October 27th, 2020

TLP White

This week, *Hacking Healthcare* dives into a less talked about aspect of U.S.–China relations, specifically, the possible detainment of American citizens as a diplomatic reprisal. We dive into how this move could affect healthcare organizations, as well as just how likely such an action might be. Next, we examine the European Union Agency for Cybersecurity's (ENISA) recent publication of their 2020 *Threat Landscape* report. The various documents that comprise this year's report take an extensive look at the current cyber threat landscape and help to highlight some areas that healthcare should be paying attention to. Lastly, we examine an attack on a Finnish healthcare organization that's making headlines for its perpetrator's tactics. Welcome back to *Hacking Healthcare*.

1. **Newest Twist in U.S.–China Tensions Creates Risk for American Businesses and Citizens.**

   The more recent bouts of political and economic sparring between the United States and China have highlighted intellectual property (IP), research, and trade secret theft as a significant issue area. The United States has repeatedly accused China of using in-person and cyber capabilities to steal valuable research from a variety of sectors often related to defense industries and emerging technologies. More recently, this has extended to include research related to COVID-19 and vaccine development. While these accusations and their accompanying diplomatic responses have generally resulted in refutations and tit-for-tat reactions, the newest development in this saga may have significant repercussions for healthcare sector entities operating in China.

   While the cyber component of Chinese research and IP theft is often decried, there is a limit to what can be feasibly done to halt it. This limitation does not extend to Chinese nationals that are accused of coming to the country under the pretense of engaging in genuine research and development only to steal valuable trade secrets and research data. The Trump administration has been particularly concerned with "Chinese postgraduate researchers in areas such as biomedicine and artificial intelligence," who they view as being part of "an intelligence-gathering operation aided by Chinese diplomats to collect cutting-edge scientific research from American universities."[1]

   In an effort to address the issue, the Trump administration began taking diplomatic and legal action this year to disincentivize such behavior. It has been reported by some that

the closure of the Chinese consulate in Houston was part of this retaliation.[2] Since then, the United States government has started investigating and charging Chinese researchers they say have concealed their affiliation with the Chinese military and who are acting in bad faith. Predictably, this has provoked a serious Chinese response.

In mid-October, the Wall Street Journal reported that Chinese officials have "repeatedly and through multiple channels" warned their United States government counterparts that if the "prosecution of Chinese military-affiliated scholars" continues, "Americans in China might find themselves in violation of Chinese law."[3] In other words, China may begin to arrest or otherwise detain American citizens on suspect charges. This development could pose a significant risk to American businesses and American citizens in China.

Action & Analysis
H-ISAC Membership Required

2. ENISA Publishes Threat Landscape 2020

Last week, ENISA published its annual *Threat Landscape* reports for 2020.[4] The dozens of pages that make up these extensive reports and infographics are invaluable to all organizations in helping to illustrate various trends in the cyber threat landscape. These reports are freely available, and we encourage everyone to have a look themselves if you haven't already. However, for those without much time, we have gone through the reports to highlight some of the key takeaways and important trends that everyone should be aware of. It should be noted that these reports are based on data from January 2019 through April 2020 and will not reflect more recent trends.

ENISA's Top Threats in 2020[5]

This one-page infographic is an excellent at-a-glance reference for ENISA's view of 2020's cyber threats. The top-five, in order, are malware, web-based attacks, phishing, web application attacks, and spam. Identity and unauthorized access appear to be on the rise, as phishing (#3) identity theft (#7), and insider threats (#9), make up three of the five categories trending up. Lastly, despite routinely making headlines, ransomware comes in 13th, although it too is trending up and likely to make a quick rise in the rankings in the next iteration.

Threat Landscape Mapping[6]

Another useful one-page infographic, the *Threat Landscape Mapping* document is an easily digestible breakdown of the "exploitation by cybercriminals and advanced persistent threat (APT) groups of the current coronavirus (COVID-19) global pandemic." The mapping provides a concise description of the delivery, exploitation, installation, and objectives of various threats.

Emerging Trends[7]

The twenty-page emerging trends report highlights ten cybersecurity challenges, four general emerging trends, five trends with cyber threats, and ten trends in attack vectors. While you can read more in-depth coverage in the report itself, the top three items of each category are:

Cybersecurity Challenges

1. Dealing with systemic and complex risks
2. Widespread use of adversarial AI detection
3. Reduction of unintentional errors

General Trends

1. Growth in cybersecurity spending
2. Usefulness of cyber threat intelligence to inform cyber strategies
3. The shortage of cyber talent

Cyber Threats

1. Malware evolution and increasing sophistication
2. Increase in threats to mobile devices
3. Increased usage of new file types (ISO, IMG)

Trends in Emerging Attack Vectors

1. Attacks will be massively distributed with a short duration and a wider impact
2. Finely targeted and persistent attacks will be meticulously planned with well-defined and long-term objectives
3. Malicious actors will use digital platforms in targeted attacks

Sectoral and Thematic Threat Analysis[8]

The twenty-two-page report does not get overly detailed, but quickly tackles numerous sectors and themes. For healthcare, the report reiterates that incidents are increasing, and they list malware, insider threats (unintentional abuse/error), and web application attacks as the most prevalent threats. Furthermore, the report cites “financial motives and the importance of the sector during COVID-19 pandemic” as the main influencing factors driving the increased targeting.

Action & Analysis

H-ISAC Membership Required

3. **Healthcare Records Ransomed Directly**

   A significant data breach of the Vastaamo psychotherapy center, a sub-contractor for Finland's public health system, has caused an uproar in the country. Reports suggest that while the initial breach may have happened as long as two years ago, malicious actors are only now attempting to take advantage of it.[9] A noteworthy and concerning development in this case is the manner in which the malicious actors are trying to profit.

   According to media reports, the perpetrators are alleged to have exfiltrated roughly 40,000 patient records and made a demand of around 450,000 Euros to not release them.[10] Undeterred by the organizations' refusal to pay, the perpetrators have allegedly begun to post the patient records on the dark web and have started offering to remove records if the affected individuals pay around 500 Euros themselves.[11] Reports suggest that the perpetrators are directly contacting affected individuals through Tor to deliver their offer.

   Action & Analysis
   H-ISAC Membership Required

U.S. Congress –

Tuesday, November 27th:
- No relevant hearings

Wednesday, October 28st:
- No relevant hearings

Thursday, October 29th:
- No relevant hearings

International Hearings/Meetings –

- No relevant hearings

EU –

Wednesday, October 28st:
European Parliament - Committee on the Environment, Public Health and Food Safety

Thursday, October 29th:
European Parliament - Committee on the Environment, Public Health and Food Safety

Sundries –

Report Heralds Perfect Storm for Insider Threats in 2021
https://www.nextgov.com/cybersecurity/2020/10/report-heralds-perfect-storm-insider-threats-2021/169555/

EU slaps sanctions on GRU leader, Fancy Bear, FBI-wanted hacker over Bundestag attack.
https://www.cyberscoop.com/eu-gru-fancy-bear-bundestag-russia/

FDA leader talks evolving strategy for AI and machine learning validation
https://www.healthcareitnews.com/news/fda-leader-talks-evolving-strategy-ai-and-machine-learning-validation

October 27th, 2020

Conferences, Webinars, and Summits –
https://h-isac.org/events/

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

---

[1] https://www.wsj.com/articles/chinese-diplomats-helped-visiting-military-scholars-in-the-u-s-evade-fbi-scrutiny-u-s-says-11598379136
[2] https://www.wsj.com/articles/chinese-diplomats-helped-visiting-military-scholars-in-the-u-s-evade-fbi-scrutiny-u-s-says-11598379136
[3] https://www.wsj.com/articles/china-warns-u-s-it-may-detain-americans-in-response-to-prosecutions-of-chinese-scholars-11602960959
[4] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends
[5] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape-2020-top-15-threats
[6] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/threat-landscape-mapping-infographic-2020
[7] https://www.enisa.europa.eu/publications/emerging-trends
[8] https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis
[9] https://abcnews.go.com/Health/wireStory/finland-shocked-therapy-center-hacking-client-blackmail-73817011
[10] https://www.cyberscoop.com/finnish-psychotherapy-data-breach-vastaamo/
[11] https://www.cyberscoop.com/finnish-psychotherapy-data-breach-vastaamo/