first quarter of 2021, there had been a 76% increase in attacks targeting healthcare organisations globally over the same quarter in 2020.

The United Kingdom was particularly ill-prepared. A survey of 100 cybersecurity managers in the UK health sector released on 19 October 2021 found that 81% of healthcare organisations in the United Kingdom had been hit by ransomware in the previous year. 38% of the healthcare organisations attacked paid a ransom demand to get their files back. 44% refused to pay a demand and lost their healthcare data as a result.

Close to two-thirds (64%) of respondents admitted their organisation has had to cancel in-person appointments because of a cyber attack. 65% believed that a cyber attack on their systems could lead to loss of life.

The survey concluded that while healthcare organisations uniformly hold sensitive data, “many are completely unprepared for cyber attacks.”

“What is worrisome is that healthcare technology is often deployed and used without security in mind. Therefore, security professionals must consider that the risk profiles of those organisations are now higher, given the complexity of the underlying infrastructure, as well as the fusion of previously physically and logically separated technologies. “

“In short, we need to act now, otherwise we will witness of the loss of human lives.”

The Obrela study also recognized the role of security awareness as a last line of defence. Its first recommendation was to “Conduct comprehensive and rigorous end-user awareness training on phishing and social engineering techniques. Not every member of the organisation will have the technical background to understand the implications of a malicious email, but everybody should understand that they are sharing a common cyber risk.”

RISING ATTACKS IN 2022

According to Check Point, UK organisations collectively experienced a surge in cyber attacks in 2022, with a 77% increase over 2021. Healthcare was the third most frequently targeted sector, with an increase of 74%. The report attributes the increase to the fact that "the ransomware ecosystem is continuing to evolve and grow with smaller, more agile criminal groups that form to evade law enforcement."

"Second, hackers are widening their aim to target business collaboration tools such as Slack, Teams, OneDrive and Google Drive with phishing exploits."

On 4 August 2022, a ransomware attack caused widespread outages across England's National Health Service (NHS) when Advanced, the service provider for numerous NHS services, including the NHS medical "hotline" 111 service, used by thousands each day, was attacked. The attack crippled systems used to refer patients for care, dispatch ambulances, book appointments, and fulfil emergency prescriptions. The clinical management systems for surgeries, care homes and mental health services, all of which were hosted by Advanced, were brought down. It was more than four weeks before the systems were restored.

The attackers accessed and extracted client data from the Advanced servers. The extent of the data theft, and financial impact of the attack, were not publicly reported.

The Advanced attack also started with unauthorized access to one computer, in this case through theft of credentials. According to the Advanced report, the hackers accessed the network using stolen credentials and established a remote desktop (RDP) session to the server. As in other attacks, once in, the attacker moved laterally in the system, conducting reconnaissance and deploying encryption malware.

2022 also saw an increase in the practice of hackers contacting patients directly and demanding payment to avoid release of health insurance information, medical records, and financial data stolen during an attack.

EMERGING THREATS FROM STATE-ALIGNED GROUPS

On 19 April 2023, the UK's NCSC issued an alert to critical national infrastructure (CNI) organisations warning of an emerging threat from state-aligned groups.

The healthcare sector is identified by the NCSC as one of the critical national infrastructure sectors, along with energy, food, water, government, transportation, communication, emergency services, and finance.

The threat, the alert said, comes particularly from state-aligned groups sympathetic to Russia's invasion of Ukraine and has emerged over the past 18 months. Some groups have stated a desire to achieve "a more destructive impact against Western infrastructure."

Dr. Marsha Quallo-Wright, NCSC Deputy Director for Critical National Infrastructure, said that in the wake of this emerging threat, the NCSC message to CNI sectors is to "take sensible, proportionate steps now to protect themselves." The agency has published heightened threat guidance, which it encourages organisations to follow.

STRENGTHENING THE HUMAN FIREWALL

While the operations and motivations of threat actors may seem extraordinary, the HSE report on the attack on Ireland's health system noted that the attackers used "relatively well-known techniques and software to execute their attack." The attack that cost the health system more than €100 million was made possible by something so "ordinary" today that we tend to brush it off – a phishing email.

Phishing and social engineering, including theft of credentials, are the leading points of entry for malware, followed by unpatched software and wrongly configured systems. In other words, across the UK/Ireland region, employees are easily the healthcare sector's largest attack surface in the sector.

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, tests and tracks vulnerability to phishing in key regions across the globe, using a "PPP" (Phish-prone^{TM} Percentage) rating.

In the United Kingdom and Ireland region, KnowBe4 testing shows that organisations that have 1-240 employees have a PPP of 26.3%. In other words, when employees were tested and sent unsafe "phishing" emails, more than one out of four clicked on the email.

The PPP for organisations with 250-999 employees fared worse, with 28% of employees opening the dangerous emails. In organisations of 1,000 or more, 39.6% were Phish-prone, up from 32.7% last year.

According to Javvad Malik, Lead Security Awareness Advocate at KnowBe4, there are probably many contributing factors to this increase, ranging from hybrid working models to staff turnover. However, despite the initial bleak outlook, the silver lining here is that with frequent security awareness training and simulated phishing, the baseline can be drastically reduced.

UK and Ireland: Phish-prone Percentages, Baseline and After Training

Number of Employees in Organisation	Baseline	After 90 days of training and simulated testing	After 1 year of training and simulated testing
1-249	26.3%	18.5%	6.1%
250-1000	28%	18.1%	8.1%
1000+	39.6%	17.6%	4.9%
Average PPP Across All Organisation Sizes	**35.2%**	**17.8%**	**5.8%**

SUMMARY

Cybersecurity remains a huge concern for the United Kingdom and Ireland, across many fronts. Social engineering is the biggest attack vector, and more needs to be done to promote awareness in organisations and individuals as to the role everyone plays in maintaining security.

With advancements in AI as well as deep fake technologies, we can only imagine how much more sophisticated social engineering attacks will become, therefore increasing the need for all organisations to beef up their defences.

Three key takeaways are:

1. The impact of breaches is proving to be more far-reaching in terms of cost and time than previously thought. Organisations could be paying off the debt of a breach for many years to come. Therefore, stopping attacks becomes an even greater priority.

2. Although some organisations may have a poor starting point, changing the overall security culture and investing in a solid security awareness training strategy can provide a rapid return on investment and significantly reduce risk.

3. Ransomware continues to be a menace, with the geopolitical climate creating an increasingly tricky situation for organisations to stay ahead of.

For futher information, read a case study on:

Action for Children and KnowBe4: Protecting Children's Data

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 is the provider of the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing attacks and enterprise-strength reporting to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | KnowBe4 UK & Ireland York - United Kingdom
Telephone +44 1347 487512 | www.KnowBe4.com | Email: Sales@KnowBe4.com