June 30th, 2021

TLP White

This week, *Hacking Healthcare* begins by breaking down how a new technology council created by US and EU representatives may ease the risk of divergent technology standards and help to ameliorate current disagreements over data privacy and security. Next, we examine a report that breaks down the growing threat of USB-related malware in industrial environments and explain why the threat may not be going away even as organizations return to pre-pandemic operations. Finally, we assess how the private sector's struggle with patching is increasingly leading to calls for new laws that mandate it and why that would be a troublesome solution.

Welcome back to *Hacking Healthcare*.

1. **EU and US look to Technology Standards Coordination**

   Divergent international standards between countries or regional blocs can create significant headaches for organizations operating in multiple markets. As lawmakers and regulators in different markets point to competing standards, private sector organizations must make extra efforts to comply with what are often similar requirements. In an effort to combat these inefficiencies and bolster shared values, the EU and US have created a council to help align their approaches to technology issues.

   The newly formed *European Union-United States Trade and Technology Council (TTC)*, is a product of the US-EU summit that occurred last week. The summit, which was billed as "an opportunity to rebuild and strengthen U.S.-EU ties and set a joint transatlantic agenda for the post-pandemic era," touched on a variety of issue areas that included cybersecurity, technology standards, digital services, and transatlantic data transfers.[1]

   The TTC will be "co-chaired on the U.S. side by Secretary Raimondo, Secretary Blinken and Ambassador Tai," and in the Department of Commerce's words, the TTC "presents a historic opportunity to deepen integration between our two economies, especially in technology-enabled sectors, through the better alignment of standards and tech policies, supporting transatlantic supply chains, and promoting the use of digital technologies by small and medium-sized enterprises."[2]

   More specifically, there appears to be a priority interest in figuring out how to regulate and set standards for emerging technologies. In particular, artificial intelligence

governance may be among the first issues to be tackled by the TTC. Commerce Secretary Raimondo is quoted as saying that the US and EU should take the lead in promoting standards and guidance that embodies US-EU shared values such as "anti-discrimination, against bias, equity, and transparency."[3]

Action & Analysis
Included with H-ISAC Membership

2. New Threat Report Highlights USB-Malware Risk

As ransomware continues to dominate news headlines, other forms of malware have continued to proliferate and evolve under the radar and risk being overlooked. One such threat that was recently highlighted by Honeywell International is USB-based malware in industrial environments.

In their freely available 11-page research report entitled *Industrial Cybersecurity: USB Threat Report 2021*, Honeywell examined data from across numerus industries in over 60 countries globally. Their key findings suggest:[4]

- A 30% increase in the use of USB media in production facilities in 2020 over 2019;
- A significant rise in "threats capable of propagating over USB, or specifically exploiting USB media for initial infection," from 19% in 2019 to just over 37% in 2020;
- That Trojans are the most prominent malware type at 76%:
- A significant jump in the number of wormable threats, increasing from just over 1/3 in 2019 to just over 1/2 in 2020;
- That 79% of noted threats were capable of disrupting Operational Technology (OT);
- Malware capable of disrupting Industrial Control Systems (ICS) increased from 59% to 79% from 2019 to 2020; and
- Just over half of these USB-malware threats "were designed to establish a permanent backdoor or remote access, and were capable of downloading and installing additional payloads, and providing command and control functions."

Honeywell's report goes on to assess the security implications of these findings. In their estimation, they believe organizations must establish security policies around removable media, regularly re-evaluate security controls against new and evolving malware, adopt more scrutiny on the introduction of digital content, ensure tight network control, implement a layered threat detection approach, and harden OT systems.[5] In closing, they advocate further for strong USB security controls.

Action & Analysis
Included with H-ISAC Membership

3. **NSA Official Suggests Laws May be Needed to Force Organizations to Patch**

   It is no secret that a significant portion of successful cyberattacks make use of known vulnerabilities that victims have not patched. Although there are many credible reasons for why organizations may not always immediately patch, there are those in the Biden administration that believe that, more often than not, organizations are not adequately prioritizing patches and that legislation may be required to force the issue.

   In a pre-taped session for the Defense One Tech Summit, Rob Joyce, who heads up the National Security Agency's (NSA) Cybersecurity Directorate, is reported as stating that older computers and software that is not kept updated is a serious problem that likely requires laws and regulations over time to ultimately fix.[6] Joyce referenced other industries, such as the automobile industry, as a point of comparison for how cybersecurity could benefit from the introduction of new bare minimum standards that could include requiring organizations to patch.[7]

   While Joyce did not elaborate on specific details, he did note that emerging technologies such as AI are going to make it easier for malicious actors to quickly identify and target specific vulnerabilities that have gone unpatched.[8]

   Action & Analysis
   Included with H-ISAC Membership

Congress –

Tuesday, June 29th:
- No relevant hearings

Wednesday, June 30th:
- House of Representatives – Committee on Energy and Commerce: "A Safe Wireless Future: Securing our Networks and Supply Chains"

Thursday, July 1st:
- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

- No relevant meetings

Conferences, Webinars, and Summits –

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

June 30th, 2021

[1] https://www.commerce.gov/news/blog/2021/06/us-secretary-commerce-gina-m-raimondo-joins-president-biden-us-eu-summit-and
[2] https://www.commerce.gov/news/blog/2021/06/us-secretary-commerce-gina-m-raimondo-joins-president-biden-us-eu-summit-and
[3] https://www.nextgov.com/policy/2021/06/us-eu-create-council-consider-and-coordinate-tech-standards/174947/
[4] https://www.honeywell.com/us/en/honeywell-forge/cybersecurity/cybersecurity-threat-report-2021
[5] https://www.honeywell.com/us/en/honeywell-forge/cybersecurity/cybersecurity-threat-report-2021
[6] https://www.nextgov.com/cybersecurity/2021/06/new-laws-are-probably-needed-force-us-firms-patch-known-cyber-vulnerabilities-nsa-official-says/174989/
[7] https://www.nextgov.com/cybersecurity/2021/06/new-laws-are-probably-needed-force-us-firms-patch-known-cyber-vulnerabilities-nsa-official-says/174989/
[8] https://www.nextgov.com/cybersecurity/2021/06/new-laws-are-probably-needed-force-us-firms-patch-known-cyber-vulnerabilities-nsa-official-says/174989/