The timeline of the Incident is broken down, in a chronological order of events from oldest to newest, under the following headings:

- Timeline prior to the Incident;
- Timeline prior to the Incident and the response at Hospital A, a Specialty Hospital ("Hospital C") and the DoH;
- Timeline of the Incident and the response at the HSE on 14 May 2021;
- Timeline post the Incident and the response and recovery at the HSE.

Timeline prior to the Incident

This section provides a timeline of what the Attacker did while present on HSE systems prior to the execution of the Conti ransomware, including the actions taken by the HSE in response to antivirus detections.

On 18 March 2021, a HSE staff member interacted with a malicious Microsoft Office Excel file attached to a phishing email. This resulted in a Malware infection of the Patient Zero Workstation.

On 23 March 2021, the Attacker created a persistence mechanism on the Patient Zero Workstation to ensure the Attacker retained access to the HSE's environment if the Patient Zero Workstation was rebooted or powered off.

On 31 March 2021, the HSE's antivirus software detected the execution of two software tools commonly used by ransomware groups: Cobalt Strike and Mimikatz, on the Patient Zero Workstation. The antivirus software was set to monitor mode so it did not block the malicious commands.

The HSE's Incident Response provider identified no significant Attacker activity between 1 April 2021 and 6 May 2021.

On 7 May 2021, the Attacker installed additional persistent Malware on the Patient Zero Workstation, conducted AD and domain reconnaissance, and compromised further systems within the HSE. The Attacker was identified as using highly privileged accounts for the first time.

On 8 May 2021, first identified evidence of the Attacker compromising systems within Hospital K and Hospital D.

On 9 May 2021, first identified evidence of the Attacker compromising a system within Hospital J.

On 10 May 2021, first identified evidence of the Attacker compromising systems within Hospital C and Hospital L. Hospital C's antivirus software detected Cobalt Strike on two systems but failed to quarantine the malicious files.

On 11 May 2021, first identified evidence of the Attacker compromising a system within Hospital A. After numerous failed logon attempts, the Attacker likely exploited an unpatched known vulnerability, [redacted] , to gain access to the domain. Hospital A's antivirus software detected and deleted the malware on several systems.

On 12 May 2021, first identified evidence of the Attacker compromising a system within Hospital B. The Attacker was identified browsing folders, opening files, creating archives and accessing or attempting to access file sharing websites on systems within Hospital A, Hospital B and Hospital D. The HSE's cybersecurity solutions provider emailed the HSE's Security Operations team to escalate alerts on two servers and requested a full on demand scan be completed.[51] The HSE responded on the same day to confirm the scans had been executed.[52]

On 13 May 2021, first identified evidence of the Attacker browsing folders, opening files, creating archives and accessing a file sharing website on systems within the HSE. The HSE's cybersecurity solutions provider emailed the HSE's Security Operations team and outlined that there were unhandled threat events since 7 May 2021 on at least 16 systems; the HSE Security Operations team requested that the Server team restart servers.

On 14 May 2021, the Attacker executed ransomware on systems within the HSE, Hospital C, Hospital K, Hospital D, Hospital L, Hospital J and Hospital B.

Timeline prior to the Incident and the response at Hospital A, Hospital C and the DoH

Two voluntary hospitals, Hospital A and Hospital C, identified suspicious activity prior to the Incident. In addition, the DoH, a third party to the HSE's environment, successfully acted on a detection of the Attacker which prevented the execution of the Conti ransomware across the vast majority of the DoH.[53]

[51] Email with subject RE: Threat not handled, 13 May 2021

[52] Email with subject RE: Threat not handled, 13 May 2021

[53] https://www.gov.ie/en/news/d48b2-a-note-for-the-public-on-the-recent-cyber-attack-on-the-department-of-health/

The following timeline describes the key activities at Hospital A, Hospital C and the DoH prior to the Incident.

On 10 May 2021, Hospital C asked Hospital C's cybersecurity solutions provider whether they should be concerned about Cobalt Strike alerts. They were advised by Hospital C's cybersecurity solutions provider that since the threat had been remediated by their antivirus software, their risk was low.[54] Hospital C did not initiate a cyber incident response investigation.

On 12 May 2021, Hospital A engaged Hospital A's Incident Response provider to investigate alerts of malicious activity. They reset passwords for 4,500 accounts[55] and made firewall configuration changes[56] to contain the activity, and made contact with the HSE to request information on two IP addresses.[57] To further contain the activity, Hospital A utilised their existing security tooling across their environment.

On 13 May 2021, the HSE identified the IP addresses reported by Hospital A related to two servers within the HSE's [redacted] domain. The HSE conducted an investigation into the activity identified by Hospital A and incorrectly concluded in an email between the HSE teams[58] that the suspicious activity originated from Hospital A, rather than the other way round.

On 13 May 2021, DoH's cybersecurity solutions provider[59] alerted the DoH to a potential attack on their network. DoH contacted the NCSC and engaged DoH's IR Provider[60] who installed endpoint detection and response ("EDR") security tooling on the majority of their systems. These actions blocked the execution of the Conti ransomware across the vast majority of the DoH's infrastructure, including critical and data servers.

Timeline of the Incident and the response at the HSE on 14 May

The following timeline describes the key activities at the HSE on the day of the Incident, 14 May 2021.

On 14 May 2021 at approximately 01:00, the Attacker executed ransomware on systems within the HSE, Hospital C, Hospital K, Hospital D, Hospital L, Hospital J and Hospital B.

At 02:50, the HSE's national service desk received the first of multiple reports from hospitals of multiple systems being unavailable as a result of the Incident.[61]

At 04:36, the HSE identified malicious encryption on multiple servers in the HSE's data centre.[62]

At 04:41, due to the widespread reports of encryption, and the presence of ransomware in the HSE's data centre, the HSE invoked their Critical Incident Process.

At 05:10, an initial critical incident call was held between network and infrastructure subject matter experts ("SMEs"). Decisions were taken to contain the threat including removing all internal and external connectivity for the NHN, and to begin engagement with voluntary hospitals.

At approximately 06:00, the CEO notified the Board of the Incident.

At 07:00, RTÉ News released a news bulletin on the Incident. Shortly afterwards, the CEO notified the EMT and National Crisis Management Team ("NCMT").

At 07:28, HSE Live, the HSE contact centre, issued a tweet notifying the public of an incident and the shutdown of services. Shortly afterwards, the HSE's Data Protection Officer ("DPO") rang the office of the DPC.

At 08:30, the first meeting of the NCMT was held.[63]

At 09:22, The HSE informed Primary Care Reimbursement Service ("PCRS") of the cyber incident and PCRS decided to shut down their systems.

At 10:00, it was reported during a Major Incident ("MI") call that the HSE had initiated a preventative lockdown strategy to contain the impact of the attack by switching off all systems within the HSE. The Garda National Cyber Crime Bureau, Interpol and the NCSC were brought in to support the response.

At 10:30, with the support of the NCSC, the HSE engaged the HSE's Incident Response provider to provide incident response services for the HSE. The HSE also engaged others such as Third Party C, Third Party A, Third Party D, Third Party B and Third Party E to provide tactical incident response and

[54] Logging call with Hospital C's cybersecurity solutions provider on 10/05/2021 17:06
[55] Information gathered from an interview with Hospital A
[56] Information gathered from an interview with Hospital A
[57] Email with subject: Recognise these addresses??, May 2021
[58] Email with subject RE: Summary, May 2021
[59] Information gathered from an interview with the NCSC
[60] Information gathered from an interview with the NCSC

[61] CIM 2 - Conti Ransomware Incident coordination Form Ver 2.1(2), 2021
[62] CIM 2 - Conti Ransomware Incident coordination Form Ver 2.1(2), 2021
[63] Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021

recovery support.

At 12:00, it was reported that a Malware sample was sent to a threat research organisation for analysis.

At 14:00, it was reported that the HSE sent a text message to all HSE work devices notifying staff members of a ransomware attack impacting the HSE, and voluntary and statutory hospitals.

At 16:30, it was reported that the HSE's Incident Response provider began deployment of their endpoint security monitoring software to gain visibility of the HSE's environment and enable a full forensic investigation of systems within the HSE. The MI meeting established a once daily operating rhythm.

Late on the evening of 14 May 2021, the HSE informed the DPC about the Incident.[64]

Timeline post the Incident and the response and recovery at the HSE

The following timeline describes the key activities post the Incident from a response and recovery perspective at the HSE.

Response

On 15 May 2021, the HSE senior management set up a war room at a third party's office building on Molesworth Street.[65] Initial workstreams were set up to enable a coordinated response and recovery from the Incident. The HSE's DPO issued a formal notification to[66] the DPC about the Incident and the HSE's Incident Response provider was engaged by voluntary hospitals to provide incident response support and questionnaires were sent to the voluntary hospitals to get an understanding of which entities were compromised. The HSE's senior leadership team were provided with clean Microsoft [redacted] mailboxes to allow for communication during the initial stages of the response, and a mailbox[67] was set up to deal with issues relating to the ransomware attack.

From 17 May 2021, the HSE coordinated daily incident management meetings between all parties supporting the response to the Incident to ensure that there was a forum to collect and share information. The OoCIO's Communications team also established a twice daily meeting rhythm. These forums were used to share information about the response and to communicate new processes to the rest of the business, in an effort to move to a recovery phase, and to keep members of the public up to date on the response to the Incident. Key response activities over the following days included, but were not limited to:

- An initial list of priority applications was identified, the [redacted] AD domain was recovered which allowed the HSE to build their foundational IT infrastructure;
- A 'go-to-green' process was proposed for recovering systems and was communicated to internal stakeholders for consideration;
- A social media monitoring system Talk Walker was set up to scan the web for leaked patient data;
- The first call between the HSE and the Defence Forces was held to discuss support requirements;
- The application NIMIS was recovered with a Model 4 Hospital[68] being the first hospital with NIMIS to go live.

It was also within this timeframe that the CIO, Head of Occupational Health and the National Ambulance Service identified a risk of staff burnout. It was at this point, Occupational Health were requested to attend the war room to check responders' health, and staff rotas were implemented.[69]

From 19 May 2021, key response activities included, but were not limited to:

- The first clean laptops were distributed to a select number of HSE staff members and HSE staff members were given derogation to use personal emails and devices for crisis communications;
- The initial list of priority applications was reprioritised and informed by clinical priorities, as dictated by the clinical and integrated governance structure that was initially set up to guide the operational response and in an effort to enable a two way flow of information; and
- The HSE established a Legal and Data workstream to oversee the appointment and subsequent work of their legal advisers and to support the work of the DPO in coordinating the HSE's data protection investigation, engagement with An Garda Síochána and subsequent reporting to the DPC.[70]

Five days into the response, the lack of integrated programme management was recognised as a risk by

[64] DPC Report 15 July 2021

[65] Programme RAID Log, 2021

[66] Original DPC Notification_May 2021

[67] Minutes of Cyber Attack MI Meeting 10 am - 15052021

[68] NIMIS RE-ENABLEMENT TRACKER CYBER ATTACK RECOVERY, 2021

[69] Programme RAID Log

[70] Document subject to legal privilege

the HSE. This led to a request for assistance from the Defence Forces who established defined Information Management processes which were scalable and agile and could cope with the complexity of a cyber crisis.

On 20 May 2021, the Defence Forces attended Molesworth Street for further discussions around the level of support that was required by the HSE during the response and recovery phases of the Incident. It was reported that on the same day, the Attacker posted a link to a software application that would decrypt files encrypted by the Conti ransomware during the Incident. The HSE's Incident Response provider, on behalf of the HSE, validated that the decryption software worked, reverse engineered its capabilities, and produced a new, more stable decryption software that was also supported by them.[71] The HSE also secured a High Court injunction[72] restraining any sharing, processing, selling or publishing of data stolen from its computer systems.

On 21 May 2021, the SCA recognised the enormous impact the Incident had on doctors, nurses, midwives and allied healthcare professionals, on the provision of health and social care services and clinical care within the HSE.[73] As these professionals were obliged to practice without the usual back up of essential systems, clinical imaging and other diagnostic-related results to assist in their assessment and treatment of patients, the SCA confirmed these professionals were fully covered by the Clinical Indemnity Scheme in relation to their ongoing clinical decision-making, in the absence of such clinical support. Separately, the physical SitCen was also established in CityWest.[74]

On the same day, the availability of the decryption key allowed the HSE to create efficiencies during the recovery process by deploying a decryptor across the environment to decrypt files on impacted systems. This enabled HSE to scale their recovery effort and make the overall process more efficient.

Recovery

From 22 May 2021 onward, the HSE moved from the response phase into the recovery phase, where they focused their efforts on decrypting systems, cleansing workstations, restoring systems and the recovery of applications.

On 24 May 2021, the HSE's Incident Response provider and the HSE released their 'go-to-green' processes to internal stakeholders, to ensure the secure recovery of systems, reduce the risk of further ransomware attacks, and to provide guidance in recovering systems. The HSE's Incident Response provider and the HSE developed requirements that every system within the HSE, voluntary hospitals and CHOs had to meet before being able to rejoin the network, and for organisations to be reconnected back to the NHN.

Figure 9: Summary of progress over the following three months

Duration	Progress made
One month after the Incident	The HSE had decrypted 47% of servers and fully restored 48% of Acute applications, 40% of Community Services applications and 64% of business services applications[75].
Two months after the Incident	This increased to 94% of servers decrypted and fully restored, 85% of Acute applications, 94% of Community Services applications and 79% of business services applications[76].
Three months after the Incident	The HSE reported that 100% of servers were considered decrypted and they had fully restored 95% of Acute applications, 98% of Community Services applications and 91% of business services applications[77].

By 21 September 2021, the HSE had recovered 1,075 applications, out of a total of 1,087 applications.[78] Finally, at the time of issuing this report the HSE had notified the DPC in relation to the Incident, however, they have not made any data subject notification for personal data exposure or exfiltration, however, they continue to work closely with the DPC in relation to this matter.[79]

[71] HSE's Incident Response provider, Intrusion Investigation Report

[72] https://www.hse.ie/eng/services/publications/order-perfected-20-may-2021.pdf

[73] https://stateclaims.ie/uploads/publications/State-Indemnity-Guidance_IT-cyber-attack-on-the-health-and-social-care-sector-from-14-may-2021_21.5.21_2021-05-21-150239_tytw.pdf

[74] Conti Cyber Response NCMT Structures Governance and Admin V1.10, 31 May 2021

[75] SITCEN SITUATION REPORT, 18:30 14 June 2021

[76] Weekly Brief, 20 July 2021

[77] Weekly Brief, 21 September 2021

[78] Weekly Brief, 21 September 2021

[79] Document subject to legal privilege