Attack Case Study

Ireland’s Health Services Executive

Advanced ransomware cyber attack

On May 14 2021, the HSE was subjected to a serious cyber attack, through the criminal infiltration of their IT systems (PCs, servers, etc.) using Conti ransomware.

Aim of the Attacker was to disrupt health services and IT systems, steal data, and demand a ransom for the non-publication of stolen data and provision of a tool to restore access to data they had encrypted.

On 28 May, the HSE confirmed confidential medical information for 520 patients, as well as corporate documents were published online.

On 23 June, 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. Nowadays, over 95% of all servers and devices had been restored.

The Health Service Executive (“HSE”) is a large geographically spread organisation which provides all of Ireland’s public health services through hospitals and communities across the country. The HSE consists of approximately 4,000 locations, 54 acute hospitals and over 70,000 devices (PCs, laptops, etc).

The HSE attack began on March 18 from a malware infection on an HSE workstation - dubbed "Patient Zero Workstation" - as the result of a user clicking and opening a malicious Microsoft Excel file that was attached to a phishing email sent to the user on March 16.

After gaining unauthorized access to the HSE’s IT environment on March 18, the attacker continued to operate in the environment over an eight week period until the detonation of the Conti ransomware on May 14. This included compromising and abusing a significant number of accounts with high levels of privileges, compromising a significant number of servers, exfiltrating data and moving laterally to statutory and voluntary hospitals.The incident was not identified and contained until after the detonation of the Conti ransomware on May 14, which caused widespread IT disruption.

Timeline

Ireland’s Health Services Executive

1- The attackers began by sending a malicious email to a workstation on 16 March 2021.

2- The email was opened on 18 March. A malicious Microsoft Excel file was downloaded, which allowed the attackers access to HSE systems

3- The HSE antivirus software detected activity on 31 March, but could not block it as it was set to monitor mode

4- 12//05/21 to 13/05/21 The Attacker browsed folders & opened files on systems within the HSE

5- On 13 May the cybersecurity provider for the HSE emailed the Security Operations team that there had been unhandled threats on at least 16 systems since 7 May. The Security Operations team had the server team restart servers.

6- The HSE was alerted to the attack at 4am on 14 May 2021. The attack affected both national and local systems, involved in all core services, with the HSE taking down their IT system in order to protect it from the attack and to give the HSE time to consider options.

Vulnerabilities

May attack took advantage of a number of vulnerabilities that are not unique to Ireland's national health system, including issues faced by other organizations.

Those issues included HSE having "a very low level of cybersecurity maturity" as evaluated against the National Institute of Standards and Technology's Cybersecurity Framework

Vulnerability #1

The IT environment not having many security controls that are most effective at detecting and preventing human-operated ransomware attacks

Vulnerability #2

Having no security monitoring capability that was able to effectively detect, investigate and respond to security alerts across HSE's IT environment or the wider National Health Network

Vulnerability #3

A lack of effective patching, including updates and bug fixes, across the IT environment that is connected to the NHN

Vulnerability #4

Reliance on a single antimalware product that was not monitored or effectively maintained with updates across the environment

Costs

Healthcare professionals lost access to all HSE provided IT systems - including patient information, clinical care and laboratory.

Non-clinical systems such as financial systems, payroll and procurement systems were also lost.

Significant disruption immediately occurred and many healthcare professionals had to revert to pen and paper to continue patient care.

Healthcare services across the country were severely disrupted with real and immediate consequences for the thousands of people who require health services every day.

The ransomware attacks took HSE months of work and approximately $600 million to decrypt, restore, and fortify their systems.

Prevention

- Appoint an interim CISO to be responsible for driving cybersecurity improvements and managing third parties that provide cybersecurity services;
- Ensure that the HSE's incident response provider's managed defense service or an equivalent is maintained to detect and respond to incidents on endpoints;
- Develop, document and exercise a plan for managing and coordinating a cybersecurity incident involving multiple organization connected to the NHN;
- Prioritize the remediation of critical legacy systems.