Subject: Attack Assessment—A Significant Cyber-Attack on Irish Health System 2021
Date: October 10, 2021

Summary

On May 14, 2021, the Health Service Executive of Ireland (HSE) faced a significant ransomware cyber-attack, and its nationwide IT systems were forced to shut down. It was one of the strings in a series of cyber-attack toward Ireland after Scotland Environment Protect Agency (SEPA). Part of the data, especially patients', was publicized. More severely, schedules of treatments and many other services were changed or stopped according to the attack that cut off access to patient records, delayed COVID-19 testing, and forced cancellations of medical appointments. Suffering from COVID-19 at the same time, HSE and individuals in Ireland had a hard time offering or getting good health care service.

Attack Overview

In May, Ireland's healthcare systems were targeted in cyber-crime attacks twice: one on Thursday, and the other one on the following Friday.[i] The latter one caused severe impacts on outpatient services and appointments. The Health Service Executive (HSE) said it had taken the precaution of shutting down its systems to further protect their data, including all the linked hospital systems and data, and to assess the situation as well as its impacts right after it noticed the attacks.[ii] A number of hospitals in the Republic of Ireland thus reported disruption on the following services:

- Dublin's Rotunda Hospital had cancelled outpatients' visits, unless women were 36 weeks pregnant or later. All gynecology clinics were cancelled; however, those with any urgent concerns should attend as normal.
- The National Maternity Hospital in Dublin claimed to have a significant disruption to its services on Friday due to a major IT issue.
- St Columcille's Hospital in Dublin postponed some virtual appointments and matters related to electronic records.
- Children's Health Ireland (CHI) at Crumlin Hospital advised people there were delays and all virtual/online appointments had been cancelled.
- The UL Hospitals Group, which consisted of six hospital sites in the Midwest, announced to their patients attending its services that "long delays are expected". Fortunately, emergency services were still operating and people with an outpatient appointment or scheduled procedure should attend unless they are contacted and advised otherwise.

- The child and family agency, Tusla, said its IT systems were not operating because the agency was hosted on the HSE network. Any person wishing to make a referral about a child could contact the office in their area directly.[iii]

Luckily, many experts updated the unaffected parts of health service. Professor Malone said all patients were safe and the hospital had contingency plans in place so it could still work normally with a paper-based system. He supplemented that this would slow down the processing of patients, which dropped by 80% in the days after the attack, and was the reason for the hospital to attempt limiting the numbers attending appointments on that Friday. He further explained that life-saving equipment was in operation and it was the computers with healthcare records that had been affected. The HSE also tweeted that the National Ambulance Service was operating as per normal with no impact on emergency ambulance call handling and dispatch nationally, and the department was working to ensure the information and the systems were protected.[iv]

It was regarded as the most significant cyber-crime attack on an Irish state agency, and the largest known attack against a health service computer system. The investigation organizations including the National Cyber Security Centre believed that these were not espionage. Instead, it was a ransomware that encrypted and locked away the data, and the computer viruses threatened to delete the victim's files unless a ransom was paid by the victims. Like other computer viruses, the virus that led to this crush found its way onto a device by exploiting a security hole in vulnerable software or by tricking somebody into installing it.[v]

Professor O'Reilly, oncologist at Cork University Hospital, pointed out that cancer care was now dependent on technology and the hospital was anxious to proceed with treatment.[vi] Donna-Marie Cullen, a 36 years old mother of two kids waiting for her last radiation treatment for sarcoma, a rare and aggressive form of brain cancer, got a call at lunchtime and was told that her radiation wouldn't be going ahead because of the cyber-attack.[vii] The period caused great worry on Ms. Cullen, knowing how fast sarcoma could grow. "If there was even a minute chance of a crumb of this cancer left in my head, that it would just start to multiply and my radiation plan would need to be completely revised." Ms. Cullen said.[viii] Krysia Lynch, chair of the Association for the Improvement in Maternity Services in Ireland, revealed that it was time to ensure the HSE if they had patient records stored in a robust way and if they have proper cyber defences for this type of ransomware.[ix]

Following the HSE, the Department of Health also got hacked, although it was said to be not as extensive as the HSE by the Minister of Communications Eamon Ryan.[x] RTÉ has reported that these attacks were from the same cyber-crime group, which the investigation organizations believed to be from eastern Europe or Russia, because a digital note from the cyber-crime group which was believed to be responsible has been left on the Department's IT systems. It was similar to the one discovered at the HSE. The National Cyber Security Centre, the Defence Forces, and Europol, had devoted into investigating the attacks with please from the HSE.[xi]

Attack Response and Recovery

After the unwilling but significant cyber-attacks, Mr. Smyth said the Irish government was deploying everything in its response, except for paying the ransom. Taoiseach, the Prime Minister of Republic of Ireland in its official language, Micheál Martin said that he had consulted with cyber security experts and that the state would not be paying a ransom. He said it would take some days to assess its impacts. He emphasized the importance of people cooperating with the HSE, and added that emergency services remained open, and the vaccine programme continued uninterrupted.[xii]

RTÉ News reported on May 17 that a digital note from the cyber-crime group, which was believed to be responsible for these damages, had left on HSE's and the Department's IT systems.[xiii] The HSE passed the related information to the National Cyber Security Centre, which was the lead response agency in cyber-attacks on critical national infrastructure, for investigation and response suggestion. Meanwhile, the Department of Social Protection had suspended a number of electronic communication channels with the HSE while the health service systems were offline to avoid the spread of affection. It then announced its systems being fully operational and were monitored at all times. It said it had cyber defence systems in place which reacted to any threat to its systems in a future cyber incident.

On June 23, it was confirmed that at least three quarters of the HSE's IT servers had been decrypted and 70% of computer devices were back in use. By September, over 95% of all servers and devices had been restored. Ms. Cullen finished her cancer treatment later in May.

Conclusion[xiv] [xv] [xvi] [xvii] [xviii] [xix] [xx]

The ransomware cyber-attack on Irish health system and the government department is a warning that none of the organizations should be relaxed from several success against the attacks. The techniques are advancing quickly and the government are being main targets that an unnoticed could lead to an irreparable damage. The medical system should be treated much more cautious than other fields because a second delay may cause a life's pass away. Ms. Cullen in this case was a lucky one who was near the end of her treatment and the attack was recognized fast.

The way that government deals with the attack is also critical to future possibility of getting hacked. The experts analyze that ransomware cyber-attacks will become more and more severe and frequent if they keep succeeding in gaining ransoms every time. Irish Government decided not to give in to the criminal groups, and to recover the damage by themselves. It is unsure what kinds of cyber-crisis Irish Government will face in the future, but it at least shows its determination to confront against the attacks.

[i] "Cyber-crime: Irish health system targeted twice by hackers", *BBC News*, May 16, 2021, https://www.bbc.com/news/world-europe-57134916

[ii] "Cyber-attack 'most significant on Irish state'", *BBC News*, May 14, 2021, https://www.bbc.com/news/world-europe-57111615

[iii] Ibid.

[iv] Ibid.

[v] Ibid.

[vi] Ibid.

[vii] Michael Sheils McNamee, "HSE cyber-attack: Irish health service still recovering months after hack," *BBC News NI*, September 5, 2021, https://www.bbc.com/news/world-europe-58413448

[viii] Ibid.

[ix] Ibid.

[x] Paul Reynolds, "'No sense' other agencies affected by attack – Ryan", *RTÉ News*, May 17, 2021, https://www.rte.ie/news/ireland/2021/0516/1221933-dept-of-health/

[xi] Ibid.

[xii] Ibid.

[xiii] Ibid.

[xiv] Nicole Perlroth and Adam Satariano, "Irish Hospitals Are Latest to Be Hit by Ransomware Attacks", *The New York Times*, June 2, 2021, https://www.nytimes.com/2021/05/20/technology/ransomware-attack-ireland-hospitals.html

[xv] Josephine Joly and Euronews & AP, "Ireland's HSE still uses 30,000 outdated computers, months after devastating cyberattack", *Biztech News*, September 23, 2021, https://www.euronews.com/next/2021/09/22/ireland-s-hse-still-uses-30-000-outdated-computers-months-after-devastating-cyber-attack

[xvi] Danny Palmer, "'Significant' ransomware attack forces Ireland's health service to shut down IT systems", *ZDNet*, May 14, 2021, https://www.zdnet.com/article/significant-ransomware-attack-forces-irelands-health-service-to-shuts-down-it-systems/

[xvii] Danny Palmer, "Ransomware: Ireland's health service remains 'significantly' disrupted weeks after attack", *ZDNet*, June 4, 2021, https://www.zdnet.com/article/ransomware-irelands-health-service-is-still-significantly-disrupted-weeks-after-attack/

[xviii] HSE services, https://www2.hse.ie/services/cyber-attack/how-it-may-affect-you.html

[xix] Naomy O'Leary, "EU cites HSE hack as it unveils plans for rapid-response cyber unit", *The Irish Times*, June 23, 2021, https://www.irishtimes.com/news/health/eu-cites-hse-hack-as-it-unveils-plans-for-rapid-response-cyber-unit-1.4601835

[xx] "Health Service Executive Ransomware Attack", *Wikipedia*, https://en.wikipedia.org/wiki/Health_Service_Executive_ransomware_attack#Background