June 15th, 2021

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* is dedicated to aggregating and analyzing the whirlwind of recent ransomware developments in both the public and private sector. In addition to breaking down what has been happening, we cite new guidance and recommendations and provide our thoughts on how these developments have been helpful or unhelpful in addressing the ransomware issue.   Welcome back to *Hacking Healthcare*.

1. Introduction

Ransomware has had no trouble maintaining the spotlight as high-profile incidents have continued to mount over the past few weeks. Government authorities and private sector organizations are scrambling to address the increasingly dire situation, and the speed by which the overall situation is evolving can make it easy to miss critical developments. With this in mind, we have dedicated this edition of *Hacking Healthcare* to examining recent ransomware developments, assessing their impact to the private sector, and highlighting a number of recommendations H-ISAC members may find valuable.

Government Response

We start with the Biden administration. The administration has made cybersecurity a priority issue area and has found no shortage of critical cybersecurity incidents to respond to. Despite the timing coinciding with the Colonial Pipeline ransomware attack, the administration's recent cyber-related executive orders on Russian interference, supply chain challenges, and cybersecurity were tailored primarily as a response to prior incidents like SolarWinds and were less focused squarely on the issue of ransomware. However, in the past few weeks the Biden administration has taken numerous steps towards addressing the unrelenting wave of ransomware.

Department of Justice

The Department of Justice (DOJ) has been especially active in this area.

> *Ransomware Task Force*: As we briefly covered in an earlier edition, an internal DOJ memo was issued in late April that announced the formation of a ransomware task force. The memo recognized that ransomware was not only a growing economic threat, but also a threat to the health and safety of American citizens.[1] It has been reported that this memo will lead to improved intelligence

sharing across DOJ, the creation of a strategy that targets every aspect of the ransomware ecosystem, and a more proactive approach overall.[2]

Ransomware Elevation: The aforementioned strategy and approach was partially unveiled at the beginning of June when it was reported that further internal DOJ guidance was circulated that gave investigations of ransomware attacks a similar priority to terrorism.[3] The move requires ransomware cases and investigations to be centrally coordinated with the ransomware taskforce in Washington, DC in order to ensure that the best possible understanding and operational picture can be created for the various stakeholders involved in ransomware incidents.

Ransom Recovery: When Colonial Pipeline paid the ransom demand in Bitcoin, many assumed the perpetrators and the money were as good as gone. However, an FBI-led operation was able to seize $2.3 million in Bitcoin paid out in the ransom.[4] The FBI allegedly tracked the movement of the ransom funds on a publicly visible Bitcoin ledger and then gained access to the virtual account where most of it ended up.[5]

US CYBERCOM

Outside of DOJ, US Cyber Command (CYBERCOM), whose mission is to “Direct, Synchronize, and Coordinate Cyberspace Planning and Operations - to Defend and Advance National Interests - in Collaboration with Domestic and International Partners,” also has a role to play in responding to ransomware threats.[6]

Hearing: In a virtual hearing last Friday, Gen. Nakasone, dual hatted as both the head of CYBERCOM and the director of the NSA, declined needing new authorities to go after cybercriminal groups.[7] He stated that he thinks he has “all the authorities I need to be able to prosecute intelligence-wise against these adversaries outside the United States.”[8] However, specifically speaking about ransomware, he relayed that the real challenge, and the one that the Biden administration is working through, is how to share and coordinate intelligence and action with various public and private stakeholders while also determining who is taking the lead on overall efforts. [9]

DHS

Guidance - CISA: Rising Ransomware Threat to OT Assets: The elevated importance of ransomware has also led to the publication of additional guidance from the government, including a CISA fact sheet entitled*, Rising Ransomware Threat to Operational Technology Assets*.[10] The three-page document gives an overview of the ransomware threat, specifically to OT assets, and then outlines actions organizations should take to prepare for, mitigate, and respond to ransomware.

Private Sector Developments

There have also been a few notable ransomware developments pertaining to the private sector in recent weeks. Unfortunately, these developments have tended to be more negative rather than positive. High-profile ransomware attacks continue to result in multi-million-dollar ransom payments, and the US Congress has been highly critical of how the private sector has responded to incidents.

IST Ransomware Task Force (RTF): The RTF, a group of ~60 experts from both the public and private sector, released an 81-page report that provides a detailed and thorough framework for combating ransomware.[11] This document should help educate individuals on the nuances of ransomware while also providing practical and actionable policy actions.

Brought together by the Institute for Security and Technology (IST), the RTF includes representation from major technology firms like Microsoft and Amazon; cybersecurity organizations like Rapid7, Palo Alto Networks, the Cybersecurity Coalition, the Cyber Threat Alliance, and the Global Cyber Alliance; and government organizations like the U.K. National Cyber Security Centre (NCSC) and the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

JBS & CNA: JBS, one of the largest meat processors in the United States, recently became one of the next high-profile ransomware incidents after Colonial Pipeline. The attack had wide-spread impacts, as JBS operations in Australia, Canada, and the US were all reportedly affected.[12] Ultimately JBS paid a ransom of roughly $11 million with the intent of ensuring the perpetrators did not steal company data.[13]

However, that payment pales in comparison to the nearly $40 million that the insurance organization CNA Financial Corp. reportedly paid out to "regain control of its network after a ransomware attack."[14] While that attack appears to have occurred in March, details of the ransom payment only became public in late May.

Congress Voices Disapproval: In a congressional hearing last week, lawmakers repeatedly engaged with Colonial Pipeline CEO Joseph Blunt on the way they responded to their ransomware incident. Some Lawmakers asserted that voluntary Transportation Security Administration cybersecurity reviews were refused by Colonial Pipeline, with Rep. Bonnie Watson Coleman (D) stating: "Delaying these assessments for so long amounts to declining them, sir."[15] Others took issue with the pipeline's decision not to immediately reach out to DHS and CISA or accept their assistance in recovery operations.[16] A few congressional members went so far as to question if voluntary cybersecurity standards and a "hands-off" approach to critical infrastructure was still tenable.[17]

Action & Analysis

Included with H-ISAC Membership

June 15th, 2021

Congress –

Tuesday, June 15th:

- No relevant hearings

Wednesday, June 16th:

- Senate – Committee on Homeland Security and Governmental Affairs: Business meeting to consider the nominations of Jen Easterly, to be Director of the Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, and Chris Inglis, to be National Cyber Director.

-House of Representatives – Committee on Homeland Security: Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack

Thursday, June 17th:

- No relevant hearings

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.wsj.com/articles/ransomware-targeted-by-new-justice-department-task-force-11619014158?mg=prod/com-wsj

[2] https://www.wsj.com/articles/ransomware-targeted-by-new-justice-department-task-force-11619014158?mg=prod/com-wsj

[3] https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/

[4] https://www.cnn.com/2021/06/07/politics/colonial-pipeline-ransomware-recovered/index.html

[5] https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981?mg=prod/com-wsj

[6] https://www.cybercom.mil/About/Mission-and-Vision/

[7] https://www.c-span.org/video/?512335-1/nsa-director-nakasone-testifies-2022-defense-intelligence-agenda&live

[8] https://www.c-span.org/video/?512335-1/nsa-director-nakasone-testifies-2022-defense-intelligence-agenda&live

[9] https://www.c-span.org/video/?512335-1/nsa-director-nakasone-testifies-2022-defense-intelligence-agenda&live

[10] https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf

[11] https://securityandtechnology.org/ransomwaretaskforce/

[12] https://www.cyberscoop.com/jbs-ransom-11-million-cybercrime/

[13] https://www.cyberscoop.com/jbs-ransom-11-million-cybercrime/

[14] https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

[15] https://www.cyberscoop.com/house-homeland-colonial-hearing-coordination/

[16] https://www.cyberscoop.com/house-homeland-colonial-hearing-coordination/

[17] https://www.cyberscoop.com/house-homeland-colonial-hearing-coordination/