Article Title:

Understanding the Synnovis Ransomware Attack: Key Insights, Vulnerabilities, and Defence Strategies

**Student ID: 2\*\*\*\*\*1**

November 18, 2024

Module Title: Advance Ethical Hacking (CMP7171)

Module Instructor: Ron Austin

**Understanding the Synnovis Ransomware Attack: Key Insights, Vulnerabilities, and Defence Strategies**

**Introduction**

The world is more digitally connected than ever, allowing real-time information sharing on everything from entertainment and breaking news to global events. Cyber-attacks are no exception. Numerous reports on cyber-attacks targeting different sectors have become a growing concern that we hear about almost daily. The recurring reports of cyber-attacks on media platforms have not only become more visible but have also given hacktivist an effective platform to promote their exploits, by using social media and news outlets to increase their visibility and influence (Coker, 2023).

On the 3rd of June 2024, Synnovis Group, LLP, a pathology company jointly owned by King’s College Hospital NHS Trust, SYNLAB, and Guy’s and St Thomas’ NHS Foundation Trust, experienced a severe ransomware cyberattack. Synnovis, a key provider of blood test processing services for multiple NHS organisations in south-east London, faced widespread service interruptions due to this incident. The cyberattack made headlines because of its significant impact on critical healthcare services, including the cancellation of operations and appointments, as well as the compromise of patients' Personal Health Information (PHI) (NHS, 2024).

**Attack Vector**

In an article published by the BBC (Casey, 2024), it was reported that the ransomware cyberattack on Synnovis Group was executed by the Russian cyber-criminal group known as Qilin. The attackers gained access to Synnovis' network by exploiting a vulnerability in systems used by two National Health Service (NHS) trusts in London. Once inside, the Qilin group deployed ransomware software to encrypt critical information, rendering systems across Synnovis' network inoperable. To exert further pressure for a ransom payment in Bitcoin, the attackers exfiltrated sensitive data, such as patient names, National Health Service (NHS) numbers, dates of birth, and descriptions of blood tests.

**Vulnerability Exploited**

The system vulnerability exploited by the Qilin ransomware group in the Synnovis cyberattack was not explicitly disclosed (Jones, 2024). However, according to (Casey, 2024), the attack succeeded through vulnerabilities in systems used by two NHS trusts in London. (Scroxton, 2024) reported that outdated IT infrastructure at the National Health Service (NHS) created vulnerable entry points, which the attackers exploited. Presumably, the Synnovis attack exploited common tactics frequently used by ransomware groups like Qilin, including exploiting unpatched software, inadequate access controls, or vulnerabilities in network security.

* **Unpatched Software**: The Qilin actors may have taken advantage of an unpatched software vulnerability, also known as a zero-day vulnerability, within the systems of the two NHS trusts. One possibility is that outdated software versions with known vulnerabilities were left unpatched.
* **Access Control Weakness**: The Qilin actors might have compromised the credentials of employees with administrative rights to gain access to Synnovis' network. Negligence by an employee could have contributed to this breach.
* **Weak Network Security Configurations**: The Qilin actors may have exploited weak network security configurations, such as improperly segmented networks, allowing them to move laterally within the two NHS trusts' systems.

**Damage Caused**

In a news and press release on Synnovis' website (Synnovis, 2024), it was revealed that almost all their IT systems were affected, resulting in widespread disruptions to pathology services. The cyberattack led to the encryption of critical data, immediately impacting patients relying on NHS services at King’s College Hospital NHS Foundation Trust, Guy’s and St Thomas’, the South London and Maudsley NHS Foundation Trust, as well as GP services across the boroughs of Lambeth, Lewisham, Greenwich Bromley, Southwark, and Bexley. This incident forced Synnovis to revert to paper-based and manual processes for analysing medical samples, significantly reducing their operational capacity and delaying diagnostic services.

In an article published by the BBC (Tidy, 2024), it was reported that the Qilin threat actors shared nearly 400GB of private information acquired on their darknet website. Samples of the data reviewed by the BBC’s cyber correspondent include descriptions of blood tests, patient names, dates of birth, and NHS numbers. The cyberattack disrupted over **3,000 GP appointments** and more than **800 planned operations**. Critical services, including **cancer treatments** and **organ transplants**, were also affected. Furthermore, according to (Casey,2024), the data published by the Qilin group also included business account spreadsheets containing financial arrangements between Synnovis, GP services, and other hospitals.

In another article published by ComputerWeekly (Skelton, 2024), it was reported that during the second week following the attack, between June 10th and 16th, 2024, more than 1,294 outpatient appointments and 320 scheduled operations were postponed at Guy’s and St Thomas’ NHS Foundation Trust and King’s College Hospital NHS Foundation Trust. Overall, the cyberattack led to the cancellation of more than **1,134 operations**.

According to a news report by (Pilditch, 2024), it was revealed that the Qilin Russian threat group attempted to extort over **£40 million** after infiltrating Synnovis systems. The incident is now considered one of the **largest cyberattacks in the UK**, affecting services valued at over **£1 billion** that are essential for the smooth functioning of the NHS.

A screenshot of a computer

Description automatically generated A screenshot from Qilin’s darknet leak site displaying information related to a data breach involving Synnovis (Tidy, 2024).

In the immediate aftermath of the Synnovis cyberattack, delays in medical test processing created a significant backlog, forcing healthcare providers to prioritise urgent cases, while non-urgent services faced further delays (HealthManagement.org, 2024). According to an NHS news release (NHS, 2024), Synnovis had ensured that unprocessed test samples were safely stored in their labs. However, due to the time that had since passed, some of these samples became unsuitable for analysis and had to be discarded. Furthermore, (Shekhar, 2024) reported that the NHS Blood and Transplant service urged individuals with O-negative and O-positive blood types to donate blood as soon as possible, to mitigate the impact of disrupted blood matching tests across London hospitals.

In the long-term aftermath of the Synnovis cyberattack, vulnerabilities in the NHS supply chain were exposed, leading to significant disruptions in General Practitioner (GP) appointments and planned operations (Lee, 2024). Synnovis and its partners could face regulatory fines if investigations reveal non-compliance with data protection laws, such as the UK Data Protection Act 2018 or General Data Protection Regulation (GDPR). Additionally, the exposure of financial arrangements and patients' Protected Health Information (PHI) could erode trust in the healthcare system, potentially resulting in lawsuits. This high-profile attack has significantly damaged the reputation of Synnovis and associated NHS trusts (HealthManagement.org, 2024).

**Mitigations and Defences**

According to an article by (Puglia, 2024), healthcare providers are custodians of vast amounts of highly confidential information, making them prime targets for cybercriminals. This data can be used as a powerful tool for coercion. Ciaran Martin, former head of the National Cyber Security Centre (NCSC), issued a stark warning to the National Health Service (NHS), urging them to upgrade their computer systems, as they remain highly vulnerable to future cyber threats. To regain trust, both Synnovis and the NHS must invest heavily in upgrading IT infrastructure and technologies to prevent future incidents.

In an article by (Sharp, 2024), it was revealed that the Synnovis cyberattack could have been avoided by taking proactive measures such as comprehensive employee training on cyber hygiene, stringent access controls, timely software updates, and investment in advanced threat detection systems. Ultimately, focusing on cybersecurity is more than a technical requirement; it is essential for preserving public trust in healthcare digital systems.

Furthermore, (Puglia, 2024) highlighted several key strategies to strengthen healthcare defences against cyber incidents like the Synnovis attack.

* **Implement basic cybersecurity measures** that include robust endpoint defences, regular software updates, and routine backups. It is also essential to adhere to established frameworks such as GDPR, NIST, and NIS2.
* **Develop well-defined processes and playbooks** that include detailed incident response plans and standard operating procedures to ensure prompt, precise, and effective responses to security breaches.
* **Perform regular vulnerability scans and penetration tests** across all healthcare IT infrastructures to uncover potential security gaps.
* **Invest in cybersecurity education and training** to equip healthcare staff with the knowledge and tools to recognise and counter potential threats.

According to an article by (Uberoi, 2024), the ransomware attack on Synnovis highlights the urgent need for effective cybersecurity measures across the healthcare sector in the United Kingdom. The incident demonstrates how such attacks can paralyse essential health services, causing fear and chaos among patients and providers. A key takeaway is the importance of **scrutinising third-party vendor security**. This can be achieved by engaging cybersecurity consultants to regularly review supply chain security and third-party agreements, ensuring vulnerabilities are consistently identified and addressed.

Additionally, (Lee, 2024) emphasises mitigation steps that the NHS and other public sector healthcare providers should adopt to protect against supply chain risks:

* **Continuous Monitoring and Improvement**: Regularly assess cyber hygiene for both your organization and suppliers, implement multi-factor authentication (MFA), and secure systems by design.
* **Select Trusted Suppliers**: Partner with suppliers that adhere to robust security practices and secure-by-design principles.
* **Proactive Threat Detection and Response**: Engage in proactive threat hunting and establish comprehensive incident response plans to ensure swift recovery from breaches.

**Conclusion**

The ransomware attack on Synnovis Healthcare systems revealed significant security weaknesses within the UK healthcare sector. This article examines the attack in detail, including the methods used, the vulnerabilities exploited, the damage caused, and the steps needed to mitigate such risks. Preventing such ransomware attacks from recurring requires proactive measures like regular third-party security audits, ongoing staff training, and targeted investments in advanced cybersecurity technologies to safeguard healthcare IT infrastructure against future threats.

Healthcare providers like Synnovis must consistently evaluate and strengthen their cybersecurity strategies by assessing current defenses, prioritizing timely updates, and ensuring rigorous monitoring of third-party security checks to protect critical digital healthcare services.

**Reference**

1. Casey, I. (2024) NHS England confirm patient data stolen in Cyber Attack, BBC News. Available at: <https://www.bbc.co.uk/news/articles/c9777v4m8zdo> [Accessed: 18 October 2024].
2. Coker, J. (2023) Cyber-attacks in the media industry making headlines, Infosecurity Magazine. Available at: <https://www.infosecurity-magazine.com/news-features/cyber-attacks-media-industry/> [Accessed: 18 October 2024].
3. [HealthManagement.org] (2024) Qilin ransomware attack on Synnovis led to 6000+ appointments cancelled, HealthManagement. Available at: <https://healthmanagement.org/c/cybersecurity/News/qilin-ransomware-attack-on-synnovis-led-to-6000-appointments-cancelled> [Accessed: 19 October 2024].
4. Jones, C. (2024) Qilin: We knew our Synnovis attack would cause a healthcare crisis at London Hospitals, The Register. Available at: <https://www.theregister.com/AMP/2024/06/20/qilin_our_plan_was_to/> [Accessed: 18 November 2024].
5. Lee, J. (2024) Synnovis cyberattack highlights vulnerability of NHS Supply Chains, Trend Micro. Available at: <https://www.trendmicro.com/en_gb/ciso/24/f/synnovis-cyberattack-highlights-vulnerability-of-nhs-supply-chains.html> [Accessed: 19 October 2024].
6. NHS, N. (2024) Synnovis cyber attack – statement from NHS England, NHS choices. Available at: <https://www.england.nhs.uk/2024/06/synnovis-cyber-attack-statement-from-nhs-england/> [Accessed: 18 October 2024].
7. NHS, N. (2024a) Synnovis cyber attack – statement from NHS England, NHS choices. Available at: <https://www.england.nhs.uk/2024/06/synnovis-cyber-attack-statement-from-nhs-england/> [Accessed: 19 October 2024].
8. Pilditch, D. (2024) Russian gang demands £40m ransom from NHS, threatens to publish ‘sensitive’ info, Express.co.uk. Available at: <https://www.express.co.uk/news/uk/1914004/russian-gang-nhs-ransom-sensitive-details> [Accessed: 19 October 2024].
9. Puglia, M. (2024) Protecting the NHS: Lessons from the synnovis attack, SC Media UK. Available at: <https://insight.scmagazineuk.com/protecting-the-nhs-lessons-from-the-synnovis-attack> [Accessed: 19 October 2024].
10. Scroxton, A. (2024) Synnovis attack highlights degraded, outdated state of NHS IT: Computer Weekly, ComputerWeekly.com. Available at: <https://www.computerweekly.com/news/366592754/Synnovis-attack-highlights-degraded-outdated-state-of-NHS-IT> [Accessed: 18 October 2024].
11. Sharp, S. (2024) What we can learn from the NHS Cyber Attack, Sharp. Available at: <https://www.sharp.co.uk/news-and-events/blog/what-we-can-learn-from-the-nhs-cyber-attack> [Accessed: 19 October 2024].
12. Shekhar, S. (2024) NHS urgently calls for O blood-type donations after London hospitals hit by Ransomware Attack - CloudSEK News, CloudSEK News - Latest Trends from Cybersecurity are here. Available at: <https://news.cloudsek.com/2024/06/nhs-urgently-calls-for-o-blood-type-donations-after-london-hospitals-hit-by-ransomware-attack/> [Accessed: 19 October 2024].
13. Skelton, S.K. (2024) Qilin Ransomware Gang publishes stolen NHS Data Online: Computer Weekly, ComputerWeekly.com. Available at: <https://www.computerweekly.com/news/366589583/Qilin-ransomware-gang-publishes-stolen-NHS-data-online> [Accessed: 19 October 2024].
14. Synnovis, S. (2024) Update on cyber incident: 01 July 2024, Synnovis. Available at: <https://www.synnovis.co.uk/news-and-press/cyberattack-update-01-july-2024> [Accessed: 19 October 2024].
15. Tidy, J. (2024) London hospitals hackers publish stolen Blood Test Data, BBC News. Available at: <https://www.bbc.co.uk/news/articles/c9ww90j9dj8o> [Accessed: 19 October 2024].
16. Uberoi, A. (2024) How a ransomware attack on Synnovis led to Chaos at NHS UK: A Timeline, Home - Cyber Security Training. Available at: <https://www.cm-alliance.com/cybersecurity-blog/how-a-ransomware-attack-on-synnovis-led-to-chaos-at-nhs-uk-a-timeline> [Accessed: 19 October 2024].