January 29th, 2020

TLP White

In this edition of Hacking Healthcare, we begin with an Idaho National Lab researcher that is shedding light on just how little we know about the threat of ICS (Industrial Control Systems) vulnerabilities. Next, we dive a little deeper into the world of ICS vulnerabilities by briefly examining cybersecurity organization TrendMicro's seven-month long ICS honeypot. Finally, we give you a short brief on where the UK's healthcare sector is likely to go in a post-Brexit environment.

Welcome back to *Hacking Healthcare*.

1. **Idaho National Lab Researcher Advocates for Research into Zero-day ICS Market.** Zero-day vulnerabilities, generally defined as software or hardware vulnerabilities that are unknown to the public and often the original software or hardware developer, are exceptionally valuable to malicious cyber threat actors. Exploits that are designed around these undisclosed vulnerabilities, can drastically multiply the effectiveness of a cyber attack by increasing the probability that cyber defenses will not be prepared for it. They are so valuable in fact, that late last year the firm Zerodium published a price list of zero-day exploits it was willing to purchase that ranged from $100,000 all the way up to $2,500,000.[1] Over the last few years, multiple investigations into dark web markets and forums that advertise and sell such vulnerabilities, as well as sites like Zerodium, have given researchers a good vantage point into the value of exploits and the trends that threat actors are pursuing.

   However, according to Sarah Freeman, an analyst at the Department of Energy's Idaho National Laboratory, there is a significant lack of insight into Industrial Control Systems (ICS) exploits.[2] Speaking at S4, a security conference that specializes in ICS security, Freeman made the case that a comprehensive record of zero-days that could affect ICS does not exist. This lack of knowledge is concerning due to the prevalence of ICS in critical infrastructure, including many parts of the healthcare sector.

2. **Trend Micro Created a Fake Factory to Test "Smart" Factory Cybersecurity.** One of the takeaways from the most recent S4 conference, is the growing trend of attacks that appear to target ICS.[3] ICS, as noted above, is especially prevalent in critical infrastructure sectors like manufacturing and healthcare. To better understand how these attacks take

place, what malicious actors look for in a potential target, and how often ICS intensive organizations find themselves targeted, cybersecurity company TrendMicro created a highly detailed honeypot to lure in ICS attackers so that they could be monitored.

A Honeypot is a computer or set of computer systems set up to mimic a real-world computing environment to catch malicious actors without exposing any important information or putting anyone at risk. TrendMicro created a highly believable "smart factory" that included all the components that would exist in a real manufacturing environment. They even went through the effort of creating a website with "a backstory for [their] fictitious company, which included made-up employee names, working phone numbers, and email addresses."[4]

3. **Where Does UK Healthcare Go Post-Brexit?** From our "Maybe Some Good News?" department, we look at one of the possible outcomes of the United Kingdom finally making its exit from the European Union. While it will likely be many years before the true scope and scale of the fallout is known, the Economist's Intelligence Unit recently released a report that summarized their views on what future UK life sciences might look like. This included their predictions as to what UK healthcare might prioritize in order to become and remain a global leader.

   Ultimately, the report concluded that the areas in which post-Brexit UK healthcare sector could excel included "capitalising on progress already made in collecting joined-up health data across the National Health Service (NHS); expanding the international influence of thought-leading institutions such as the Medicines and Healthcare products Regulatory Agency (MHRA) and the National Institute for Health and Care Excellence (NICE); and developing healthcare innovations that build on the UK's strengths in other areas, including financial services, creative arts and education."[5]

   The report cited how the UK was well positioned to use its reputation and historical track record of creating innovative products to focus on the development of more sophisticated medical software, mobile health apps, and medical education tools.[6] In particular, it outlined how the country now has an excellent opportunity to take advantage of "its ability to bring together cohesive health data, genomics, its expertise in clinical trials and its world-leading role in the gathering of real-world data."[7] The ability to unite data from sources such as the UK Biobank, Genomics England, NHS, and others could create one of the most expansive and useful healthcare data sets in the world. Not only would this be beneficial for crafting new health care solutions, but it would also be an intriguing incentive for researchers and healthcare organizations.

Congress –

Tuesday, January 28th:
- No relevant hearings

January 29th, 2020

Wednesday, January 29th:
- House Committee on Homeland Security – Markup - Cybersecurity Vulnerability Identification and Notification Act of 2020

Thursday, January 30th:
- No relevant hearings

International Hearings/Meetings –

EU –

-No relevant hearings

Conferences, Webinars, and Summits –

--H-ISAC Security Workshop – London, UK (2/5/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-2/
--Healthcare Cybersecurity Forum - Southern California – San Diego, CA (2/5/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/Southern_California
--Global Cyber Security in Healthcare & Pharma Summit - London, UK (2/6/2020)
http://www.global-engage.com/event/cybsec-health-summit/
--H-ISAC Analysts Security Workshop - Titusville, FL (3/4/2020)
https://h-isac.org/hisacevents/h-isac-analysts-security-workshop-titusville-fl/
--H-ISAC Security Workshop - Chennai, India (3/27/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-india/
--2020 APAC Summit – Singapore (3/31/2020-4/2/2020)
https://h-isac.org/summits/apac-summit-2020/
--H-ISAC Security Workshop - Cambridge, MA (4/7/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-cambridge-ma/
--H-ISAC Security Workshop - Atlanta, GA (4/14/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-atlanta/
--Healthcare Cybersecurity Forum - Mid-Atlantic – Philadelphia, PA (4/20/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426497
--H-ISAC Security Workshop - Frederick, MD (6/9/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-frederick-md/
--Healthcare Cybersecurity Forum - Rocky Mountain – Denver, CO (7/20/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426499
--Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517
--Healthcare Cybersecurity Forum – Northeast – Boston, MA (9/22/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/427126
--Healthcare Cybersecurity Forum – Texas – Houston, TX (10/8/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840
--Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886
--Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)
https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/

January 29th, 2020

Sundries –

--Inside the World's Highest-Stakes Industrial Hacking Contest: Hackers had no trouble dismantling systems that help run everything from car washes to nuclear plants.
https://www.wired.com/story/pwn2own-industrial-hacking-contest/
--Does Your Domain Have a Registry Lock?
https://krebsonsecurity.com/2020/01/does-your-domain-have-a-registry-lock/
--How Iran's Military Outsources Its Cyber Threat Forces
https://www.nextgov.com/ideas/2020/01/how-irans-military-outsources-its-cyber-threat-forces/162597/
--Secret Service to launch private-sector cybercrime council
https://www.cyberscoop.com/secret-service-private-sector-cybercrime-advisers/

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

---

[1] https://www.wired.com/story/android-zero-day-more-than-ios-zerodium/
[2] https://www.cyberscoop.com/ics-zero-day-exploit-idaho-lab-s4/
[3] https://www.darkreading.com/threat-intelligence/ryuk-ransomware-hit-multiple-oil-and-gas-facilities-ics-security-expert-says-/d/d-id/1336865
[4] https://documents.trendmicro.com/assets/white_papers/wp-caught-in-the-act-running-a-realistic-factory-honeypot-to-capture-real-threats.pdf
[5] https://pages.eiu.com/rs/753-RIQ-438/images/Ana%20Nicholls%20-%20healthcare%20life%20sciences%20V6.pdf?mkt_tok=eyJpIjoiWlRjeFpEa3lOekZtTVRrMSIsInQiOiJsdVNNYjRRTDVuXC9DOEx2b0t0Z0F2dWN4eEtuUkx1bzRZUFdzMzhPb21VRzQ3cDA3ek41SjMrWlJ5YlI2VmNhUmRmbmxMZWtLa1RpZ0k4RU9BbjI0ODhRQUgrYk5OWjdnZnVSUEtnbVBwYkRlUWVxSHJmZWNTdTBpSHE4clBmdG4ifQ%3D%3D
[6] https://pages.eiu.com/rs/753-RIQ-438/images/Ana%20Nicholls%20-%20healthcare%20life%20sciences%20V6.pdf?mkt_tok=eyJpIjoiWlRjeFpEa3lOekZtTVRrMSIsInQiOiJsdVNNYjRRTDVuXC9DOEx2b0t0Z0F2dWN4eEtuUkx1bzRZUFdzMzhPb21VRzQ3cDA3ek41SjMrWlJ5YlI2VmNhUmRmbmxMZWtLa1RpZ0k4RU9BbjI0ODhRQUgrYk5OWjdnZnVSUEtnbVBwYkRlUWVxSHJmZWNTdTBpSHE4clBmdG4ifQ%3D%3D
[7] https://pages.eiu.com/rs/753-RIQ-438/images/Ana%20Nicholls%20-%20healthcare%20life%20sciences%20V6.pdf?mkt_tok=eyJpIjoiWlRjeFpEa3lOekZtTVRrMSIsInQiOiJsdVNNYjRRTDVuXC9DOEx2b0t0Z0F2dWN4eEtuUkx1bzRZUFdzMzhPb21VRzQ3cDA3ek41SjMrWlJ5YlI2VmNhUmRmbmxMZWtLa1RpZ0k4RU9BbjI0ODhRQUgrYk5OWjdnZnVSUEtnbVBwYkRlUWVxSHJmZWNTdTBpSHE4clBmdG4ifQ%3D%3D