July 13th, 2021

TLP White

This week, *Hacking Healthcare* begins by examining how the Biden administration is approaching the Russian government in an effort to crack down on recent egregious cybercriminal activity. Next, we breakdown Japan's move to counter the threat of sophisticated cyberattacks by boosting its cyber personnel and introducing new regulations on critical infrastructure sectors. Finally, we briefly touch on how unrelated cybercriminals are using the Kaseya compromise to leverage their spam malware campaign and outline why it's imperative that organizations maintain their security posture even in the face of major incidents. Welcome back to *Hacking Healthcare*.

1. **Cyberattacks Escalate United States-Russian Tensions**

   In the aftermath of the ransomware attack that victimized the software company Kaseya and affected an estimated 1,500 other organizations, the White House has verbalized the unacceptability of these cybercriminal attacks in an increasingly stern tone to the Russian government.[1] While high level talks and other forms of signaling have been ongoing, pressure is growing on the Biden administration to forcefully respond with concrete actions rather than just words.

   In a press briefing on July 6th, White House Press Secretary Jen Psaki was pressed on whether recent talks between President Biden and President Putin had left her "under the impression that Putin would do more to prevent these kind of attacks."[2] Psaki stated that high-level expert-level talks were ongoing on the issue and that Biden has made clear to President Putin that "if the Russian government cannot or will not take action against criminal actors residing in Russia, we will take action or reserve the right to take action on our own."[3]

   However, some of the decisiveness of that statement was tempered by her follow-ups. First, she cautioned that the intelligence community had not yet attributed the attack, despite acknowledging REvil's presence in Russia.[4] Secondly, she would not detail any specifics on whether confirmation that the attack was carried out from Russia would result in the US taking action against the Russian state.[5]

   Similar statements were made just three days later, on July 9th, as Biden held a phone conversation with Putin in which some of those equivocations were replaced by an

adamant warning that the US was prepared to act. The discussion has been reported as possibly the Russian government's "final chance to take action on Russia's harboring of cybercriminals before the United States moved to dismantle the threat."[6]

Biden warned that "attacks would no longer be treated only as criminal acts, but as national security threats," signaling the seriousness of future transgressions and opening the door to more drastic response options.[7] Elaborating on potential actions, Biden acknowledged his openness to knocking out the servers and infrastructure associated with the cybercriminal attacks. The next few weeks will likely put such warnings to the test as it is likely only a matter of time before another significant incident occurs.

Action & Analysis
Included with H-ISAC Membership

2. Japan To Boost Cyber Forces, Restrict Foreign Technology, and Introduce New Regulations

In an effort to counter growing cyber risks, and to specifically counter Colonial Pipeline-like incidents with national security implications, the Japanese government is in the process of boosting its cybersecurity defense personnel while also introducing new regulations that should improve cybersecurity in critical infrastructure areas. These will hopefully help address the shortcomings that led to the internationally recognized think tank *International Institute for Strategic Studies* (IISS) to give them a low rating for cyber capability in their recent assessment of 15 of the most advanced cyber capable states.[8]

The expansion of their cyber defense personnel is substantial and is reported as partially a response to a cyberattack that impacted government agencies earlier this year as well as recognition that cyber threats from other nation-states are proliferating.[9] Noting the need to "deal with increasingly sophisticated attacks by China, Russia, and others," Japan's Ministry of Defense is planning to more than double its current cyber defense personnel from around 660 to about 1500 by March of 2022 while also restructuring their organization.[10][11]

Among the more significant changes will be new regulations for 14 critical infrastructure sectors, including healthcare, that will reportedly "require operators of such key infrastructure to address national security concerns when procuring foreign-made equipment."[12] Changes to various laws that govern each sector will apparently be amended in a single motion that will add a clause "requiring each sector to be conscious of national security risks."[13]

These changes appear to be centered on security concerns over the use of "foreign equipment or services, including cloud data storage, as well as connections to servers located overseas," and the government will allegedly "monitor companies for compliance and will suspend or cancel their license should any major issues arise."[14] More concrete details are not yet available.

Action & Analysis
Included with H-ISAC Membership

3. **Don't Lower your Guard in Rushing to Find A Fix**

   On July 2nd, the software company Kaseya reported that it had been victimized by a cyberattack that has turned into a supply chain nightmare affecting upwards of roughly 1500 organizations.[15] Those affected or potentially affected rushed to employ mitigations and patches as news of widespread ransomware attacks stemming from the compromise began to make headlines. Never missing an opportunity to take advantage of a crises, unrelated cyber threat actors went to work leveraging the attack for their own gain.

   Anticipating that fears of victimization may lead organizations to lower their guard, some cyber threat actors began pushing out malware in spam messages claiming to be security updates to address the Kaseya software vulnerability.[16] Instead of helping, the link and attachment provided in the messaging deploys Cobalt Strike, a pen testing tool with dual-use functionality, on anyone unfortunate enough to have clicked on it.[17]

   Action & Analysis
   Included with H-ISAC Membership

Congress –

Tuesday, July 13th:
- No relevant hearings

Wednesday, July 14th:
- No relevant hearings

Thursday, July 15th:
- Senate – Committee on Commerce, Science, and Transportation: Hearings to examine implementing supply chain resiliency.

International Hearings/Meetings –

- No relevant meetings

EU –

- No relevant meetings

Conferences, Webinars, and Summits –

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

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

[1] https://www.zdnet.com/article/ransomware-us-warns-russia-to-take-action-after-latest-attacks/
[2] https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/06/press-briefing-by-press-secretary-jen-psaki-july-6-2021/
[3] https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/06/press-briefing-by-press-secretary-jen-psaki-july-6-2021/

[4] https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/06/press-briefing-by-press-secretary-jen-psaki-july-6-2021/
[5] https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/06/press-briefing-by-press-secretary-jen-psaki-july-6-2021/
[6] https://www.nytimes.com/2021/07/09/us/politics/biden-putin-ransomware-russia.html
[7] https://www.nytimes.com/2021/07/09/us/politics/biden-putin-ransomware-russia.html
[8] https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-three
[9] https://www.zdnet.com/article/japan-to-bolster-national-cybersecurity-defence-with-800-new-hires-report/
[10] https://asia.nikkei.com/Business/Technology/Japan-to-bulk-up-cybersecurity-units-for-nation-s-defense
[11] https://www.zdnet.com/article/japan-to-bolster-national-cybersecurity-defence-with-800-new-hires-report/
[12] https://asia.nikkei.com/Business/Technology/Japan-to-restrict-use-of-foreign-tech-in-telecom-power-grids
[13] https://asia.nikkei.com/Business/Technology/Japan-to-restrict-use-of-foreign-tech-in-telecom-power-grids
[14] https://asia.nikkei.com/Business/Technology/Japan-to-restrict-use-of-foreign-tech-in-telecom-power-grids
[15] https://www.zdnet.com/article/kaseya-ransomware-attack-what-we-know-now/
[16] https://twitter.com/MBThreatIntel/status/1412518446013812737
[17] https://www.bleepingcomputer.com/news/security/fake-kaseya-vsa-security-update-backdoors-networks-with-cobalt-strike/