Ireland's Health Service Executive ransomware attack (2021)

Razan Muhammed Aljuhani – 1806065 – GAR

Background

In the mid of May 2021, Ireland's Health Service Executive was subjected to a fierce major ransomware cyberattack which negatively affected the national and local systems as well as their services. It was started on May 13 when the National Center for Cyber Security in Ireland was notified of strange activity on the Department of Health (DoH) network, and necessary measures were taken to verify the incident, and then on May 14, it was confirmed that a cyber-attack had occurred on HSE systems. Therefore, the health services official in Ireland was notified about the attack. The breach occurred during the Corona pandemic and some systems such as the close contact referral system were disrupted. It was the most significant cybercrime attack on an Irish state agency and the biggest known breach against a system of health services.

It was observed that the hackers were not easily detected as it was reported that they had been in the systems for about a week before they were identified and disclosed. The attackers used the Conti ransomware, it was observed that the responsible criminal group was known as Wizard Spider.

Type of attack	Ransomware (Malware)
Aim	Financial profit
Target victim	The Health Service Executive
Target system	Microsoft windows-based systems

Type of attack

Ransomware is a type of malicious software (malware), it demands a ransom from the victim that is usually paid using bitcoin. It can be divided into two categories. First, the well-known type is named crypto-ransomware and, it works through encrypting files and data. The second type is locker-ransomware, it makes harm by only locking the device and blocking the victims from using it, and typically

the stored data in that device stay intact, it less effective in exploiting the victims to pay the ransom due to that the valuable resource "Data" safe and can be recovered by moving the storage device to another computer. Some ransomwares can diffusion to other machines on the network.

The damages

The attack made a big impact on the system include:

- Stopping services at several Irish hospitals for a while.
- The closing of the HSE's national and local networks causes the cancellation of many healthcare services.
- Accessing the personal and medical information of many patients and staff.
- Sharing of sensitive data of 520 patients on the dark web.
- HSE workers were unable to access e-mail.
- Disrupting the COVID-19 testing referral system that mandatory suspected individuals to attend for testing without an appointment.

Finally, by September it was fortified that over 95% of all servers of HSE IT and devices had been restored.

Security breaches

The NCSC discovered the use of remote access tool called Cobalt Strike by the criminals to infect systems and execute the ransomware. The attack started when a single computer shut down due to clicking on the infected link caused by the HSE employer. At the end of May, the HSE proved sensitive medical information for 520 patients spread, and confidential documents of the organization and their employees' data were published for the public through the internet as a result of the breach.

How could it have been avoided

On 20 May 2021, The HSE brought a High Court order that limits the hackers' scope for exploiting the stolen data. The Criminals provided a decryption key that could recover the HSE encrypted IT systems, and all the files locked by hackers. In response to the attack, the HSE create a cyber security operations center to control and

monitor its networks. Also, the law doesn't encourage the payment of ransom demands and avoid scamming because there is no guarantee, and it will cause more harm.

Four ways to mitigate the impact of a Ransomware attack on organization systems:

1. Up-to-date backups are necessary for all important files and keep them in a separate location.
2. Install, update, and run antivirus software.
3. Security education and awareness training to organization stakeholders.
4. Automatic updates for OSs, applications, and firewalls.

Suggestions

The organization should follow effective cybersecurity controls include:

- Secure Email communication.
- Protect the roaming devices.
- Identify stolen and compromised devices.
- Maintain user privacy.
- Cyber security incidents can be reported to the NCSC.

References:

- Huang, D. Y., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K., ... & McCoy, D. (2018, May). Tracking ransomware end-to-end. In *2018 IEEE Symposium on Security and Privacy (SP)* (pp. 618-631). IEEE.
- https://cyberlaw.ccdcoe.org/wiki/Ireland%E2%80%99s_Health_Service_Executive_ransomware_attack_(2021)
- https://en.wikipedia.org/wiki/Health_Service_Executive_ransomware_attack