Orange
Cyberdefense

Cyber Intelligence Online

The threat of cyberattacks on healthcare establishments during the COVID-19 pandemic

Abstract

While COVID-19 infections around the world are exploding, cyber threat actors are trying to capitalise on this global health crisis by creating malwares or launching attacks with a COVID-19 theme. Last week, a COVID-19 testing centre was hit by a cyberattack, leading to a disruption in the proper functioning of the hospital. In the context of a global sanitary crisis due to a pandemic, risk of cyberattack must be given close attention to by hospital and healthcare organisations. In the following paper, we describe the risks involved for these organisations and our recommendations.

OSINT Unit

a division of the Orange Cyberdefense Epidemiology Lab

March 20th 2020

orange™

Summary

Abstract *1*
1. Context: a COVID-19 testing centre hit by cyberattack *3*
1.1. A worldwide pandemic 3
1.2. A COVID-19 testing centre hit by cyberattack in Czech Republic 3
2. How high is the alert for healthcare organisations? *5*
2.1. A sector that can be spared by ransomware operators… 5
2.2. … but has already been targeted: the alert is high 6
3. Analysis: a more global increase of cyberattacks linked to COVID-19 ..... *7*
3.1. The use of “Live Coronavirus Data Map” from John Hopkins CSSE to spread malware 8
3.2. The use of COVID-19 map malware on Android smartphones 9
3.3. Healthcare organisations must be considered as potential victims 10
4. What are the risks of a cyberattack for a hospital in the context of COVID-19? *11*
5. Recommendations: what are the lessons for hospitals as the crisis is striking? *12*
6. Disclaimer *13*

1. Context: a COVID-19 testing centre hit by cyberattack

1.1. A worldwide pandemic

COVID-19 infections are growing around the world, with 218,827 cases and 8,811 deaths as of March 19th 2020[1]. However, some countries only practice tests on severely ill people, and some cases are "asymptomatic", meaning the real number of infected people could already be extremely high. Hospitals, clinics and healthcare centres worldwide are already facing a wave of new infections or are preparing to face them soon.

Ordinarily, a cyberattack against critical infrastructure, such as hospitals is extremely dangerous and potentially disastrous, but it is even more damaging in the case of a sanitary crisis, such as COVID-19.

1.2. A COVID-19 testing centre hit by cyberattack in Czech Republic

The situation needs to be closely monitored since one testing centre in Europe was hampered by cybercriminal activity[2]. Computer systems at the University Hospital Brno, in Czech Republic, were shut down on March 14th 2020 because of a cyberattack. This hospital is the **second largest in the country and hosts one of the 18 laboratories used for testing the new virus**. Since the outbreak, the institution carried out up to 20 tests a day.[3]

M**ore than 500 confirmed cases are reported in the country as of March 19th 2020[4]** and thousands of people are now in quarantine. A state of emergency has been declared and restrictions against crossing borders have imposed.

The director of the hospital said that computer systems started "falling gradually" and "had to be shut down", and members of the staff received instructions not to turn on their computers[5]. According to Bleeping Computer, a computer help site, "systems serving laboratories like hematology, microbiology, biochemistry, tumor diagnostics, or radiology appear to be on a different network than the affected systems as they continue to work."[6]

However, **the attack was considered as serious enough to prompt a shutdown of IT systems and to move acute patients to an alternative facility**.

According to a news report from Tech**Radar[7], the hospital was unable to transfer information from key clinical systems to its database**. As prescriptions are written by hand or typed, this

[1] https://coronavirus.jhu.edu/map.html

[2] https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/

[3] Ibid.

[4] https://coronavirus.jhu.edu/map.html

[5] https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/

[6] Ibid.

[7] https://www.techradar.com/news/coronavirus-hospital-suspends-activity-over-cyberattack

leads to longer examination times, which puts additional strain on doctors need who need all the means available to them to fight the virus.

The National Cyber and Information Security Agency (NÚKIB) is working to identify the root of the problem and remedy the situation. The National Organised Crime Centre is also involved in the case[8].

[8] https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/

2. How high is the alert for healthcare organisations?

2.1. A sector that can be spared by ransomware operators…

Contrary to typically targeted sectors, such as banking/finance or e-commerce, the healthcare sector is sometimes spared by hackers. In this regard, the group behind Maze ransomware informed BleepingComputer that they "don't attack hospitals, cancer centres, maternity hospitals and other socially vital objects."[9]

In the case of COVID-19, there does appear to be hope as **two ransomware operators have stated that they will no longer target health and medical organisations during the pandemic**[10].

On March 18th 2020, Bleeping Computer asked Maze, DoppelPaymer, Ryuk, Sodinokibi a.k.a REvil, PwndLocker and Ako Ransomware, some of the most active ransomware organisations if they would continue targeting health and medical organisations during the crisis. As of March 19th 2020, two of these organisations answered:

- **DoppelPaymer** stated they normally don't target hospitals or nursing homes, and will not change this approach during the crisis. They also said that if a medical organisation was targeted by mistake, they will decrypt the encrypted files for free. In this regard, they said to Bleeping Computer that if a healthcare organisation has been encrypted, "it should contact them through their email or Tor webpage to provide proof and get a decryptor"[11].
- **Maze operators** issued a "press release" stating they will stop all activity against all kinds of medical organizations until the end of the outbreak. However, they did not give any indication of any action they might take if a healthcare organisation gets encrypted by mistake.

Source : "Press release" to researchers and dedicated journalists published by the hacker group Maze.

[9] https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/

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

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

According to this press release, Maze also offers “discounts” to organisations that were encrypted by Maze ransomware, allowing them to pay a discounted ransom.

The other ransomware operators are yet to responded.

2.2. … but has already been targeted: the alert is high

Healthcare organisations have to be on high alert: hackers do not always have the conscience of Maze or DoppelPaymer and **several cyberattacks have been reported against the healthcare sector.** This sector is indeed attractive for hacker groups, especially because of the **sensitivity of patient data.** In this regard, a Reuters report indicated that the financial value of healthcare data can be as much as ten times that of a credit card number on the black market[12].

In 2017, as part of a global cyberattack, a number of UK healthcare facilities fell victim to ransomware, requiring the payment of a ransom to retrieve their data. The **attack simultaneously targeted 16 NHS[13] dependent entities, disrupting the use of computers and leading to the refusal of patients**. **Some facilities were forced to cancel or postpone medical procedures.** However, the UK Prime Minister made it clear that the attack "was not directed solely at the NHS". Various organisations in different countries in Europe, Mexico and even the United States were also reportedly affected. The WannaCry ransomware was later found responsible for this attack.

In 2018, **the SamSam ransomware hit at least two hospitals** in the US, and in 2019 **Ryuk ransomware had attacked hospitals mercilessly**. DHC hospitals in Alabama had to pay the ransom to obtain a decryption key that unlocked the medical data[14].

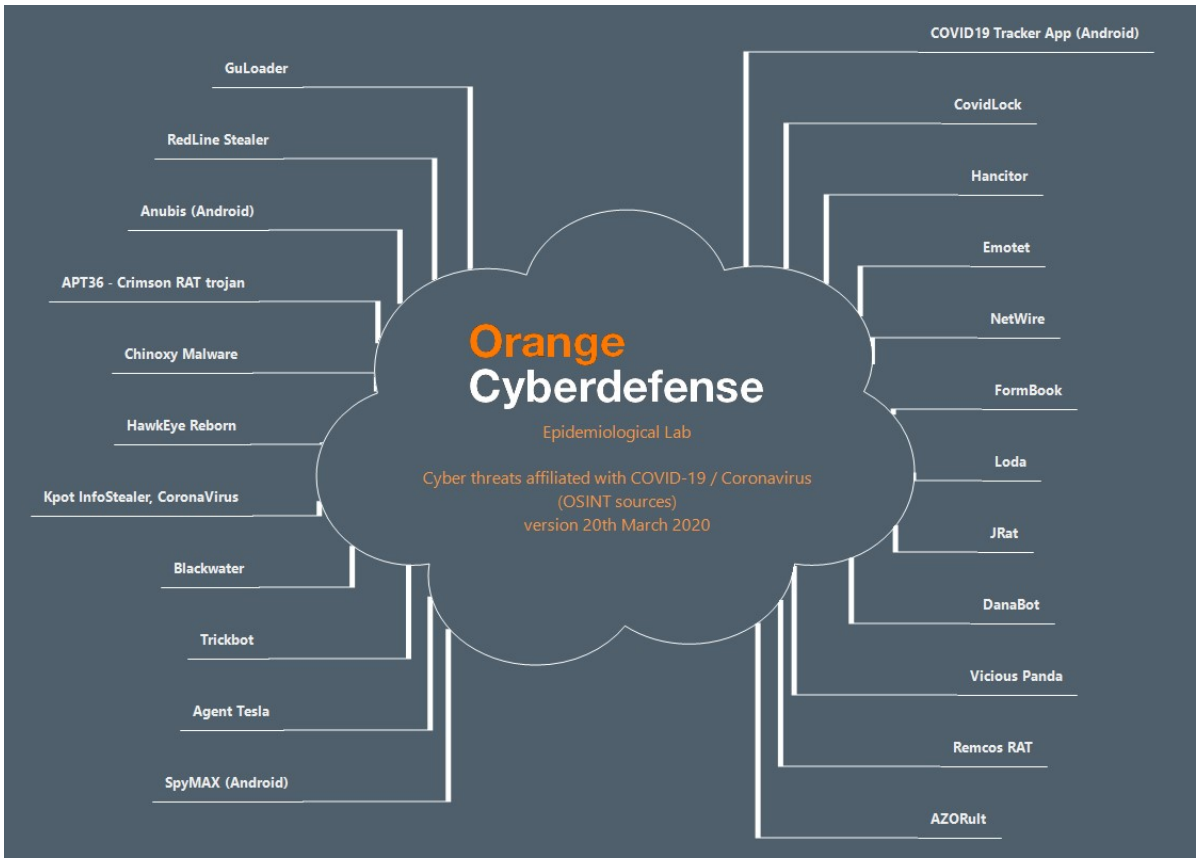
[12] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924

[13] National Health Service: the publicly funded healthcare system of the United Kingdom.

[14] https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/

3. Analysis: a more global increase of cyberattacks linked to COVID-19

There are actually other threat actors trying to capitalise on this global health crisis by creating a malware or launching attacks with a COVID-19 theme. The Laboratory of Epidemiology and Signal Intelligence made this map based on OSINT sources and on our own investigations.

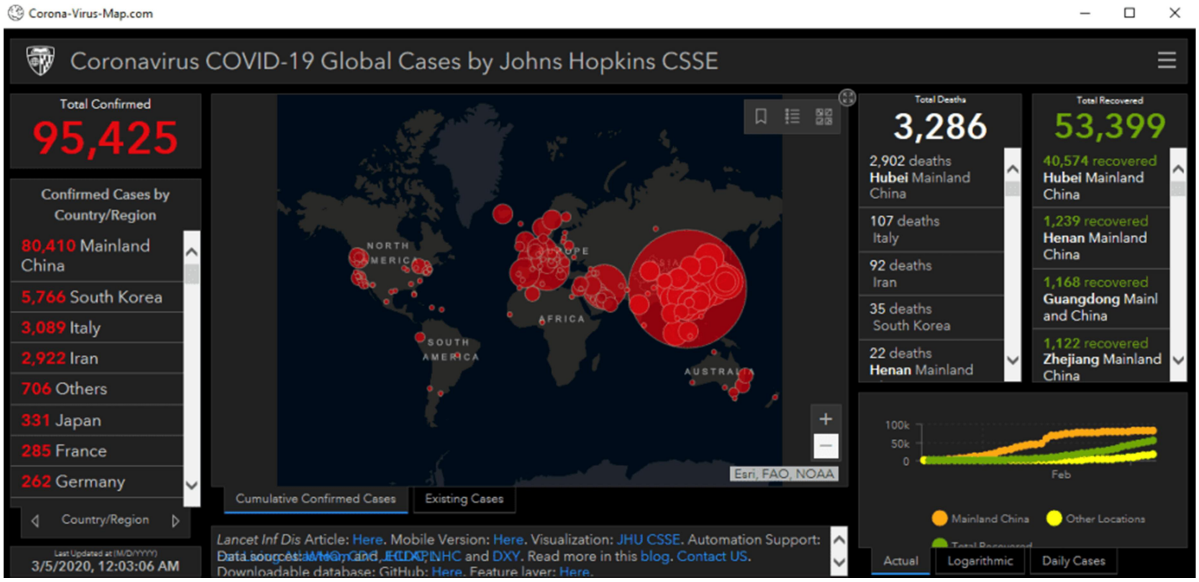


Source : Laboratory of Epidemiology and Signal Intelligence – Orange Cyberdefense

We chose to focus on some of these malwares to explain how they operate.

3.1. The use of "Live Coronavirus Data Map" from John Hopkins CSSE to spread malware

The "Live Coronavirus Data Map" from the John Hopkins Center for Systems Science and Engineering (CSSE) has been used as a lure to spread malware.



Source: Security Affairs

https://securityaffairs.co/wordpress/99446/cyber-crime/coronavirus-map-delivers-malware.html

This interactive dashboard is being used by malicious websites (and possibly spam emails) to spread password-stealing malware. According to Krebsonsecurity.com, a member of "several Russian language cybercrime forums began selling a digital coronavirus infection kit that uses the Hopkins interactive map as part of a Java-based malware deployment scheme. The kit costs $200 if the buyer already has a Java code signing certificate, and $700 if the buyer wishes to just use the seller's certificate."[15]

The lure is very realistic. It acts as a full working online map of coronavirus infected areas, which is "resizable, interactive, and has real time data from the World Health Organisation and other sources". The offer selling the kit stated that "users will think that PreLoader is actually a map, so they will open it, spread it to their friends and it goes viral!".[16]

The number of infected people or organisations is unclear, but security experts from Malwarebytes Labs warned of **new malicious websites that used interactive versions of the same map, to catch attention and distract visitors while the sites tried to foist the password-stealing "AZORult" malware[17].**

[15] https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/

[16] Ibid.

[17] https://blog.malwarebytes.com/social-engineering/2020/02/battling-online-coronavirus-scams-with-facts/

3.2. The use of COVID-19 map malware on Android smartphones

Recently, **links were sent to some Android phones (typically, via SMS or watering hole websites), promising an app tracking coronavirus**. This is a lure. Once the application is downloaded, people suspected to be operating from Libya can **watch through the smartphone camera, gain access to text messages or listen through the microphone**. The malware identified is be a customised version of **SpyMax,** a commercial spyware than can be acquired very easily online and for free.[18] A researcher from Lookout, a cybersecurity company, has associated this malware with 30 other rogue Android applications using the same C2 infrastructure[19] of a wider surveillance campaign, apparently active since at least April 2019. There is no evidence that this malware is state-sponsored, but Lookout researchers noted "the use of these commercial surveillanceware families has been observed in the past as part of the tooling used by nation-states in the Middle East"[20].

Another Android app has also been detected by DomainTools, using the same map as a lure, but this time causing the phone to lock **and asking for a ransomware payment for it to be unlocked**[21]. This ransomware is called **CovidLock**.

[18] https://www.forbes.com/sites/thomasbrewster/2020/03/18/coronavirus-scam-alert-covid-19-map-malware-can-spy-on-you-through-your-android-microphone-and-camera/#784e85a75fd8

[19] "C2" means "Command and control": a set of organizational and technical attributes and processes that employs human, physical, and information resources to solve problems and accomplish missions to achieve the goals of an organization or enterprise.

[20] https://blog.lookout.com/commercial-surveillanceware-operators-latest-to-take-advantage-of-covid-19

[21] https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware

3.3. Healthcare organisations must be considered as potential victims

All of those malicious links or apps are a risk to healthcare organisations, as **doctors or caregivers can innocently download these apps onto their smartphones or personal computers**, and then connect them to their hospital networks.

Even by accident, many employees are often the root cause of successful cyberattacks, according to Accenture's 2018 State of Cyber Resilience survey[22]. Data leakage (mobile users giving permissions to apps on their phones without checking security) potentially allows sensitive data to be forwarded on. According to AccountancyAge[23], this "is due to smartphone users being more likely to check their emails frequently and being more likely to make a mistake by clicking a dodgy email link".

This could lead to the propagation of a malicious code inside a hospital's network and turn into a disaster, especially during a crisis such as the COVID-19 outbreak.

This means that the threat is high on healthcare centres, because they could be targeted by a wide range of malwares.

[22] https://www.accenture.com/in-en/insights/security/2018-state-of-cyber-resilience-index

[23] https://www.accountancyage.com/2020/01/16/mobile-as-a-threat/

4. What are the risks of a cyberattack for a hospital in the context of COVID-19?

In the short term, the disruption of business continuity can lead to **health risks for patients.** Usually, ransomware spreads by email on computers that have not been updated. Once a machine has been contaminated, the malware penetrates the local network and contaminates all vulnerable computers.

The inability to use all computers jeopardises the proper functioning of hospitals. **Some patients in a state of emergency could therefore be refused entry, while hospitals are waiting for a mass influx in the context of COVID-19 spreading**. **The state of available stocks of medicines in hospitals and pharmacies can also be encrypted and thus disrupt the proper distribution of medicine.** Failure to access data on patients' health and their treatment may result in an inability to treat them properly.

In the long term, shutting down a healthcare institution carries a risk of **significant financial loss**, since the service cannot operate until the cyberattack has been managed and the damage has been repaired. The cost of repairs can also be extremely high in the short term (data reconstitution,, viral decontamination, additional operating costs, etc.).

There is also **a risk of widespread patient concern, even panic,** if the confidentiality of data is threatened, and, in the case of the COVID-19 pandemic, if urgent care cannot be provided to seriously ill patients.

5. Recommendations: what are the lessons for hospitals as the crisis strikes?

In order to avoid a cyberattack, it is advisable to **ask all managers of healthcare institutions to distribute prevention recommendations to employees. For instance,** "do not open suspicious emails or links", "warn the institution in case of doubt," "change all passwords" or "ensure that backups have been made...". The goal is to avoid an infection and the subsequent spread of the ransomware. The main message that must be addressed to health sector officials is **not to give in to panic**.

However, we want to focus your attention on the following remark**: although a lot of cybersecurity companies highly recommend not to pay a ransom, this decision must be considered on a case-by-case basis.** In some cases, ransomware act in two ways:

- At first, they send a first viral strain that will allow to exfiltrate data before an encryption;
- Then, a few hours or days later, they launch the ransom to encrypt the entire data.

The hackers then publish the data on the internet, or to researchers and journalists if the ransom is not paid. Maze ransomware operates in this way. This is therefore **an even bigger threat than a typical ransomware attack, especially for healthcare organisations as patient data could be released into the public domain.**

Moreover, some ransomware organisations stated that they would not target medical organisations in the context of the outbreak. DoppelPaymer operators even said that if a medical organisation were targeted by mistake, they would decrypt the encrypted files for free. That is why **we highly recommend to medical organisations to get in touch with ransomware operators, in order to get a free decryption of data.** Proof that they are a medical organisation is required.

In France, if a cyberattack occurs and the threat is proven, the alert must be triggered by the **Regional Health Agency**. The scope of the alert will determine the level of information distribution (regional, regional requiring national information, regional requiring support, national). In addition, **the Operational Centre for Regulation and Response to Health and Social Emergencies may be activated**.

Measures to protect the image of the sector and to manage the crisis can also be put in place. Indeed, a large-scale cyberattack should be the subject of a crisis communication in order to defuse concerns. A crisis management centre common to Public Hospitals could therefore be set up for the general public, which could be rapidly mobilised if necessary to manage communication with the media. As the crisis will be particularly dangerous in the case of a COVID-19 outbreak, the Prime Minister may decide to activate an Interministerial Crisis Unit, which will work in collaboration with the Ministry of Health and Solidarity.

In the longer term, it might be possible to impose an internal or external audit of all health establishments. This would allow time to identify present and future vulnerabilities in order to put in place an action plan. French hospitals could be blamed for the obsolescence of their systems if a cyberattack occurred. If an incident happens, technical investigations have to be carried out to determine the source of the breach that allowed the intrusion, and the extent of the material or immaterial damage.

6. Disclaimer

Orange Cyberdefense strives to ensure the accuracy of the information gathered in this document, but no warranty, express or implied, can be given.

Orange Cyberdefense disclaims any liability for errors or omissions resulting from/related to the use of the information and material in this document.

Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 16 SOCs, 10 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries.

We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.