HHS: Conti ransomware encrypted 80% of Ireland's HSE IT systems

Sergiu Gatlan

By
Sergiu Gatlan

- February 4, 2022
- 11:01 AM
- 0

A threat brief published by the US Department of Health and Human Services (HHS) on Thursday paints a grim picture of how Ireland's health service, the HSE, was overwhelmed and had 80% of its systems encrypted during last year's Conti ransomware attack.

This led to severe disruptions of healthcare services throughout Ireland and exposed the information of thousands of Irish people who received COVID-19 vaccines before the attack after roughly 700 GB of data (including protected health information) was stolen from HSE's network and sent to attackers' servers.

The short incident report [PDF], based on a PwC independent post-incident review [PDF] commissioned by the Board of the HSE in June 2021, reveals that the impact of this attack on HSE's IT environment was primarily caused by the organization's lack of preparedness to deal with such an incident.

"The HSE did not have a single responsible owner for cybersecurity, at senior executive or management level at the time of the incident. There was no dedicated committee that provided direction and oversight of cybersecurity and the activities required to reduce the HSE's cyber risk exposure," the HHS Cybersecurity Program said.

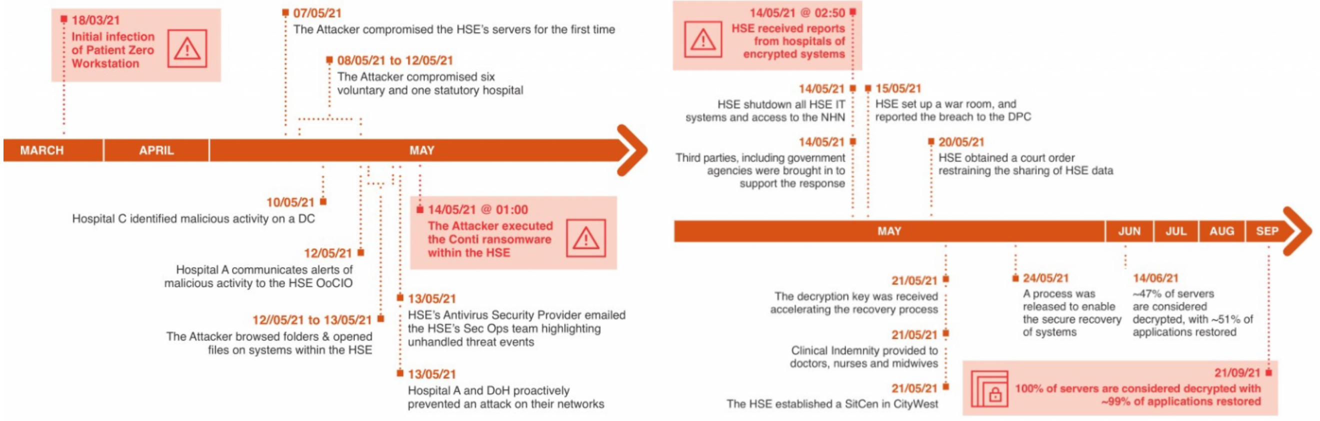
"The lack of a cybersecurity forum in the HSE hindered the discussion and documentation of granular cyber risks, as well as the abilities to identify and deliver mitigating controls. The HSE did not have a centralized cybersecurity function that managed cybersecurity risk and controls."

To top it all off, the HSE also had no security monitoring solutions deployed to help investigate and respond to security threats detected across its IT environment.

This led to a lack of response to Conti operators' malicious activity, which was far from stealthy, seeing that Cobalt Strike beacons deployed on multiple HSE servers starting with May 7, 2021, were detected by endpoint antivirus solutions, with the alerts being ignored.

"The impact of the ransomware on the IT environment was reported by the HSE's management to lead to 80% encryption," the HHS added.

"The impact of the ransomware attack on communications was severe, as the HSE almost exclusively used on-premise email systems (including Exchange) that were encrypted, and therefore unavailable, during the attack."


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
14/05/21 @ 02:50
HSE received reports from hospitals of encrypted systems
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

HSE Conti ransomware incident timeline (PwC/HSE)

Luckily, the Conti ransomware gang gave the HSE a free decryptor to restore systems, with the added warning that the attackers would still sell or publish the stolen data if the HSE did not pay a $20 million ransom.

"We are providing the decryption tool for your network for free. But you should understand that we will sell or publish a lot of private data if you will not connect us and try to resolve the situation," the Conti ransomware gang said on the negotiation chat page.

"The HSE is aware that an encryption key have been provided," the Irish Department of Health told BleepingComputer at the time. "However further investigations have to be conducted to assess if it will work safely, prior to attempting to use it on HSE systems."

Although the incident led to widespread disruption across Ireland's healthcare services, Taoiseach Micheál Martin, the Prime Minister of Ireland, said that the HSE would not be paying any ransom.

Following the attack, an archive containing samples of stolen HSE files containing patient data was subsequently uploaded to the VirusTotal malware scanning site.

An Irish court later ordered VirusTotal to provide any info on subscribers who downloaded or uploaded the confidential data (including email addresses, phone numbers, IP addresses, or physical addresses) stolen from Ireland's national health care network.

The archive of stolen HSE data was downloaded 23 times by VirusTotal subscribers before the service removed it on May 25, 2021, according to The Journal.

Related Articles:

The Week in Ransomware - May 20th 2022 - Another one bites the dust

Conti ransomware shuts down operation, rebrands into smaller units

The Week in Ransomware - May 13th 2022 - A National Emergency

Costa Rica declares national emergency after Conti ransomware attacks

US offers $15 million reward for info on Conti ransomware gang