May 24th, 2021

TLP White

This week, *Hacking Healthcare* takes a long look at the recent cyberattacks perpetrated against the Irish Health Service Executive (HSE) and Irish Department of Health. We break down what exactly happened, why the Irish government is being lauded for its response, the impact the attack had on healthcare services, and why refusal to pay is unlikely to be a silver bullet for ransomware. Finally, we examine some new comments from US national security figures on a possible approach to a national breach notification law, and we detail two of the hurdles to the creation of such a single, federal breach notification standard. Welcome back to *Hacking Healthcare*.

1. **Irish Healthcare Victimized by Severe Ransomware Attack**

   Ransomware shows few signs of slowing as attacks against critical infrastructure continue. While the fallout of the Colonial Pipeline attack was still dominating headlines, two ransomware attacks hit Ireland's health sector. The attacks caused widespread disruption and may be a concerning escalation in the targeting of the healthcare sector as a whole.

   <u>What Happened in Ireland</u>

   On May 14th, it was reported that the HSE, Ireland's $25 billion public health system, had shut down its IT system as a "precautionary measure" due to a cyberattack.[1,2] The HSE reported it had been the target of a "significant ransomware attack" and was "[assessing] the situation with [its] own security partners."[3] Irish health minister Stephen Donnelly reported that the attack was severely impacting health and social care services, and according to the BBC, HSE chief executive Paul Reid reported that "the cyber attack was affecting all national and local systems involved in all core services."[4, 5]

   To make matters worse, a similar attack was reported against the Irish Department of Health. Thankfully, this attack was reportedly not as extensive, and major disruption was avoided through the actions of the National Cybersecurity Centre (NCSC). It is believed that both attacks were carried out by the same malicious actor.[6, 7]

   In HSE's case, "malware had been inserted across the HSE healthcare system network 'in multiple locations.'"[8] A security researcher published what was alleged to be communications between the cybercriminals and the HSE in which the cybercriminals claimed to have stolen 700 GB of data over two weeks.[9] The cybercriminals also claimed

that the data included the personal data of patients and employees, contracts, financial statements, payroll records, and other sensitive information.[10]

The NCSC was alerted shortly after the HSE attack and confirmed that they began working to provide support. The NCSC also confirmed that the attackers used Conti ransomware and that they were engaging with public and private international partners on the issue.[11, 12]

Government Response

Public statements from government figures helped put the attack into context. One Irish minister called the attack, "possibly the most significant cybercrime attack on the Irish state," explaining that it was an international attack but denying that it was an act of espionage.[13] A criminal cyberattack for profit was later all but confirmed, and the Irish head of government Micheál Martin determined that Ireland would not pay a ransom demand.[14] It was reported that the cybercriminals demanded $20 million to decrypt the affected systems.[15]

Recovery

As of last Sunday, the HSE reported that "[a] structured and controlled deployment of the new decryption tool continues to take place across the core network and its end point devices."[16] However, the scale of the attack was highlighted as government officials relayed that it would take weeks before the HSE systems could be fully operational again, and recovery would be uneven across affected organizations.[17] Until then, government officials have stated that they anticipate continued service disruptions.[18]

Impact to Health Services

The severe impact to services caused by the cyberattack was confirmed by the UL Hospitals Group in Ireland in a statement posted to Twitter about the HSE attack. The statement warned of "LONG delays" and asked for patience as services were switched to manual back-up systems.[19] Additionally, the impact to patients did not take long to escalate, as on May 17th, the UL Hospital group posted another update confirming there would be widespread cancellations of many patient services and appointments across numerous hospitals, with significant delays to all ongoing services.[20] Impacted patient services included maternity care, infant care, radiology, cancer screening, COVID-19 services, and child safety services.[21]

While this outcome would have been harmful enough under normal conditions, the Director of Public Health Mid-West stated that "[This] sinister cyber attack has placed a massive hurdle in front of our health service that is already tackling its biggest ever health crisis as a result of the pandemic."[22] Furthermore, at least some affected healthcare services that tie into HSE systems confirmed they were unaware if HSE stores the patient records they use in a "robust" way, calling into question reliance and communication issues between HSE and various healthcare organizations.[23]

Action & Analysis

Included with H-ISAC Membership

2. The Conversation Around Breach Notification Laws

Recent major cyber incidents like SolarWinds and the Colonial Pipeline attack have placed a renewed focus on improving the cybersecurity and resiliency of the United States as a whole. Among the issues that have remained contentious is the possibility of a national breach notification law as a means to give the government better insight into the health of private sector networks and potential cyber espionage operations. The topic was revisited at the RSA Conference as top national security officials weighed in with their thoughts on what a breach notification law for the private sector might look like.

Last Tuesday, Tonya Ugoretz, Deputy Assistant Director of the FBI, and Adam Hickney, Deputy Assistant Attorney General at the Department of Justice's National Security Division, outlined some of the characteristics they believed would make sense if such an approach was pursued. Ugoretz acknowledged that such a law would need to be clear, concise, minimally burdensome, and primarily focused on sensitive breaches, such as those that impact critical infrastructure or national security.[24] While neither individual advocated for a specific solution, they appeared dismissive of the idea that every incident should be reported.[25]

While a minimally invasive and targeted approach may have appeal for industry and some in government, there are others that stress that a comprehensive breach notification law would go a long way to illuminating just what exactly the cyber threat environment looks like. They argue that without such a law, it becomes impossible to have reliable statistics from which to assess trends and gaps.[26] This in turn makes planning for and allocating appropriate capabilities and resources difficult to impossible.

Adding additional pressure to the creation of a national breach notification law is the current patchwork of independent state breach notification laws. With each state employing its own breach notification law, and no necessary standardization among definitions or requirements, organizations operating in multiple jurisdictions face difficult and costly tasks to ensure they remain compliant with notification requirements. President and CEO of the Cyber Threat Alliance Michael Daniel pointed out to the publication CSO, "At this point, where you've got all 50 states and all our territories having data breach notification laws, everybody's agreed that we need to have breach notification."[27]

Action & Analysis
Included with H-ISAC Membership

Congress –

Tuesday, May 25th:
- House - Committee on Science, Space, and Technology: *SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains*

Wednesday, May 26th:
- No relevant hearings

May 24th, 2021

Thursday, May 27th:
- No relevant hearings

International Hearings/Meetings –

- No relevant hearings

EU –

Wednesday, May 26th:
- European Parliament - Committee on the Environment, Public Health and Food Safety

Conferences, Webinars, and Summits –

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

[1] https://www.healthcareitnews.com/news/emea/ireland-s-health-service-hit-significant-ransomware-attack
[2] https://www.cyberscoop.com/ireland-ransomware-hse-hospitals-offline/
[3] https://www.healthcareitnews.com/news/emea/ireland-s-health-service-hit-significant-ransomware-attack
[4] https://www.bbc.com/news/world-europe-57111615
[5] https://www.healthcareitnews.com/news/emea/ireland-s-health-service-hit-significant-ransomware-attack
[6] https://www.cyberscoop.com/ireland-ransomware-hse-hospitals-offline/
[7] https://www.rte.ie/news/ireland/2021/0516/1221933-dept-of-health/
[8] https://www.bbc.com/news/world-europe-57134916
[9] https://www.bleepingcomputer.com/news/security/irelands-health-services-hit-with-20-million-ransomware-demand/
[10] https://www.bleepingcomputer.com/news/security/irelands-health-services-hit-with-20-million-ransomware-demand/
[11] https://www.gov.ie/en/press-release/22f88-update-on-cyber-attack-on-hse/
[12] https://www.cyberscoop.com/ireland-ransomware-hse-hospitals-offline/
[13] https://www.bbc.com/news/world-europe-57111615
[14] https://www.bbc.com/news/world-europe-57111615
[15] https://www.bleepingcomputer.com/news/security/irelands-health-services-hit-with-20-million-ransomware-demand/
[16] https://www.hse.ie/eng/services/news/media/pressrel/hse-cyber-security-incident.html
[17] https://www.hse.ie/eng/services/news/media/pressrel/hse-cyber-security-incident.html
[18] https://www.cyberscoop.com/ireland-ransomware-health-conti-recovery/
[19] https://twitter.com/ULHospitals/status/1393159107008516100/photo/1
[20] https://twitter.com/ULHospitals/status/1394319508379209739/photo/2
[21] https://www.cyberscoop.com/ireland-ransomware-hse-hospitals-offline/
[22] https://twitter.com/ULHospitals/status/1395767974120853514/photo/2
[23] https://www.bbc.com/news/world-europe-57111615
[24] https://www.cyberscoop.com/data-breach-notification-law-biden/
[25] https://www.cyberscoop.com/data-breach-notification-law-biden/
[26] https://www.csoonline.com/article/3619066/solarwinds-exchange-attacks-revive-calls-for-mandatory-breach-notification.html
[27] https://www.csoonline.com/article/3619066/solarwinds-exchange-attacks-revive-calls-for-mandatory-breach-notification.html