March 29, 2022

TLP White

This week, *Hacking Healthcare* begins by assessing a report from a U.S. senator on the Homeland Security and Governmental Affairs committee, which alleges that the Federal Bureau of Investigation (FBI) may not always be doing an adequate job of helping ransomware victims who have reached out for assistance. Then, we briefly break down some of the main statistics and predictions from the FBI's new *Internet Crime Report* and make a few recommendations for healthcare organizations.

Welcome back to *Hacking Healthcare*.

1. **Senate Report Casts Doubt over FBI Response to Cyber Incidents**

   On March 24th, U.S. Sen. Rob Portman (R-OH), the Ranking Member of the Senate Homeland Security and Governmental Affairs Committee, published a report detailing the ransomware threat to the United States. Among the executive summary's compelling points was the notion that the federal government did not effectively aid the two victim organizations that needed it.[1] The details will do little to improve the skepticism that many organizations already have when it comes to reporting cyber incidents to law enforcement.

   The 51-page report, titled *America's Data Held Hostage: Case Studies in Ransomware Attacks on American Companies*, provides a brief introduction to the topic of ransomware, evaluates trends, and even assesses the various roles of the private sector in responding to an incident through insurance, legal counsel, and negotiators.[2] However, the most interesting portions of the report are the three case studies of U.S.-based organizations that were victimized by REvil.

   The report notes "that the three companies have little in common in terms of business model, purpose, or number of employees," and that they comprise a large global multi-sector Fortune 500 company, a global manufacturing company, and a small technology firm.[3] According to the report, all three companies reported their cyber incidents to the

federal government, but the two organizations that are alleged to have needed outside assistance received "little help."[4]

The victim companies reported to the committee that "the Federal Bureau of Investigation (FBI) prioritized its investigative efforts into REvil's operations over protecting the companies' data and mitigating damage," and that they "did not receive advice on best practices for responding to a ransomware attack or other useful guidance from the Federal Government."[5]

The report went on to recommend that the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) "strengthen their partnership to assist ransomware victims" in such a way as to allow CISA to provide technical assistance while the FBI investigates.[6] Additionally, the report recommended that the "FBI should ensure it considers ransomware victim priorities like protecting data and mitigating damage," in order to "preserve FBI's constructive working relationship with the private sector."[7]

Action & Analysis
Membership required

2. FBI Releases Internet Crime Report

Sticking with our FBI theme, earlier this month the FBI's Internet Crime Complaint Center (IC3) published its 2021 *Internet Crime Report*. The details largely confirm what many of us already suspected, but there are several items worth assessing in detail. The 33-page report is freely available and contains a significant number of statistical categories that can be compared over previous years.

FBI Deputy Director Paul M. Abbate sets the tone of the paper in his opening introduction, noting that 2021 saw "an unprecedented increase in cyber attacks and malicious cyber activity."[8] Some of the notable statistics and key points are:

- 847,376 reported complaints — up 7% from 2020
- Potential losses exceeding $6.9 billion — up from $4.2 billion in 2020
- Business Email Compromise (BEC) resulted in adjusted losses of roughly $2.4 billion
- IC3's Recovery Asset Team (RAT) was able to freeze approximately $329 million in potential losses
- Phishing/vishing/smishing/pharming are far and away the most reported category of internet crime

- The IC3 report notes that the Healthcare and Public Health sector was the critical infrastructure sector with the most reported ransomware victims (148), well ahead of Financial Services (89) and Information Technology (74)
- IC3 anticipates an increase in critical infrastructure victimization in 2022

Action & Analysis
Membership required

Congress

Tuesday, March 29th:
- House of Representatives - Committee on the Judiciary: Oversight of the Federal Bureau of Investigation, Cyber Division

Wednesday, March 30th:
- House of Representatives - Committee on Energy and Commerce: Hearing: "FDA User Fee Reauthorization: Ensuring Safe and Effective Medical Devices"
- House of Representatives - Committee on Homeland Security: Hearing: “Mobilizing our Cyber Defenses: Securing Critical Infrastructure Against Russian Cyber Threats”

Thursday, March 31st:
- House of Representatives - Committee on Appropriations: FY 2023 Budget Request for the Department of Health and Human Services

International Hearings/Meetings –

- No relevant meetings

EU –

Conferences, Webinars, and Summits

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

March 29, 2022

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.hsgac.senate.gov/imo/media/doc/Americas%20Data%20Held%20Hostage.pdf

[2] https://www.hsgac.senate.gov/imo/media/doc/Americas%20Data%20Held%20Hostage.pdf

[3] https://www.hsgac.senate.gov/imo/media/doc/Americas%20Data%20Held%20Hostage.pdf

[4] https://www.hsgac.senate.gov/imo/media/doc/Americas%20Data%20Held%20Hostage.pdf

[5] https://www.hsgac.senate.gov/imo/media/doc/Americas%20Data%20Held%20Hostage.pdf

[6] https://www.hsgac.senate.gov/imo/media/doc/Americas%20Data%20Held%20Hostage.pdf

[7] https://www.hsgac.senate.gov/imo/media/doc/Americas%20Data%20Held%20Hostage.pdf

[8] https://www.aarp.org/content/dam/aarp/money/scams_fraud/2022/03/2021-ic3-annual-report.pdf