FOI MEMO
Projekt/Project
CBRN-händelser i störd miljö

Sidnr/Page no
1 (9)

Projektnummer/Project no
A405120

Kund/Customer
Fö

FoT-område
Inget FoT-område

Handläggare/Our reference
Annica Waleij

Datum/Date
2020-04-09

Memo nummer/Number
FOI Memo 7062

Cyberattacks in the healthcare sector during the first three months of the Covid-19 pandemic

David Lindahl, Birgitta Liljedahl och Annica Waleij

Illustration: Hans Lundholm, Halustudio

Introduction

On December 31st 2019, Chinese authorities notified the World Health Organisation (WHO) that a new infectious disease had broken out in the Hubei province. Since then, the outbreak of the coronavirus, SARS CoV-2, has turned into a pandemic. Globally (as of 2020-04-09 2:00 am CEST), there were 1,395,136 confirmed cases of COVID-19, including 81,580 deaths.[1] In the wake of the pandemic, misinformation as well as disinformation including conspiracy theories have spread in e.g. social media almost as fast as the virus itself.[2,3,4] Furthermore, criminal elements have seized the opportunity to exploit the situation and launched a large number of cyber frauds, and cyberattacks both on targets in the healthcare sector and against any target they believe will yield a profit.[5] A number of attacks have also been attributed to state actors.[6]

This brief is one in a series of follow up briefs regarding the conclusions made in the report "A wider perspective on CBRN related threats".[7]

[1] See https://who.sprinklr.com/

[2] The virus of disinformation: Echoes of past bioweapons accusations in today's Covid-19 conspiracy theories https://warontherocks.com/2020/04/the-virus-of-disinformation-echoes-of-past-bioweapons-accusations-in-todays-covid-19-conspiracy-theories/

[3] Oksanen, P, och Sundbom, H., 2020, "Informationspandemi - desinformation i spåren av Covid19", Frivärld. 3 April.

[4] EU vs Disinformation Coronavirus database https://euvsdisinfo.eu/disinformation-cases/?text=coronavirus&date=

[5] EUROPOL: Pandemic profiteering how criminals exploit the COVID-19 crisis March 2020, https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

[6] Attributed in this case simply means that some organisation and/or state has made the claim. No independent verification of these claims have been made by the Swedish Defence Research Agency (FOI).

[7] Waleij, A. Liljedahl, B. Börjegren, S. Lindahl, D. (2019) Vidare kontext för en CBRN-relaterad hotbild. FOI, Stockholm, Sweden, FOI-R--4781—SE, ISSN 1650-1942 https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4781--SE

Malware risks in the healthcare sector

Much has already been written about how the healthcare sector is vulnerable to cyber-attacks and that digital risks have increased.[8,9,10,11,12,13,14]

One such risk is posed by ransomware, malware that encrypts storage media in an attempt to blackmail system owners. Such attacks have in the past caused severe disruptions and damage. In fact the so far most costly cyberattack in the world, Wannacry, was of this type. It took place in May 2017 and within days 230 000 hosts were infected.[15] In the United Kingdom, the National Health Services (NHS) reported 80 of its 236 trusts affected, five of which had to turn away even emergency patients. In addition to the trusts, 603 primary care facilities and other NHS organisations were affected.[16]

The current crisis has seen similar attempts; On April 4, 2020, Interpol warned of cybercriminals targeting critical healthcare infrastructure fighting the Covid-19 pandemic with ransomware.[17] Also, biotech firms, researching for possible Covid-19 treatments, have been targeted.[18]

---

[8] ICRC (2019) The potential human cost of cyber operations. 29 May 2019 https://www.icrc.org/en/document/potential-human-cost-cyber-operations

[9] Genovese, M. (2019) Top 5 cyberattacks against the health care industry, 26 August 2019, Stormshield, 26 August 2019, https://www.stormshield.com/news/top-5-cyberattacks-against-the-health-care-industry/

[10] Farr, C. (2020) Cyberattack on NRC Health sparks privacy concerns about private patient records stored by US hospitals. CNBC News, 20 February 2020. https://www.cnbc.com/2020/02/20/nrc-health-cyberattack-sparks-privacy-concerns-about-patient-records-in-us.html

[11] Dyrda. L (2020) What hospital CIOs are doing differently in 2020 to combat cyberattacks — it may not be tech related. Becker's Health IT, 14 February 2020 https://www.beckershospitalreview.com/cybersecurity/what-hospital-cios-are-doing-differently-in-2020-to-combat-cyberattacks-it-may-not-be-tech-related.html

[12] Security Magazine (2020) Greatest Cybersecurity Threats Facing Healthcare Networks in 2020 18 February 2020, https://www.securitymagazine.com/gdpr-policy?url=https%3A%2F%2Fwww.securitymagazine.com%2Farticles%2F91751-greatest-cybersecurity-threats-facing-healthcare-networks-in-2020

[13] Eddy, N (2020) Coronavirus outbreak triggers wave of apps, online tools for diagnosis, testing Healthcare IT News. 16 March 2020, https://www.healthcareitnews.com/news/coronavirus-outbreak-triggers-wave-apps-online-tools-diagnosis-testing

[14] Milliard, M. (2020) Trump administration expands Medicare telehealth benefits for COVID-19 fight. Healthcare IT News. 17 March 2020, https://www.healthcareitnews.com/news/trump-administration-expands-medicare-telehealth-benefits-covid-19-fight

[15] Kaspersky (2017) What is WannaCry ransomware? https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

[16] Smart, William. Lessons learned review of the WannaCry Ransomware Cyber Attack. London: National Health Service, 2018 s. 5 & s. 14. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learnedreview-wannacry-ransomware-cyber-attack-cio-review.pdf

[17] Interpol (2020) Cybercriminals targeting critical healthcare institutions with ransomware. 4 April 2020 https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

[18] Stone, J. (2020) Ransomware strikes biotech firm researching possible COVID-19 treatments. Cyberscoop, 2 April 2020. https://www.cyberscoop.com/covid-19-ransomware-10x-genomics-data-breach/

There is rapidly growing dependency of IT solutions, internet of things (IoT) in telemedicine[19], tele-communication, tele-training/education[20] and tele-information,[21] recently in tests for Bluetooth-tracking of Covid-19.[22] The trend is that complex IT supply chains is subject to increased security and safety concerns. Healthcare data is furthermore especially vulnerable to cyberattacks, with risk of individuals being identified even from anonymised data.

Also, indirect vulnerabilities in the healthcare chain has increased, related to increased use of IT-solutions in other critical infrastructure e.g. the energy, water and transport sectors.[23, 24] On April 3rd 2020, in the daily national Covid-19 brief, vulnerabilities regarding cyberattacks, and dependencies on essential personnel, was highlighted by The Swedish Civil Contingencies Agency (MSB).[25]

Trojans, Phishing and Watering hole-attacks

Social engineering is the term used for when an attacker attempts to get a victim to take actions that seem reasonable, but in fact result in a security breach. In general terms, it is what con artists and fraudsters have done since time immemorial. A crisis such as the Covid-19 pandemic opens up an opportunity for social engineering attacks. People will be worried, emotionally vulnerable and actively looking for information about a subject they have little prior knowledge about. The attackers thus have a greater than normal chance of getting victims to access websites, download software, and open emails than in a normal situation. Also, the large numbers of people working from home, connected to their workplace by the internet will result in a dramatic increase in security lapses as the home setup have not been designed for use in a corporate environment, and few users have been trained in security measures outside the office.

Since the outbreak of Covid-19 began, attackers have created many tens of thousands[26] of websites that masquerade as legitimate healthcare information sites where they offer

---

[19] Siwicki, B (2020) Health system uses telehealth to steer patients away from ER, urgent care Healthcare IT News. 17 March 2020, https://www.healthcareitnews.com/news/health-system-uses-telehealth-steer-patients-away-er-urgent-care

[20] SVT DIREKT 14.00h Covid update March 18th 2020 MSB highlights the risk of frauds via email, as work and education becomes home based due to Covid19.

[21] Holmes, A. (2019) The rise of cyber attacks and data breaches against US hospitals has been linked to an uptick in heart attack deaths. Business Insider 13 November 2019. https://www.businessinsider.com/cyber-attacks-hospitals-rise-in-heart-attack-deaths-study-2019-11?r=US&IR=T

[22] PI (2020) Bluetooth tracking and COVID-19: A tech primer, https://privacyinternational.org/explainer/3536/bluetooth-tracking-and-covid-19-tech-primer

[23] Collier, K (2020) Prepared for the worst, electrical grid workers isolate as coronavirus spreads. NBC News 31 March 2020 www.nbcnews.com/tech/security/prepared-worst-electrical-grid-workers-isolation-coronavirus-spreads-n1173171

[24] The seven prioritised sectors are: Energy supplies, Food and water resources, Transportation systems, Healthcare and welfare, Information and telecommunications networks, Security and Safety, Financial services, see MSB (Myndigheten för samhällsskydd och beredskap, 2017) Nationell risk- och förmågebedömning 2017, April 2017

[25] SVT Direkt 14.00h Covid-19 update April 3rd 2020 news public information by MSB regarding critical infrastructure and telecom in healthcare (SVT)

[26] ZdNet (2020) Thousands of COVID-19 scam and malware sites are being created on a daily basis, 18 March 2020 https://www.zdnet.com/article/thousands-of-covid-19-scam-and-malware-sites-are-being-created-on-a-daily-basis/

software that can track the spread of the illness but that are actually ransomware[27,28] or other kinds of Trojan horses.

The Trojan Horse can be embedded in an app. Many people have gotten used to downloading apps for temporary needs they have, such as finding local restaurants, shopping tips, gardening and so on. A crisis will inevitable result in many thousands of people automatically searching for apps using some search terms that seem fitting.

The attackers know this and hence a large number of various malware-delivering apps appeared on the internet almost as soon as the first headlines about the Covid-19.

Figure 1. Ad for an app that contained a Malware called Cerberus designed to steal banking and credit card information.

In order to make the apps as attractive as possible, several of the attacks have been designed around real information services.

One such example was an app called the Covid-19 Tracker (see Figure 1), which claimed to offer a real-time map tracking the virus spread. In reality, the malware website showed data from a totally different web service, infection2020.com, and the download offered was ransomware that locked the user out from their phones.

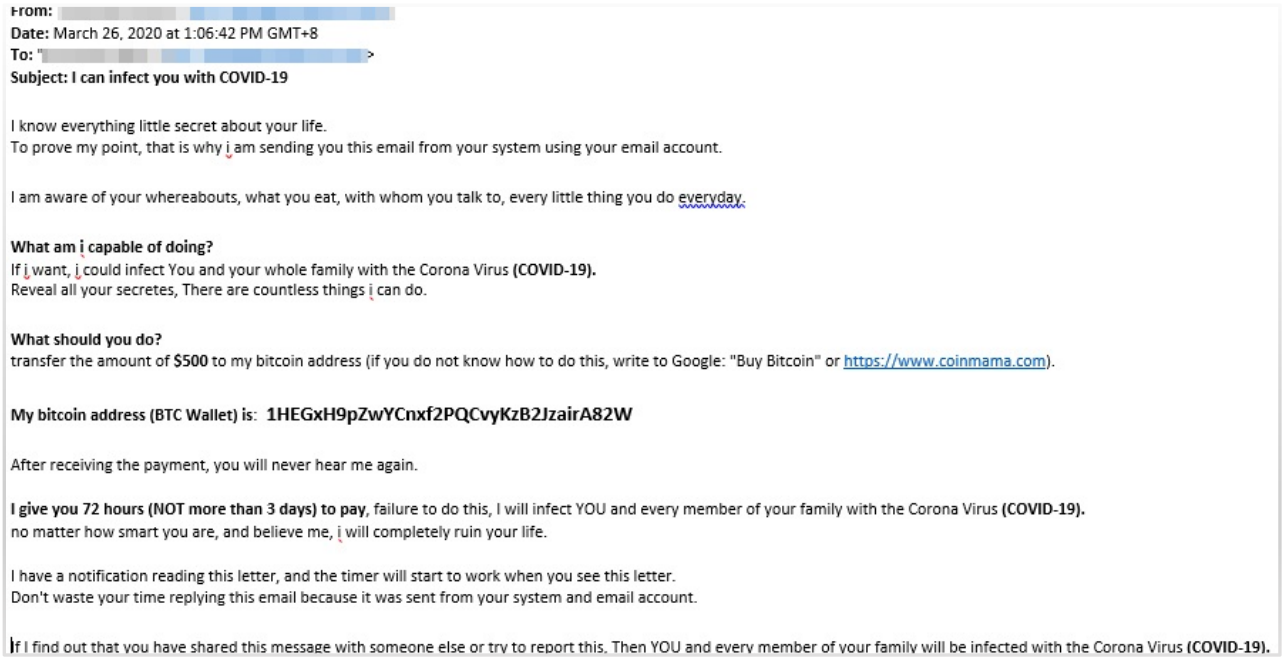
The attackers thus take advantage of how people download apps from various sources as a daily remedy for specific information needs. And as the normal ecosystem of app-makers produce hundreds of legitimate apps to cater to this need, the malware app makers do too.

[27] Stefanko, L. (2020) Android – Coronavirus – related malware tracker. March 17, 2020 https://lukasstefanko.com/2020/03/android-coronavirus-malware.html

[28] Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Cyberattacks and phishing in the healthcare sector have been reported in e.g. the United States, France, Spain and Thailand.[29,30] On March 13th 2020, a major hospital in Brno, Czech Republic, in charge of administrating Covid-19 tests, was hit by a cyberattack. The attack resulted in a need to shut down the IT network, reportedly with impact on surgical operations, a need to reroute acute patients and the delay of administrating Covid-19 tests by several days.[31]

One example of Covid-19 email extortion is seen in Figure 2, where the receiver and its family was threatened to be infected by Covid-19, unless paying 500 dollar in bitcoin.[32]



From: [redacted]
Date: March 26, 2020 at 1:06:42 PM GMT+8
To: [redacted]
Subject: I can infect you with COVID-19

I know everything little secret about your life.
To prove my point, that is why i am sending you this email from your system using your email account.

I am aware of your whereabouts, what you eat, with whom you talk to, every little thing you do everyday.

What am i capable of doing?
If i want, i could infect You and your whole family with the Corona Virus **(COVID-19).**
Reveal all your secretes, There are countless things i can do.

What should you do?
transfer the amount of **$500** to my bitcoin address (if you do not know how to do this, write to Google: "Buy Bitcoin" or https://www.coinmama.com).

My bitcoin address (BTC Wallet) is: 1HEGxH9pZwYCnxf2PQCvyKzB2JzairA82W

After receiving the payment, you will never hear me again.

I give you 72 hours (NOT more than 3 days) to pay, failure to do this, I will infect YOU and every member of your family with the Corona Virus **(COVID-19).**
no matter how smart you are, and believe me, i will completely ruin your life.

I have a notification reading this letter, and the timer will start to work when you see this letter.
Don't waste your time replying this email because it was sent from your system and email account.

If I find out that you have shared this message with someone else or try to report this. Then YOU and every member of your family will be infected with the Corona Virus **(COVID-19).**

Figure 2. An example of Covid-19 email extortion.

A recent Europol report on the development of Covid-19[33] highlights how criminals has seized opportunities to exploit the Covid-19 crisis, and adapted their modus operandi. As an example, perpetrators gain access to private homes by impersonating medical staff, providing Covid-19 tests, hygiene products or information. The Interpol Operation Pangea, that took place in March 2020, confiscated over 34 000 counterfeit masks, "corona sprays" and other counterfeit products purportedly for protection against the corona virus.

---

[29] Gisel, L. et al (2020) Cyber attacks against hospitals and the COVID-19 pandemic: How strong are international law protections? Humanitarian Law and Policy. April 2, 2020, https://blogs.icrc.org/law-and-policy/2020/04/02/cyber-attacks-hospitals-covid-19/
[30] EUROPOL: Pandemic profiteering how criminals exploit the COVID-19 crisis March 2020, https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic
[31] Scoxton. A. (2020) Coronavirus-linked hacks likely as Czech hospital comes under attack. Computer Weekly, 13 March 2020, https://www.computerweekly.com/news/252480022/Coronavirus-linked-hacks-likely-as-Czech-hospital-comes-under-attack
[32] Trend Micro (2020) Developing Story: COVID-19 Used in Malicious Campaigns, 2 April 2020 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains
[33] Ibid

Criminals have used the Covid-19 crisis to carry out social engineering attacks themed around the pandemic to distribute various malware packages. Criminals aiming to exploit the Covid-19 situation also leverage the fact that there will a high demand for certain goods, such as individual protective gear and selected pharmaceutical products. Increased anxiety and fear from the new situation may thus create new vulnerabilities to specific online exploitation in this field. Also, as citizens increasingly are teleworking from home, people will rely on digital solutions, and thus displacing people to less secure online settings than would be in a normal workplace.

Piggybacking trust

In order to increase the trust in the malicious apps, many attackers try to add some kind of quality assurance to the apps. Examples include sending emails purporting to be from the WHO advising readers that in order to gain vital information about how to stay safe from the virus they should use the link in the mail to go to (a fake version of) the WHO website to download an app.[34]

This tactic, to fraudulently pose as trusted organisations, have been used in several variations, from setting up fraudulent copies of websites like the WHO example above, to sending out emails claiming to be from FedEx (Fedex Corporation) offering information about changes in deliveries.[35]

It appears that the majority of attacks have been either simple fraud, sending out mass emails with malware-laced files, or setting up fake websites where the victim is directed through malicious links. However, there has also been a number of more advanced attacks such as attacking routers from D-link and Linksys to change their DNS-settings. This results in a user typing a web address being sent to the attackers' website rather than the intended.[36] These attacks are typically not targeted against specific individuals or organisations, but "to whom it may concern". As such the main motivator seems to be monetary gain.[37]

Politically motivated attacks

A number of attacks have been attributed to state actors.[38] For instance, several targets in Ukraine received emails purportedly sent from the Ukraine Centre for Public Health, containing documents regarding Covid-19 research, but infected with malware. The

[34] Meyers, A (2020) Situational Awareness: Cyber Threats Heightened by COVID-19 and How to Protect Against Them. Crowdstriek Blog, 24 March 2020, https://www.crowdstrike.com/blog/covid-19-cyber-threats/
[35] Saengphaibul, V. & Gutierrez; F. (2020) Attackers Taking Advantage of the Coronavirus/ COVID-19 Media Frenzy, Fortinet Blog, March 04, 2020, https://www.fortinet.com/blog/threat-research/attackers-taking-advantage-of-the-coronavirus-covid-19-media-frenzy.html
[36] Davis, J. (2020) COVID-19 Cyber Threats: Hackers Target DNS Routers, Remote Work, Health IT Security, March 27, 2020 https://healthitsecurity.com/news/covid-19-cyber-threats-hackers-target-dns-routers-remote-work
[37] Meyers, A (2020)
[38] Attributed in this case simply means that some organisation and/or state has made the claim. No independent verification of these claims have been made by the FOI.

attack was attributed to the Hades group[39], thought to be a Russian government sponsored hacking group.[40] At the same time, what appears to be a coordinated attempt to foment unrest, took place when a mass email campaign orchestrated from abroad[41] spreading rumours about the spreading of Covid-19 by evacuees from China. This, in combination with posts on social media, led to panic and riots in parts of the country.[42]

The same tactics, using a fake trusted source sending what looks like Covid-19 information, has also reportedly been used by Pakistani-linked[43] APT36 masquerading as the Indian government, by the North Korean Intelligence services[44] to imitate the South Korean CDC (Centre for Disease Control), and the Chinese-sponsored[45] Mustang Panda group, to impersonate the Vietnamese Prime Minister.

Conclusions

The Covid-19 pandemic has resulted in an unprecedented increase of cyberattacks, including, among many other, ransomware attacks linked to downloading of malicious "fake" apps for Covid-19 information. Why?

In modern society, citizens will react to uncertainty by searching for information, often online, and by downloading apps offering information or services to handle the situation. However, the users of these apps have very limited ability of knowing which apps are malicious or not, nor which websites are to be trusted. Technically naïve users may not even know the attacks outlined above are possible.

The similarity regards to the Wannacry example is worth repeating. If the hospitals and healthcare facilities are not adequately protected from malware sent by email or downloaded from other networks they risk degraded, or disrupted operations. And if the persons within the healthcare sector are not adequately trained in cyber hygiene they risk cross contaminating hospital systems with their personal devices by e. g. charging smart phones by connecting them to hospital computers. It is therefore vital that all healthcare personnel receive such training well ahead of time.

It follows that a crisis of any kind where the population feels worried and/or threatened and in need of information gives rise to a very target-rich environment for attackers.

---

[39] Healthcare Purchasing News (2020), State-sponsored hackers using coronavirus lures to infect their targets, March 16th, 2020 https://www.hpnonline.com/infection-prevention/crisis-planning-outbreak-response/article/21129791/statesponsored-hackers-using-coronavirus-lures-to-infect-their-targets

[40] APT28: A Window into Russia's Cyber Espionage Operations? https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf

[41] Arciga, J. (2020) Coronavirus Disinformation Sparked Violent Protests in Ukraine February 20, 2020 https://www.thedailybeast.com/coronavirus-disinformation-sparked-violent-protests-in-ukraine

[42] Coronavirus: Ukraine protesters attack buses carrying China evacuees, 21 February 2020, https://www.bbc.com/news/world-europe-51581805

[43] AlwarebytesLab (2020) jumps on the coronavirus bandwagon, delivers Crimson RAT, March 16, 2020, https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/

[44] IssueMakersLAb (2020) Tweet 1 April 2020, https://twitter.com/issuemakerslab/status/1245335214252933123

[45] Healthcare Purchasing News (2020)

Psychological operations, misinformation spread, espionage, ransomware extortion among others are attacks that are greatly facilitated by this situation.

It also follows that the channels of information that society might use in order to provide health-related information are under direct threat. If the public starts to distrust the channels used by legitimate health information services, or other authorities, they will not access it. If the channels can be imitated, or the communication diverted, as in the examples above, the public can be misled and victimised.

We can expect any major crisis in the future to be followed by large numbers of social engineering attacks combined with more technical cyberattacks. The actors are likely to be both common criminals and politically motivated actors. Examples where criminals and politically motivated actors work together cannot be ruled out either.

There is a need, but also an opportunity, to begin to learn from the direct and indirect cyber related impacts of the Covid-19 pandemic, on the wider healthcare system, in order to be better prepared for future disruptions.

It is among other things recommended that research is performed regarding what measures can be taken to mitigate or stop future attacks. Potential measures are e.g. the establishment of pre-arranged secure information channels, information campaigns about how to access them, how to avoid misinformation and legal requirements for app suppliers to have robust vetting of crisis apps.

Indeed, the future use of digital systems will demand a great deal from the healthcare sector, especially during a global pandemic such as Covid-19. In order to secure their digital systems against cyber threats a holistic approach with many layers of overlapping activities must be in place.

This brief will be followed by an update from ongoing work, regarding cyber-aspects of the Covid-19 pandemic and the healthcare sector.