March 22, 2022

TLP White

This week, *Hacking Healthcare* begins by examining how the Russian invasion of Ukraine and the wave of follow-on sanctions may be further complicating organizations' deliberations on making a ransomware payment. Then we assess what to make of the sudden White House statement on private sector cybersecurity and potential Russian cyber operations. Welcome back to *Hacking Healthcare*.

1. **Russian Aggression Further Complicates Ransomware Payment Debate**

   While many countries do not outright ban the payment of ransom demands to cybercriminal groups, some countries have introduced restrictions on payment to specified actors where it's deemed to be in the national interest. This approach has been upended by the conflict in Ukraine, where Russian aggression has resulted in that country's becoming the most sanctioned on Earth, with over 5,500 separate restrictions placed on it.[1] Combined with the already murky relationship between cybercrime groups and the Russian government's security and intelligence services, these new sanctions, and the regulatory focus that accompanies them, may create additional risk for healthcare organizations that make ransomware payments to unknown actors.

   Within the United States, the Department of the Treasury has taken the lead on ransomware and sanctions-related activities. Back in October 2020, the United States' Office of Foreign Assets Control (OFAC) released guidance reminding organizations within its jurisdiction of how ransomware payments to specified actors on its sanctions lists, in particular the Specially Designated Persons (SDF) list, could land them in regulatory trouble.[2] An update to that document in September 2021 reiterated that those organizations subject to OFAC jurisdiction "may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC."[3]

   Since the start of the Russian invasion of Ukraine, numerous Russian individuals and institutions have been added to sanctions lists. Within the United States, the Financial Crimes Enforcement Network (FINCEN), a bureau within the Department of the Treasury whose mission is in part to "safeguard the financial system from illicit use," even issued an alert in early March warning financial institutions to be vigilant in identifying efforts

by Russian entities to evade the expansive sanctions.[4] This action is likely to make financial institutions even more wary of taking part in deals and transactions that could tie back to Russia. All of these actions make paying a ransom demand to an unknown, potential Russian entity fraught with risk.

This could become a serious issue since the Russian economy is projected by some analysts to decline by as much as 7 percent due to Western-led sanctions. Some individuals believe the Russian government and Russian cybercriminal groups could resort to ransomware attacks in response.[5, 6] With the conflict on the ground likely to be some way from resolution, and with some Western leaders hinting that a return to normalcy with a Putin-led Russia would be a mistake, this may be an issue facing the healthcare sector for some time.[7]

Action & Analysis
Included with H-ISAC Membership

2. Biden Cybersecurity Warning

On Monday, March 21st, the Biden administration released a short, four-paragraph statement imploring the private sector to harden cyber defenses immediately and warned of new intelligence that "the Russian Government is exploring options for potential cyberattacks."[8] The statement appears to be the most significant public indication from the Biden administration that Russia may ramp up cyber operations against the U.S. private sector.

The statement touched on warnings of possible impending Russian cyber operations, listed the actions taken by the current administration to improve the nation's cybersecurity, and promised to use "every tool to deter, disrupt, and if necessary, respond to cyberattacks against critical infrastructure."[9] However, the most consequential aspect might be the administration's imploring the private sector to do its part in implementing cybersecurity best practices.

To that end, the White House released a fact sheet that contained more detailed information on what the administration wanted to see from the private sector.[10] The fact sheet contained eight steps that should be executed with urgency and five more to be adopted over time.

In the immediate term, the administration urged the private sector to:[11]

- Mandate the use of multifactor authentication on your systems to make it harder for attackers to get onto your system
- Deploy modern security tools on your computers and devices to continuously look for and mitigate threats
- Check with your cybersecurity professionals to make sure that your systems are patched and protected against all known vulnerabilities, and change passwords

across your networks so that previously stolen credentials are useless to malicious actors

- Back up your data and ensure you have offline backups beyond the reach of malicious actors
- Run exercises and drill your emergency plans so that you are prepared to respond quickly to minimize the impact of any attack
- Encrypt your data so it cannot be used if it is stolen
- Educate your employees to common tactics that attackers will use over email or through websites, and encourage them to report if their computers or phones have shown unusual behavior, such as unusual crashes or operating very slowly
- Engage proactively with your local FBI field office or CISA Regional Office to establish relationships in advance of any cyber incidents. Please encourage your IT and security leaders to visit the websites of the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI, where they will find technical information and other useful resources

The long-term goals focused more on adopting secure-by-design principles and supply chain security.[12]

Some additional details can be found at:

https://h-isac.org/health-isac-and-hc3-joint-bulletin-potential-malicious-cyber-attacks-from-russia/

Action & Analysis
Included with H-ISAC Membership

Congress

Tuesday, March 22nd:

- No relevant hearings

Wednesday, March 23rd:

- No relevant hearings

Thursday, March 24th:

- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

- No relevant meetings

March 22, 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.axios.com/russia-most-sanctioned-country-0de10d02-51aa-46c4-9711-bb45303fdfb8.html

[2] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

[3] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

[4] https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evasion%20FINAL%20508.pdf

[5] https://www.bankinfosecurity.com/russias-war-further-complicates-cybercrime-ransom-payments-a-18712

[6] https://www.theguardian.com/world/2022/mar/02/russia-economy-could-shrink-by-7-per-cent-as-result-of-ukraine-sanctions-war-recession-covid

[7] https://www.reuters.com/article/us-ukraine-crisis-britain-johnson/uks-johnson-sees-no-return-of-normal-relations-with-putin-idUSKCN2LG0E3

[8] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/

[9] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/

[10] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/

[11] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/

[12] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/