August 24th, 2021

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* begins with a look at how law enforcement's improved capabilities in tracing ransomware cryptocurrency payments, and their recent successes in degrading criminal cryptocurrency infrastructure, is incentivizing the evolution of new criminal services. Next, we highlight the importance of good cybersecurity communication by examining a recent SEC settlement against Pearson plc. Finally, we wrap up with a brief breakdown of a new healthcare sector cybersecurity report and use it as a springboard for a thought exercise.

Welcome back to *Hacking Healthcare*.

1. Law Enforcement's Cryptocurrency Gains Force Criminal Rethink

Law enforcement's battle with cybercriminals, particularly with ransomware perpetrators, remains an uphill battle. International legal complications and sophisticated technical challenges continue to negatively impact response effectiveness. However, law enforcement has made tangible gains in recent months and now criminal actors have started looking for ways to respond to these new tactics.

One of the acknowledged difficulties in tackling ransomware is the prevalence of ransoms demanded in cryptocurrency. Criminal actors generally have a preference for this method of payment due to the belief that it is far more difficult for regulators, law enforcement, and others to trace and identify the individuals involved. This has made cryptocurrency and its surrounding infrastructure a crucial element of the cybercriminal ecosystem.

The sense of anonymity is not entirely misplaced, but law enforcement has recently had a number of notable successes in tracing and recovering ransomware payments, as well as prosecuting individuals helping to launder the digital currencies. The most notable of these may be recovery of a large portion of the ransom paid by Colonial Pipeline in June. The Department of Justice (DOJ) was able to ultimately seize $2.3 million in cryptocurrency related to the ransom and experts have stated this shows "how successful U.S. law enforcement has been in developing the capacity to execute this sort of complex operation using blockchain analysis in real time."[1]

Other notable actions include the recent Justice Department case against an American who pleaded guilty to operating “Helix,” a “darknet-based bitcoin service that laundered over $300 million,” and the U.S. arrest of Roman Sterlingov, a Russian-Swedish national, who is believed to be the “operator of Bitcoin Fog, a cryptocurrency-obfuscation service.”[2, 3]

In response, cybercriminals have been actively searching for ways to better evade law enforcement’s improved capabilities and *Antinalysis* is a perfect example of this. The service is designed to help users understand the risk of their crypto funds being flagged as being related to criminal activity. In theory, this should help criminals trying to launder ransomware payments avoid the kinds of analysis tools used by law enforcement.[4] While there are questions about how effective the service is in its current form, the potential value is obvious and it wouldn’t be surprising to see the idea improved upon or copied in the near future.[5]

Action & Analysis

2. The Importance of Good Cybersecurity Communication

Last week, Pearson plc, a “London-based public company that provides educational publishing and other services to schools and universities,” agreed to settle charges with the SEC amounting to $1 million for misleading investors about a 2018 cyber intrusion.[6] The result is a high-profile example of an organization paying a price for not carefully communicating cybersecurity matters in an honest and understandable manner.

The case stems from a 2018 data breach that involved “the theft of student data and administrator log-in credentials of 13,000 school, district, and university customer accounts.”[7] Despite the fact that Pearson knew of the incident, their next semi-annual report described “a data privacy incident as a hypothetical risk,” and that the hypothetical “breach may include dates of births and email addresses, when, in fact, it knew that such records were stolen.”[8]

Furthermore, Pearson stated that they “had ‘strict protections’ in place, when, in fact, [they] failed to patch the critical vulnerability for six months after [being] notified,” and “Pearson's disclosure controls and procedures were not designed to ensure that those responsible for making disclosure determinations were informed of certain information about the circumstances surrounding the breach.”[9] Ultimately, the SEC found that Pearson did not disclose that a breach had occurred until after the media had reached out for comment and “even then Pearson understated the nature and scope of the incident, and overstated the company's data protections.”[10]

Action & Analysis

3. New Philips Study Raises Thought Exercise for Healthcare Senior Management

A new study that “examines attitudes, concerns, and impacts on medical device security as well as cybersecurity across large and midsize healthcare delivery organizations” raises a number of interesting questions for senior management to consider.[11]

Sponsored by Philips and CyberMDX, the 16-page report is the product of a survey of 130 experienced “hospital executives in Information Technology (IT) and Information Security (IS) roles, as well BioMed technicians and engineers.”[12] Some of their findings reiterate longstanding trends, but others may surprise you. Some of the more interesting and important findings include:[13]

- 48% of hospitals reported either a forced or proactive shutdown in the last six months as a result of external attacks or queries
- Less than 11% reported cybersecurity as a high priority spend for their organization
- A majority of respondents reported they were “unprotected” against long-known vulnerabilities like BlueKeep, WannaCry, and NotPetya
- Midsized hospitals experienced significantly longer downtime (~10 hours) and costs ($45,700) associated with shutdowns caused by external factors than their larger counterparts (6.2 hours - $21,500)
- A plurality of biomedical engineers (30%) expected that medical device security protection is expected from the medical device manufacturer, while a plurality of IT personnel (37%) expected it from the IoT/medical device security solution provider
- Two out of three respondents do not track return on investment for cybersecurity spending

The report is freely available and filled with other information that members may find valuable.

Action & Analysis

Congress –

<u>Tuesday, August 24th</u>:
- No relevant hearings

<u>Wednesday, August 25th</u>:

August 24th, 2021

- No relevant hearings

Thursday, August 26th:
- No relevant hearings

International Hearings/Meetings –
- No relevant meetings

EU –

Conferences, Webinars, and Summits –

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

[1] https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/colonial-pipeline-ransom-funds/

[2] https://www.justice.gov/usao-dc/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300

[3] https://www.cyberscoop.com/bitcoin-fog-arrest-roman-sterlingov/

[4] https://krebsonsecurity.com/2021/08/new-anti-anti-money-laundering-services-for-crooks/

[5] https://www.bbc.com/news/technology-58176113

[6] https://www.sec.gov/news/press-release/2021-154

[7] https://www.sec.gov/news/press-release/2021-154

[8] https://www.sec.gov/news/press-release/2021-154

[9] https://www.sec.gov/news/press-release/2021-154

[10] https://www.sec.gov/news/press-release/2021-154

[11] https://www.cybermdx.com/lp-perspectives-in-healthcare-security-ipsos-report/

[12] https://www.cybermdx.com/lp-perspectives-in-healthcare-security-ipsos-report/

[13] https://www.cybermdx.com/lp-perspectives-in-healthcare-security-ipsos-report/