# Attacks on Healthcare

Threat Memo - Date: 23/03/2020 - Version: 1.0

TLP:WHITE

| | Category | Type | Domain(s) | Sector(s) | Confidence |
|---|---|---|---|---|---|
| FOR INFORMATION | Cybercrime Espionage | Ransomware, personal data exposure, targeted intrusions, | World | Healthcare, Research | A1 |

## Key Points

- Healthcare organisations provide interesting targets to cyber criminals.
- Due to the criticality of their function, they are more prone to submit to cyber-extortion.
- The most prevalent type of attack in the sector is ransomware.

## Summary

The recent onset of the Coronavirus pandemic has put healthcare organisations and professionals worldwide in the spotlight. Due to the criticality of their mission as well as their unique positioning to hold and process treasure troves of private sensitive information, healthcare organisations, now and in the past, have attracted cyber criminals.

In the last year, there have been several high profile attacks in the sector resulting in significant financial and data losses. Beyond the highly publicized cases, cyber-criminal groups overall are mounting continuous attempts to exploit vulnerabilities of healthcare organisations The current report attempts to summarise the main IT security challenges for the healthcare sector, illustrating how this critical service can be affected by cyber threat actors. The Annex provides details on recent attacks in the sector.

### a. Direct attacks against health organisations

Ransomware. The most prominent cases of attacks against healthcare institutions are ransomware incidents. The organisations in the sector have to operate in a time-sensitive manner and any disruption in the availability and correct flow of information may not only have dire consequences in their ability to function but may also directly threaten lives of patients. Under these restraints, healthcare institutions experiencing a ransomware attack are under immediate pressure to give in to ransom demands. Taking into consideration the need to retain the trust of public, attackers may furthermore use as a leverage the threat to publicly disclose any incident, possibly along with a release of captured proprietary information (for more on that, please also see TM 20-028). The latter case would additionally carry the risk of significant administrative retribution for the organisation. Overall, healthcare organisations are characterised by cyber criminals as "Big Game hunting".

As a side note, news media reported on March 18 2020 that criminal threat actors, when asked about their planned actions during the coronavirus crisis, responded in at least two cases (Doppelpaymer, Twisted Spider/Maze ransomware) with a pledge to forgo attacking healthcare organisations[1].

Stealing personal, health, and financial data. Due to their function, healthcare organisations need to store and manage large volumes of client information as well as other business data (procurement, contracts, internal documents etc.) This makes them particularly valuable as targets for cyber criminals. Regularly, cyber criminals regular advertise on underground marketplaces either access to healthcare networks or data sets for sale.

### b. Improper handling of information

There have been several cases of private and public health and social care establishments showing neglect or technical incapability to safeguard patient and client data. As any other IT operation, healthcare organisations have adopted the practice of utilising Managed Services Providers (MSP) as well as the storage and processing facilities of cloud providers. Cyber criminals may leverage breaches to MSPs to get access to healthcare records. In parallel, utilisation of cloud services exposes the organisations to cloud threats. Some common cases to underline the exposure to such threats are insecure, publicly accessible (local) ElasticSearch databases or (cloud based) Amazon Web Services (AWS) S3 buckets (see incident in Annex).

### c. Efforts to acquire scientific data, research results etc.

Organisations in the health sector, in particular ones involved in scientific research or handling disease containment efforts may also be subject to espionage efforts by nation states. In several cases, nation-state actors have tried to infiltrate such organisations to acquire non-publicly available scientific information. These are cases in which, instead of having to defend against cyber criminals, the organisations have to consider the efforts of state-sponsored intelligence agencies.

[1] https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/

China in particular attempts to address a number of health problems for its large population in the near future. In parallel, China aims to become a leader in the healthcare industry and promote its own research and technology. Finally, with the recent coronavirus pandemic, disease control techniques of other countries have become particularly interesting to Chinese authorities (for an analysis of Chinese activities in the sector, please see TM 190621-1).

Beyond the immediate value to the attacker's scientific establishment, such information would also have a high market value, as it may lead to the development of novel drugs and treatments, as well as the possible bypass of international sanctions concerning educational and research institutions. Another aspect of this type of threat is the possibility of nation states acquiring internal reports from disease fighting organisations and use them in tainted leaks as part of disinformation campaigns.

**d. Disinformation**

As public facing institutions, healthcare organisations are targeted by state actors, hacktivists, cyber criminals, and others who want either to make a public point, disrupt the normal operation of society, or create a disinformation narrative. In the case of coronavirus in particular, there have been cases of supposedly "leaked" information about hospitals with "terrified" personnel, reports of hiding the numbers of victims, as well as epidemic handling misinformation. Such incidents in Ukraine led to a number of public protests in February 2020 (please see TA 20-008 for additional information).

**e. Vulnerabilities on medical equipment**

Bugs allow for a takeover of devices, which could allow attackers to disable them, harvest personal data, change alarm settings, and alter functionality. Such devices have repeatedly been found to ship with default login credentials or lack security patches for multiple years.

Lists of vulnerable medical devices includes gear from all the major manufacturers, ranging from simple software programs up to CT scanners. Many types of devices are affected with different levels of impact, but often resulting in full takeover of the device. Some particular examples include vulnerabilities to cyber-attacks for Medtronic insulin pumps, data leakage for Alaris medicine infusion workstations, and takeover risks for Siemens Healthineers products. In some circumstances, this could have a lethal impact (please also see TM-20-012 for further details).

## Comments

As the Coronavirus pandemic is still in full swing, threats and opportunistic attacks to Healthcare institutions are expected to continue. In parallel, EU-I in any way associated with health should also operate at a heightened state of security to prevent incidents that may jeopardise their operation or lead to leaks of critical data.

**Annex I – Most significant recent security incidents in the healthcare sector**

| Date | Country | Victim organisation | Attack type | Threat Actor/ Malware | Details/ Impact |
|---|---|---|---|---|---|
| 16.03.2020 | US | US Dept. of Health and Human Services | DDoS | | Attempted disruption of dissemination of coronavirus information. Site slowed down. There is a plausible connection with a hoax message, circulated on the same day that the US would impose a quarantine. |
| 14.03.2020 | Czech Republic | Brno University Hospital | Disruption | | Hospital and its branches forced to shut down IT network. The Brno University Hospital is one of the Czech Republic's biggest COVID-19 testing centres. |
| 11.03.2020 | US | Champaign-Urbana Public Health District | Ransomware | Netwalker | Website unavailable. The site was distributing information on the coronavirus pandemic. |
| 09.03.2020 | US | Arkansas Children's Hospital | Undetermined | | IT system had to be restarted |
| 02.03.2020 | US | Walgreens drugstore | Mobile app vulnerability | | Customer personal information exposed |
| 19.02.2020 | US | Plastic surgery technology company NextMotion | Insecure DataBase | | An insufficiently secured Amazon Web Services (AWS) S3 bucket allowed access to 900.00 patient records, including plastic surgery photos. |
| 17.02.2020 | US | Iowa-based medical facility | Data breach | | Unauthorised access to 7.500 patient records containing personal information |
| 11.02.2020 | US | Two Puerto Rican hospitals | Ransomware, Regulatory issues | | Class action suit filed by two patients for exposure of personal and financial information during a February 2019 ransomware attack |
| 15.11.2019 | France | Rouen University Hospital | Ransomware | | The Rouen University Hospital was hit by a WannaCry-style ransomware attack on Friday, Nov. 15, 2019, that forced the hospital to shut down its IT systems and operate in what it calls "degraded mode." |