February 1, 2022

TLP White

This week, *Hacking Healthcare* begins by examining how an interesting development in the ongoing Ukraine crisis that involves Belarusian hacktivists could provide a preview of a new cyber threat to the healthcare sector. We then break down why the Federal Communications Commission (FCC) recently took a decision to revoke a Chinese telecommunications firm's ability to operate in the United States, and what the fallout of the decision may be.

Welcome back to *Hacking Healthcare*.

1. **Belarusian Hacktivist Group Disrupts Critical Infrastructure In Opposition to Government Policy**

   A new development related to the crisis in Ukraine may eventually lead to serious implications for the healthcare sector. Recently, a Belarusian hacktivist group was alleged to have hacked into and disrupted its country's railways in an attempt to hamper the movement of Russian military personnel entering the country and deploying near the Ukrainian border. The operation appears to represent a politically motivated cyberattack carried out by individuals against the critical infrastructure of their own country with the specific objective of influencing government policies.

   <u>What Happened?</u>

   The group, referred to as "Cyberpartisans," appears to have conducted a cyberattack against the country's railways system, claiming that it "encrypted or destroyed internal databases that the Belarusian railways use to control traffic, customs and stations, an action that could cause delays to commercial and non-commercial trains."[1] Additionally, it's been reported that they have not ruled out more serious steps that would include "downing the signaling and emergency control systems" if they were "confident that innocent people won't get injured as a result."[2]

   <u>Who Are the Cyberpartisans?</u>

The Cyberpartisans are not a new or unknown entity. Estimated by some to consist of roughly "25 anonymous IT experts and other activists," the group is highly critical of Belarusian President Alexander Lukashenko and his government.[3] In recent years, the Cyberpartisans have carried out numerous cyber operations against their government, including cyberattacks against the Ministry of Interior Affairs, state companies, and firms.[4] They are alleged to have stolen data related to security officials, spies, and government-related criminality, and they became listed as "extremists" last summer by the Lukashenko government.[5]

What Is Their Motive?

The group claims that this attack is partially in response to their government's admission of Russian military personnel and equipment into Belarus ahead of what is being billed as a military exercise. The Cyberpartisans and others in the international community see the movement as potentially another step in preparation for an invasion of Ukraine. For the Cyberpartisans, the decision to allow Russian troops into the country threatens the sovereignty of Belarus by "[putting Belarus in] danger of occupation," and potentially pulls Belarus into a war with Ukraine and the West.[6]

However, the Cyberpartisans' motives would also appear to extend to foreign and domestic politics in general, as the demand to return service to normal includes the release of 50 political prisoners that are in need of medical assistance. Hundreds of Belarusians have been jailed as political prisoners in recent times for challenging the legitimacy of the Lukashenko regime and its increasing alignment with Russia. An alleged representative of the Cyberpartisans has stated the group's desire is to ultimately "overthrow Lukashenko's regime, keep the sovereignty and build a democratic state with the rule of law, independent institutions and protection of human rights."[7]

Action & Analysis

2. FCC Takes Action Against Chinese Telco

Sticking with geopolitics, a recent FCC action to revoked *China Unicom (Americas) Operations Limited* authority *to* "[provide] domestic interstate and international telecommunications services within the United States" is likely to further strain already tense relations between the two countries.[8] The revocation was published on January 27th under the justification that the "action safeguards the nation's telecommunications infrastructure from potential security threats," and it directs China Unicom Americas to discontinue affected services within 60 days.[9]

The FCC's news release outlined its rationale:[10]

- China Unicom Americas is a subsidiary of a Chinese state-owned enterprise, making it "subject to exploitation, influence, and control by the Chinese government."
- U.S.-China relations are strained, creating a "changed national security environment" that may create "significant national security and law enforcement risks." Specifically, those risks include providing opportunities for the "Chinese government to access, store, disrupt, and/or misroute U.S. communications, which in turn allow them to engage in espionage and other harmful activities against the United States."
- China Unicom Americas' "conduct and representations to the Commission and Congress demonstrate a lack of candor, trustworthiness, and reliability."
- Attempts to mitigate the underlying issues "would not address these significant national security and law enforcement concerns."

The action was taken with unanimous approval from the chairwoman and three confirmed FCC commissioners, and it means that two of China's state-owned telecommunications enterprises have been banned from operating in the United States.

Action & Analysis

Congress

Tuesday, February 1
Senate – Committee on Commerce, Science, and Transportation - Subcommittee on Consumer Protection, Product Safety, and Data Security: Hearings to examine COVID-19 fraud and price gouging.

Wednesday, February 2nd:
- No relevant hearings

Thursday, February 3rd:
- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

February 1, 2022

Wednesday, February 9th:
- HSE cyber-attack: a wake-up call for healthcare right across Europe | How European-funded research can boost your cyber resilience in 2022

Conferences, Webinars, and Summits

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

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

About the Author

Hacking Healthcare is written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, and as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

---

[1] https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup

[2] https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup

[3] https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup

[4] https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup

[5] https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup

---

[6] https://www.atlanticcouncil.org/blogs/belarusalert/cyber-partisans-target-russian-army-in-belarus-amid-ukraine-war-fears/

[7] https://arstechnica.com/information-technology/2022/01/hactivists-say-they-hacked-belarus-rail-system-to-stop-russian-military-buildup/

[8] https://www.fcc.gov/document/fcc-revokes-china-unicom-americas-telecom-services-authority

[9] https://www.fcc.gov/document/fcc-revokes-china-unicom-americas-telecom-services-authority

[10] https://www.fcc.gov/document/fcc-revokes-china-unicom-americas-telecom-services-authority