An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

NCSC:IE

RANSOMWARE ATTACK

IMPACT > RECOVERY > AFTERMATH

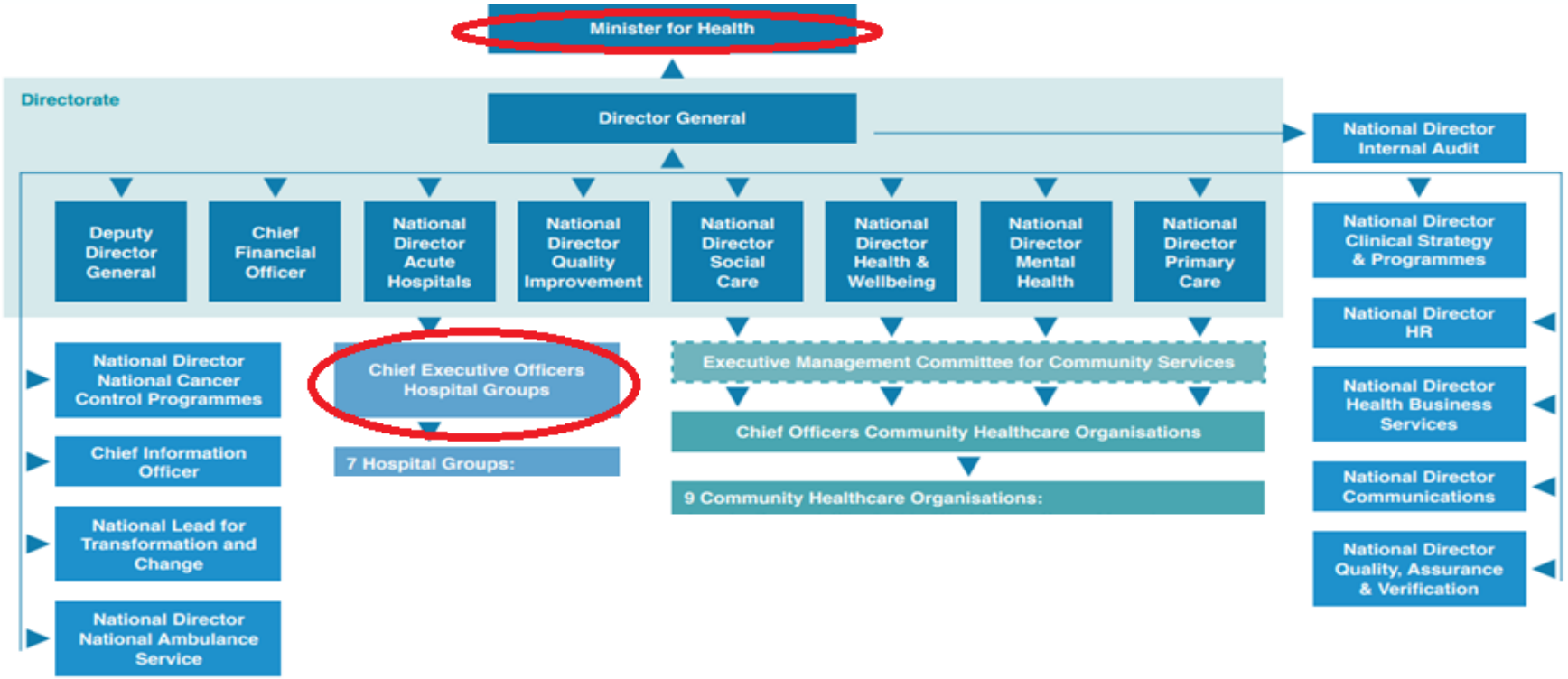
TLP:GREEN

About Us

- Planning for and responding to cyber incidents
- Working with critical national infrastructure to improve resilience of Services
- National Competent Authority for Network and Information Security Directive

Public Health Services

- Budget: 19.45B pa.
- ED attendances: 1.1 million
- 54 Acute Hospitals
- 130,000 Employees
- 70,000 IT devices
- 4,000 locations
- Day Cases Procedures: 920,000
- Inpatient Hospital discharges: 560,000


Minister for Health
Directorate
Director General
National Director Internal Audit
Deputy Director General
Chief Financial Officer
National Director Acute Hospitals
National Director Quality Improvement
National Director Social Care
National Director Health & Wellbeing
National Director Mental Health
National Director Primary Care
National Director Clinical Strategy & Programmes
National Director HR
National Director Health Business Services
National Director Communications
National Director Quality, Assurance & Verification
National Director National Cancer Control Programmes
Chief Information Officer
National Lead for Transformation and Change
National Director National Ambulance Service
Chief Executive Officers Hospital Groups
7 Hospital Groups:
Executive Management Committee for Community Services
Chief Officers Community Healthcare Organisations
9 Community Healthcare Organisations:

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

I – Ransomware Deployment

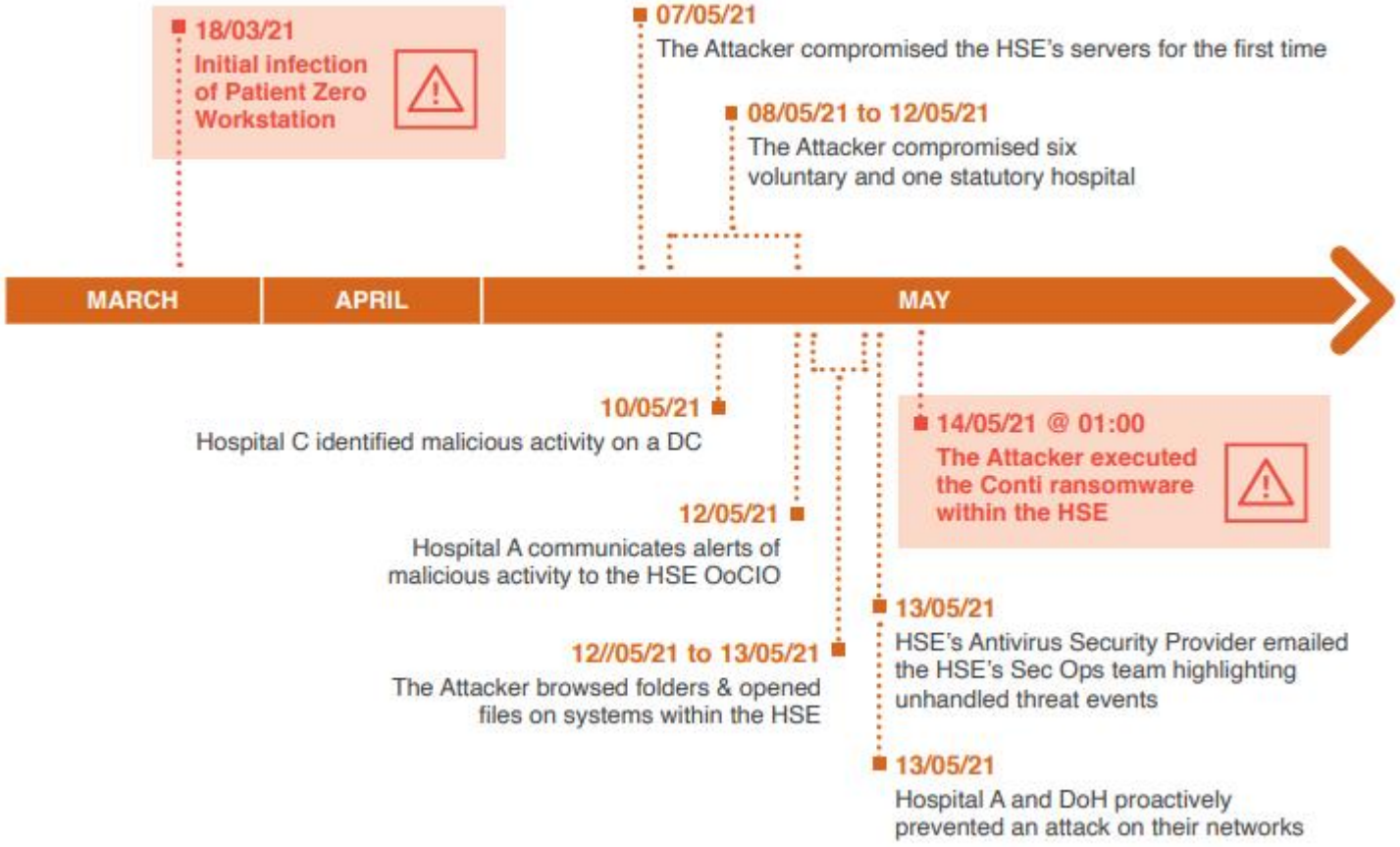
14.05.2021

SR:05:16
SS:21:28

NATIONAL CYBER SECURITY CENTRE

TLP:GREEN

- At approx. 07:00 hrs on 14th May 2021, the NCSC was made aware of a significant incident affecting HSE systems. Initial reports indicated a human-operated 'Conti' ransomware attack that had severely disabled a number of systems
- **Containment:** The majority of other HSE systems were isolated
- Hospitals and healthcare providers mostly reverted back to paper records.
- Head of HSE - "Posed a serious clinical risk"
- A major incident response process was invoked


18/03/21
Initial infection of Patient Zero Workstation
07/05/21
The Attacker compromised the HSE's servers for the first time
08/05/21 to 12/05/21
The Attacker compromised six voluntary and one statutory hospital
MARCH
APRIL
MAY
10/05/21
Hospital C identified malicious activity on a DC
12/05/21
Hospital A communicates alerts of malicious activity to the HSE OoCIO
12//05/21 to 13/05/21
The Attacker browsed folders & opened files on systems within the HSE
14/05/21 @ 01:00
The Attacker executed the Conti ransomware within the HSE
13/05/21
HSE's Antivirus Security Provider emailed the HSE's Sec Ops team highlighting unhandled threat events
13/05/21
Hospital A and DoH proactively prevented an attack on their networks

- Obvious and immediate impact - Morning news carried story of hospitals turning away patients
- NCSC provided initial messaging to the “centre” - NCSC is engaged with victim and coordinating IR
- Position on ransom payment taken immediately
- Series of Political briefings throughout weekend and early into the next week

Patient Impact

- Emergency Departments
- Radiology
- Pathology/Laboratories
- Cancellations in elective appointments
- Primary Care
- Screening Services
- Video Call appointments

Clinical Principles

- Protect **unscheduled** and **urgent** care
- Reinstate services in a manner that does **not** threaten recovery or compromise the safe follow-up of patients seen during the cyberattack
- **Support** Health staff and acknowledge the risks to them of operating in an environment where we begin to recover the usual information systems support

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Threat Actors

NATIONAL CYBER SECURITY CENTRE

TLP:GREEN

Hello, this is ContiLocker Team.
Please, introduce yourself (Company name and your position) and we'll provide all necessary information.
Sometimes our staff is busy, but we will reply as soon as possible.
Be in touch, thank you.
yesterday

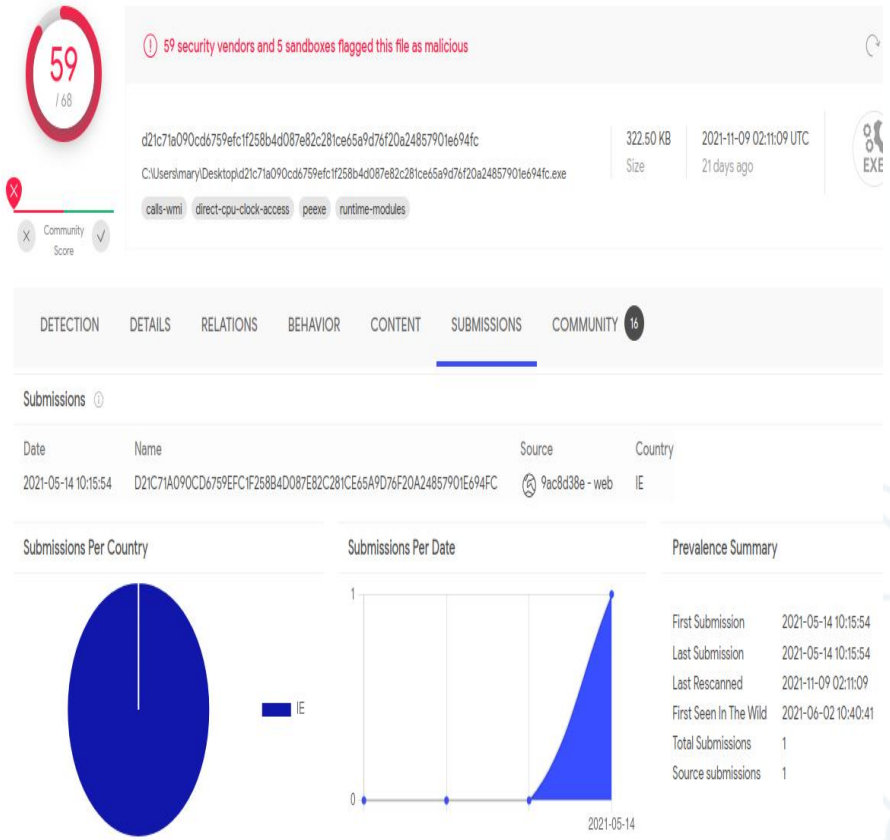
hello
yesterday

my machine isn't working and i was asked to contact you in a file
yesterday

can you help?
yesterday

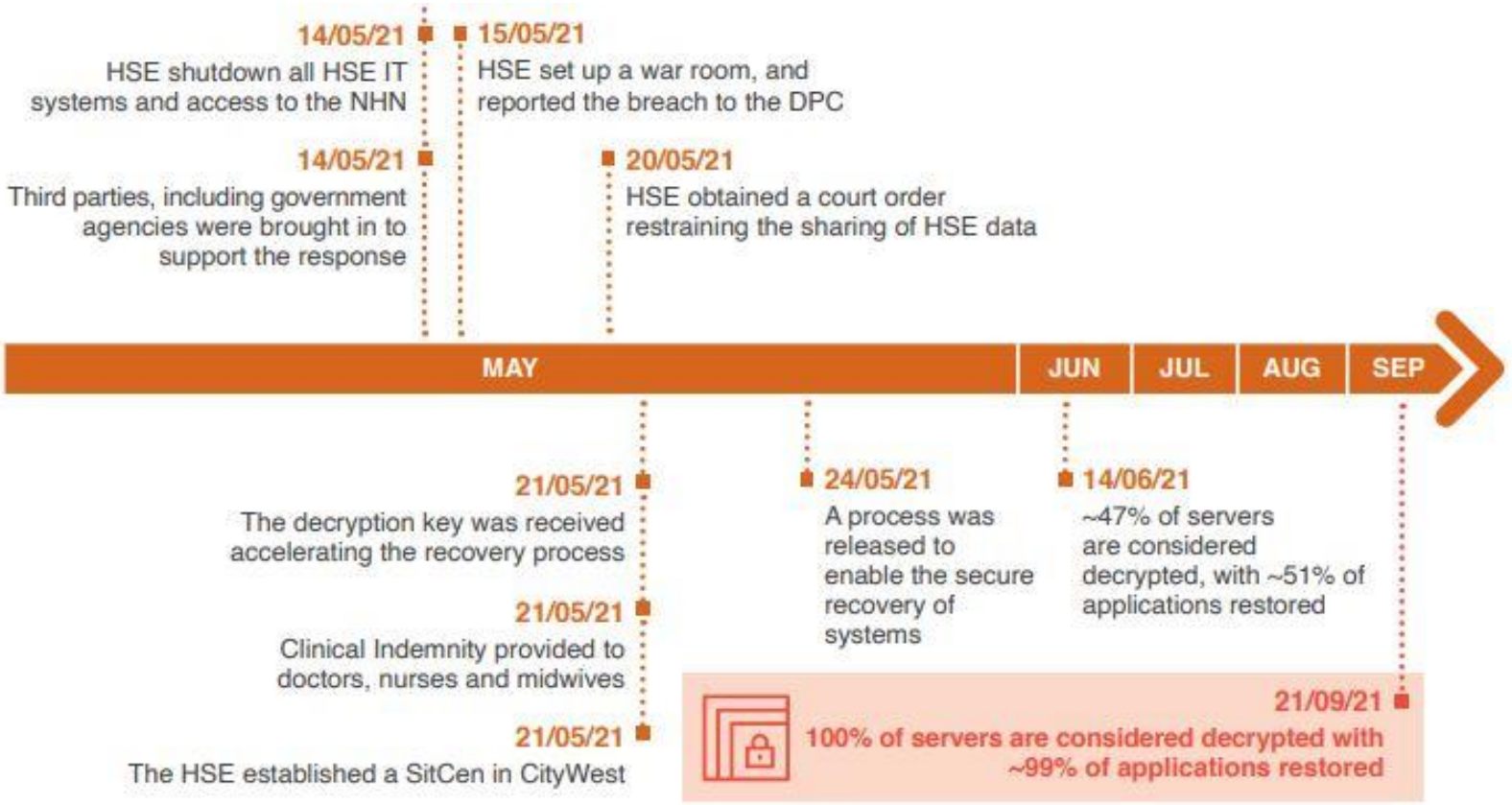
As you already know, we infiltrated your network and stayed in it for more than 2 weeks(enough to study all your documentation), encrypted your file servers, sql servers, downloaded all important information with a total weight of more than 700 GB: personal data of patients(home addresses, phone numbers of the contract), employees (home addresses, employment contracts, scans of personal documents, phone numbers), contracts, customer bases, consolidated financial statements, payroll, settlements with partners, bank statements.
The good news is that we are businessmen. We want to receive ransom for everything that needs to be kept secret, and don't want to ruin your business
The amount at which we are ready to meet you and keep everything as collateral is $ 19,999,000.
yesterday

how do i know you have any data?
yesterday



An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

II - Recovery


14/05/21
HSE shutdown all HSE IT systems and access to the NHN
15/05/21
HSE set up a war room, and reported the breach to the DPC
14/05/21
Third parties, including government agencies were brought in to support the response
20/05/21
HSE obtained a court order restraining the sharing of HSE data
MAY
JUN
JUL
AUG
SEP
21/05/21
The decryption key was received accelerating the recovery process
21/05/21
Clinical Indemnity provided to doctors, nurses and midwives
21/05/21
The HSE established a SitCen in CityWest
24/05/21
A process was released to enable the secure recovery of systems
14/06/21
~47% of servers are considered decrypted, with ~51% of applications restored
21/09/21
100% of servers are considered decrypted with ~99% of applications restored

Release of the Key

21 May 2021: The threat actors released a link to a decryption tool on their Conti recovery website.

Upon receipt of the de-cryptor from the TA, NCSC and partners had to establish if it was genuine and if it potentially contained any further malicious payload

The de-cryptor itself was not suitable but the decryption code was valid

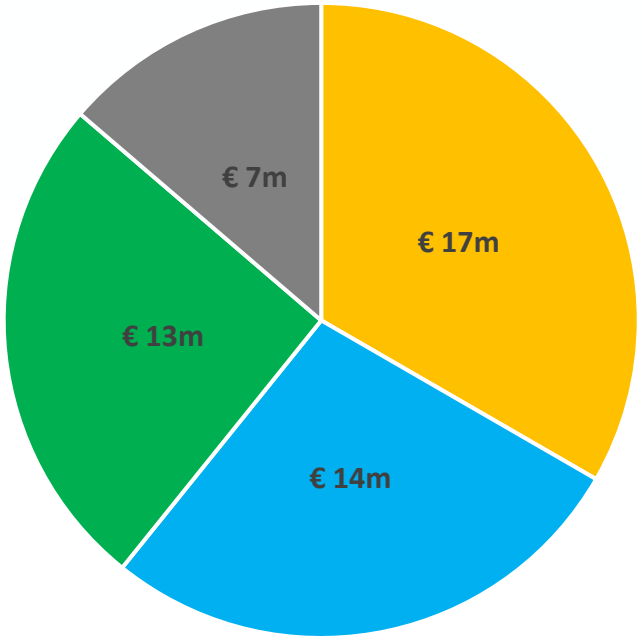
Progress steady but slow as the HSE continued to rebuild and restore services

- The Investigation into the incident continued with artefacts and TTPs continuing to be discovered
- NSCE:IE informed National/International colleagues on the evolving incident
- TLP: AMBER advisories were issued with updated IOC list
- TLP: WHITE Advisories issued

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

III - Aftermath

Costs of the Cyber Attack 2021



PwC key recommendations, September 2021

Area	Focus of review	Key recommendations
Overall	Transformational change[a]	22
Focus area 1	Technical investigation and response	15
Focus area 2[b]	Organisation wide preparedness and strategic response	24
Focus area 3	Preparedness of the HSE to manage cyber risks	22

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Conclusion

- Roles & Responsibilities
- Communication
- Test, Test, Test
- Workarounds

- Understand your environment
- Control Assurance
- Security Culture

References

- *https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-executive-summary.pdf*
- *https://www.audit.gov.ie/en/find-report/publications/2022/12-financial-impact-of-cyber-security-attack.pdf*