April 20th, 2021

TLP White

This week, *Hacking Healthcare* begins by exploring the possible cybersecurity-related ramifications of worsening relations between the United States, Russia, and China. Then, we briefly examine the increase in cloud cyberattacks and advocate for assessing security controls. Finally, we spotlight a new set of domain name service (DNS) vulnerabilities that potentially impacts millions of internet-connected devices, including those in the healthcare sector, and look towards mitigation strategies. Welcome back to *Hacking Healthcare*.

1. **The United States Takes Actions Against China and Russia**

   Earlier this month, the United States Commerce Department added seven Chinese technology firms to its "Entity List" for "conducting activities that are contrary to the national security or foreign policy interests of the United States."[1] The Commerce Department accused each of assisting in the "development of supercomputers used by China's military actors, its destabilizing military modernization efforts, and/or weapons of mass destruction (WMD) programs."[2] The move to place these companies on the Entity List is likely to inflame tensions between the United States and China, especially as this action may be viewed by China as an expansion of United States economic policies used to limit Huawei, ZTE, and others during the Trump administration.

   Being added to the Entity List effectively means that a company is banned from buying parts and components from US companies without government approval. However, there are various options possible to make such a ban more or less restrictive, and the most recent Entity List designation for the seven new Chinese companies does not go quite as far as when Huawei was added to the list. In that instance, the Trump administration invoked the *foreign direct product rule*, "which would ban any foreign company that uses US technology" from supplying the listed companies.[3]

   As for Russia, on April 15th, the White House released a statement and Executive Order that called out Russia for "harmful foreign activities."[4] The Executive Order included numerous official actions against Russia, such as sanctions against individuals and entities tied to the Russian Federation's malicious cyber activities, unspecified actions in relation to reported bounties against United States military personnel, the expulsion of diplomatic personnel, and the naming and shaming of Russian groups in connection to the SolarWinds attack. These actions represent a comprehensive public censure of

Russian activities over the past few years and signal that the Biden administration appears ready to strongly confront that country.

And you don't have to look far to see some of what has been going on, like the continued active exploitation of vulnerabilities by Russian intelligence services, including the Pulse VPN vulnerability for which the H-ISAC has recently published an alert.[5,6]

Action & Analysis
Included with H-ISAC Membership

2. **Cloud Cyber Attacks Increase as Companies Pivot During the Pandemic**

In March 2020, when offices closed and shelter in place orders went into effect, citizens relied on delivery services, virtual services, and e-commerce like never before in history. During this time, many sectors turned to using cloud platforms to continue business operations, as some of their workforces began to work remotely. This shift was reflected in cloud spending estimates, which reportedly increased by 28% in the second quarter of 2020.[7] Unfortunately, this increased investment has incentivized malicious actors to increase efforts to target the cloud as an attack vector. Palo Alto Networks' *Cloud Threat Report* shows that companies critical to providing services in the COVID-19 era are struggling to manage cloud security by cataloging an increase in reported cloud security incidents.[8]

According to the *Cloud Threat Report*, the retail, manufacturing, and government sectors have seen the sharpest increase in attacks. However, chemical manufacturing and research organizations have also become increasingly targeted by malicious actors. This is particularly true for companies involved in vaccine development.

The four most prevalent types of attacks facing these critical industries are SQL database encryption disablement, malicious port scans, disabling database version encryption, and firewall rules allowing all traffic. These types of attacks have all seen an increase of over 120% in the past year. These cloud network attacks could have serious ramifications for businesses, including data leaks of sensitive information or personal client information and the slowing down of critical business operations.

Action & Analysis
Included with H-ISAC Membership

3. **Domain Name System (DNS) Vulnerability Discovered on Commonly Used Operating Systems**

Given that nearly all internet-connected devices require DNS to function in some fashion, any new threat to that system warrants attention.

Newly discovered DNS vulnerabilities allegedly make internet connected devices vulnerable to remote code execution and denial-of-service attacks. Forescout Research

Lab found nine such vulnerabilities in the Transmission Control Protocol/International Protocol (TCP/IP) stack.

Daniel dos Santos, a research manager at Forescout Research Lab, said, "any software that processes DNS packets may be affected, such as firewalls, intrusion detection systems, and other network appliances," highlighting how widespread these vulnerabilities could be.[9] The report released by Forescout explains how the vulnerabilities can allow bad actors to take devices offline, download malware onto them, or steal data.

Out of the vulnerabilities identified in the report, two of the specific operating systems that could be targeted are used in medical systems and medical devices. Nucleus RTOS, which can be used in medical and airborne systems, and ThreadX, an operating system found in many medical devices, are both potentially vulnerable to the vulnerabilities.

The two operating systems mentioned, Nucleus RTOS and ThreadX, have both had patches issued for these vulnerabilities. Affected organizations should assess an optimal approach to patching, however. Since these vulnerabilities are now public, organizations might want to consider taking a more proactive approach.[10]

Action & Analysis
Included with H-ISAC Membership

Congress –

Tuesday, April 20th:
- Senate – Committee on Health, Education, Labor, and Pensions: Hearings to examine COVID-19 recovery, focusing on supporting workers and modernizing the workforce through quality education, training, and employment opportunities.

Wednesday, April 21st:
- No relevant hearings

Thursday, April 22nd:
- No relevant hearings

International Hearings/Meetings –

- No relevant hearings

EU –

Thursday, April 22nd:
- European Parliament – Committee on the Environment, Public Health and Food Safety

Conferences, Webinars, and Summits –

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

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

April 20th, 2021

[1] https://www.commerce.gov/news/press-releases/2021/04/commerce-adds-seven-chinese-supercomputing-entities-entity-list-their
[2] https://www.commerce.gov/news/press-releases/2021/04/commerce-adds-seven-chinese-supercomputing-entities-entity-list-their
[3] https://arstechnica.com/tech-policy/2021/04/us-adds-chinese-supercomputing-companies-to-export-blacklist/
[4] https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/
5 https://health-isac.cyware.com/webapp/user/myfeeds/0f73a4b5

[6] https://www.bleepingcomputer.com/news/security/nsa-top-5-vulnerabilities-actively-abused-by-russian-govt-hackers/
[7] https://www.zdnet.com/article/industries-critical-to-covid-19-response-suffer-surge-in-cloud-cyberattacks/
[8] https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research
[9] https://www.darkreading.com/vulnerabilities---threats/dns-vulnerabilities-expose-millions-of-internet-connected-devices-to-attack/d/d-id/1340664
[10] https://www.darkreading.com/vulnerabilities---threats/dns-vulnerabilities-expose-millions-of-internet-connected-devices-to-attack/d/d-id/1340664