August 3rd, 2021

TLP White

This week, *Hacking Healthcare* begins by breaking down various aspects of the White House's new national security memo, including why some of the "voluntary" elements of the memo may not actually end up being so voluntary. Next, we make sense of President Biden's recent remarks that the most likely cause of a "shooting war" between the United States and a rival power would be a significant cyber incident. Finally, we examine why you should take an interest in a multi-government joint advisory that highlights the most common vulnerabilities being exploited, and we discuss what you can do about it.

Welcome back to *Hacking Healthcare*.

1. **White House Memo on Improving Cybersecurity for Critical Infrastructure Control Systems**

   On July 28th the White House released a National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. The memo reiterates the importance of securing critical infrastructure from cyber threats and cites how "[t]he degradation, destruction, or malfunction of systems that control this infrastructure could cause significant harm to the national and economic security of the United States." In particular, the memo announces the launch of an "Industrial Control Systems Cybersecurity Initiative," which may lead to future significant impacts on critical infrastructure sectors like healthcare.[1]

   Section two of the memo states that the Industrial Control Systems Cybersecurity Initiative will be a voluntary effort between the public and private sectors to improve industrial control systems (ICS) cybersecurity by "encouraging and facilitating deployment of technologies and systems that provide threat visibility, indications, detection, and warnings, and that facilitate response capabilities for cybersecurity in essential control system and operational technology networks."[2]

   Additionally, the memo stresses that this initiative should be viewed as building upon previous and ongoing efforts to secure critical infrastructure. There appears to be a particular concern with visibility in section three, which states that industry and

government "cannot address threats we cannot see; therefore, deploying systems and technologies that can monitor control systems to detect malicious activity and facilitate response actions to cyber threats is central to ensuring the safe operations of these critical systems."[3]

Finally, while acknowledging that each sector's cybersecurity needs vary, the memo highlights the need for "baseline cybersecurity goals that are consistent across all critical infrastructure sectors, as well as a need for security controls for select critical infrastructure that is dependent on control systems."[4]

Actions to be taken include:[5]

- A pilot effort within the electricity subsector that will expand to other sectors later in the year, including the chemical sector.
- Sector Risk Management Agencies and others will work with "critical infrastructure stakeholders and owners and operators to implement the principles and policy outlined in [the] memorandum"
- The development and issuance of cybersecurity performance goals for critical infrastructure to further a common understanding of the baseline security practices that critical infrastructure owners and operators should follow to protect national and economic security, as well as public health and safety
- The issuance of preliminary goals for control systems across critical infrastructure sectors no later than September 22, 2021
- The issuance of final cross-sector control system goals within 1 year
- The Issuance of sector-specific critical infrastructure cybersecurity performance goals within 1 year

Action & Analysis
Membership required

2. President Biden Warns that Cyberattacks Could Lead to an actual "Shooting War"

In a speech at the US National Counterterrorism Center last week, President Biden addressed the seriousness of malicious cyber activities aimed at the United States and the possibility of particularly egregious cyber actions leading to actual war.[6]

Speaking to members of the intelligence community, Biden emphasized the diversity and sophistication of challenges the country's intelligence community is set to face in the coming years and noted the increasing capability of cyber threats to cause real world damage and disruption. Going further, he stated: "well, if we end up in a war, a real shooting war with a major power, it's going to [likely] be as a consequence of a cyber breach of great consequence."[7] While not directly mentioning any one country as

the target of that remark, his immediate follow-up outlined how the global environment and the personal motivations of Russian President Putin and Chinese President Xi made both Russia and China dangerous competitors to the United States.

Biden continued by underlining the threat of mis/disinformation and the importance of keeping up with other nations in emerging science and technology fields. These comments come at a time of particularly heightened tensions with Russia over numerous high-profile hacks which have caused Biden to forcefully state that the United States would take matters into its own hands if Russia is unwilling to alter their strategy. That warning may be put to test as recent reports suggest that hacking infrastructure tied to the Russian government has remained active.[8]

Action & Analysis
Membership required

3. Joint Advisory Calls Attention to Common Vulnerabilities

In an attempt to help mitigate the success of malicious cyber actors, a joint cybersecurity advisory was released from U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Australian Cyber Security Centre (ACSC), the United Kingdom's National Cyber Security Centre (NCSC), and the U.S. Federal Bureau of Investigation (FBI) detailing the "top 30 vulnerabilities routinely exploited by malicious cyber actors in 2020 and those being widely exploited thus far in 2021."[9]

Published last Thursday, the 18-page joint advisory helpfully collects a description of each of the vulnerabilities alongside technical details, mitigations, and indicators of compromise, and it provides references for organizations to assess.

In its key findings, the advisory notes how "a majority of the top vulnerabilities targeted in 2020 were disclosed during the past two years," something they attribute to the rapid expansion of remote work, the use of virtual private networks (VPNs), and cloud-based environments.[10] Additionally, the advisory estimates that these vulnerabilities will continue to remain in heavy usage as long as "they remain effective and systems remain unpatched," which will continue to complicate attribution, reduce costs on perpetrators, and minimize malicious actors' own risk.[11] The advisory ends with a call for all organizations to remediate or mitigate these vulnerabilities as quickly as possible.

Action & Analysis
Membership required

Congress –

August 3rd, 2021

Tuesday, August 3rd:
- No relevant hearings

Wednesday, August 4th:
- Senate – Committee on Homeland Security and Governmental Affairs: Business meeting to consider S.2559, to establish the National Deepfake and Digital Provenance Task Force, S.2305, to enhance cybersecurity education, S.2439, to amend the Homeland Security Act of 2002 to provide for the responsibility of the Cybersecurity and Infrastructure Security Agency to maintain capabilities to identify threats to industrial control systems, S.2525, to amend the Homeland Security Act of 2002 to require research and development to identify and evaluate the extent to which critical domain risks within the United States supply chain pose a substantial threat to homeland security

Thursday, August 5th:
- 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.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/
[2] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/
[3] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/
[4] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/
[5] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/
[6] https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/27/remarks-by-president-biden-at-the-office-of-the-director-of-national-intelligence/

[7] https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/27/remarks-by-president-biden-at-the-office-of-the-director-of-national-intelligence/
[8] https://www.riskiq.com/blog/external-threat-management/apt29-bear-tracks/
[9] https://us-cert.cisa.gov/sites/default/files/publications/AA21-209A_Joint%20CSA_Top%20Routinely%20Exploited%20Vulnerabilities.pdf
[10] https://us-cert.cisa.gov/sites/default/files/publications/AA21-209A_Joint%20CSA_Top%20Routinely%20Exploited%20Vulnerabilities.pdf
[11] https://us-cert.cisa.gov/sites/default/files/publications/AA21-209A_Joint%20CSA_Top%20Routinely%20Exploited%20Vulnerabilities.pdf