UNIVERSITY OF CAMBRIDGE

Cambridge Cybercrime Centre
COVID Briefing Paper # 21

Cyberattacks on Healthcare Systems During the COVID-19 Pandemic

Maria Bada

8 December 2020

Executive summary

CCC COVID Briefing Papers are an ongoing series of short-form, open access reports aimed at academics, policymakers, and practitioners, which aim to provide an accessible summary of our ongoing research into the effects which the coronavirus pandemic (and government responses) are having on cybercrime.

In this report, we discuss cyberattacks on healthcare systems during the COVID-19 pandemic, noting that some are merely profit-driven, whilst others appear to have been performed for strategic advantage. Policy responses have been limited and have failed to make this distinction.

Ransomware and healthcare

Healthcare systems have suffered from ransomware attacks for some time and the effects have often been substantial, with the NHS notably suffered serious outages during the 2017 WannaCry incident. However, since the beginning of the COVID-19 pandemic we have witnessed a surge in reporting of cyberattacks on healthcare systems. It is unclear the extent to which this reporting reflects actual levels of attacks in different sectors (because of the relative importance of healthcare). It is certainly the case that although some of these attacks have been extremely successful, defenders have thwarted some very significant attempts at compromising institutions within this sector.

Ransomware attacks have been evolving recently. Malware is used to gain control of networks and data is then exfiltrated before the original copy is encrypted. The ransom demand is then not only for the restoration of the data, which an organisation with good backups can ignore, but also for destroying the data copy rather than publishing it on the Internet with consequent reputational damage. The substantial amounts of money, sensitive data, and the importance of continued operation has made some healthcare sectors prime targets.

For example, in March 2020 a cyberattack took down the network of a Czech hospital which was one of Czech Republic's biggest COVID-19 testing laboratories [3]. In the same month a ransomware attack on a vaccine trial group in UK led to the publication of personal details of former patients, but it failed in its attempt to disable the network [2].

The groups who carry out these attacks continue to innovate, and in October 2020 a serious data breach in Finland affected the records of thousands of psychotherapy patients [5] and some of the confidential information was leaked online. Shocked patients were then asked to pay individual bitcoin ransoms to prevent the contents of their discussions with therapists being made public.

Industrial espionage

In parallel with these ransomware attacks there have also been cyberattacks targeting research institutions working on COVID-19 related research and intellectual property associated with COVID-19 vaccine development [4]. Recently, there were reports of attempts by hackers to obtain details of the COVID-19 vaccine 'cold chain' [1] and a global phishing campaign was launched targeting organisations associated with the distribution of COVID-19 vaccines [8]. These attacks seem less driven by profit, instead indicative

of corporations and countries looking to gain a strategic advantage or perhaps to short-cut their own research activities. To the extent that this is seen as nation state activity there is a risk of causing an increase in geopolitical tensions, potentially leading to sanctions or retaliation – a situation clearly at odds with widespread calls by world leaders for collaboration between all nations in tackling the pandemic.

Policy developments

There have been several policy initiatives in response to these security incidents in the healthcare sector and as an example the 'Paris Call for Trust and Security in Cyberspace' [7] has been signed by a number of health care-related organizations. Its first principle is the *"prevention of malicious cyber activities that threaten indiscriminate or systemic harm to people and critical infrastructure"*.

In addition, in May, a 136-strong group of the world's most prominent international law experts, in what has become known as the Oxford Process [6], issued a statement making it clear that international law protects medical facilities at all times, emphasizing that organizations that research, manufacture and distribute COVID-19 vaccines are also protected.

Conclusions

There has been an increase in reports of cyberattacks on healthcare systems during the COVID-19 pandemic. A ransomware trend towards exfiltrating and publishing data whilst encrypting the master copy has accelerated in this time of crisis and it is clear that more collective action is needed. At the same time we've seen a rise in corporate or state level espionage – which may prove more tractable to a policy response – and we've outlined two current initiatives that could potentially make some difference to this aspect of the problem.

References

[1] BBC. *Coronavirus: Hackers targeted Covid vaccine supply 'cold chain'*. 2020. URL: https://www.bbc.co.uk/news/technology-55165552.

[2] ComputerWeekly.com. *Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack*. 2020. URL: https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus.

[3] Grierson J, Devlin H. *Hostile states trying to steal coronavirus research*. 2020. URL: https://www.theguardian.com/world/2020/may/03/hostile-states-trying-%20to-steal-coronavirus-research-says-uk-agency.

[4] Menaka Muthuppalaniappan and Kerrie Stevenson. "Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health". In: *International Journal for Quality in Health Care* (Sept. 2020). DOI: 10.1093/intqhc/mzaa117.

[5] The Guardian. *'Shocking' hack of psychotherapy records in Finland affects thousands*. 2020. URL: https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland.

[6] The Oxford Institute for Law, Ethics and Armed Conflict (ELAC). *The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector*. 2020. URL: https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea.

[7] The Paris Call. *Paris Call for Trust and Security in Cyberspace*. 2020. URL: https://pariscall.international/en/.

[8] The Verge. *Hackers are targeting the COVID-19 vaccine supply chain, IBM finds*. 2020. URL: https://www.theverge.com/2020/12/3/22151016/hackers-phishing-coronavirus-vaccine-ibm-security.

At the Cambridge Cybercrime Centre we make our research data available to other academics, sometimes before we have looked at it ourselves! Researchers can be provided access to our 'CrimeBB' dataset of (26 and counting) underground cybercrime forums, our extensive collections of chat channel data, and our new collections of forums relating to online right-wing extremism and radicalisation. We can also share email spam and sensor data related to DDoS and IoT malware. All these collections are regularly updated and can be rapidly provided under licence – for full details see: https://cambridgecybercrime.uk

---

The full set of CCC COVID Briefing Papers can be found at: https://cambridgecybercrime.uk/COVID