March 9, 2022

TLP White

This week, *Hacking Healthcare* begins with an update on the cyber incident reporting bill that was passed by the United States Senate. We examine what the bill requires and what comes next as it looks to become law. Additionally, we explain why implementation may still be some ways off even if it is signed quickly. Next, we examine some of the interesting details to emerge from the Conti ransomware group leaks. We assess what the leaks tell us about the group's willingness to attack healthcare organizations, how it operates, and why leaks like this could pose a legal or regulatory risk to organizations.

Welcome back to *Hacking Healthcare*.

1. **Cyber Incident Reporting Bill Approved by U.S. Senate**

   After failing in a bid to tack on cyber incident reporting to the most recent National Defense Authorization Act (NDAA) in December, a bipartisan group of senators has been keen on pushing the issue forward at the start of the new year's legislative cycle. Their efforts were rewarded last week.

   On March 1st, the Senate passed S. 3600, the *Strengthening American Cybersecurity Act of 2022* by unanimous consent.[1] The bill is a combination of several stalled cybersecurity-related issues, including Federal Information Security Modernization Act (FISMA) Reform, Federal Risk and Authorization Management Program (FedRAMP), and cyber incident reporting.

   Among the key highlights for the incident reporting side are:[2]

   - The requirement that critical infrastructure owners report covered cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours after a covered entity "reasonably believes" that a covered incident has occurred.

   - The requirement that covered entities report ransomware payments to CISA within 24 hours of the payment being made.

- A section on how to submit voluntary reports of non-covered cyber incidents for those who want to help improve CISA's situational awareness.

- A section on the process and penalties for non-compliance, including CISA's ability to request information from entities that it believes have not reported and CISA's subpoena authority.

- A section outlining the circumstances and breadth of protections for entities that share reports and the limitations on how information contained in reports can be used.

The bill has since been broken up, with the intention of passing the cyber incident reporting language as part of the Omnibus. Should it pass, it will almost certainly be signed into law, as the Biden administration has already signaled support for the issue.

Action & Analysis
Membership required

2. Conti Ransomware Group Internal Leak

The Russian invasion of Ukraine has also sparked some interesting developments within the cybercrime ecosystem. One of the most significant developments to be publicly reported is the internal schism that appears to have occurred within the Conti ransomware group. On February 27th, numerous internal Conti chat logs were published on Twitter, and further leaks have come out since then.[3] The leaks have provided a valuable window into Conti's operations and may pose some questions about regulatory action.

It appears as if a pro-Ukrainian element within Conti did not appreciate the group's official statement that it backed the Russian government over the recent invasion of Ukraine and decided to leak a significant amount of data that included Conti's internal chats over a period of years, screenshots of tools, and information on Conti's cyber infrastructure.[4, 5] Based on the amount and level of information, cybersecurity company Rapid7 believes that whoever is behind the leaks is likely a senior member of the group.

Some of the more notable takeaways from the leaked information include:

- Information on Conti's "primary bitcoin address," with a value of more than two billion USD as of February 28th.[6]

- Evidence of Conti's relationship with the Russian Federal Security Service (FSB)[7] and other communications from 2021 suggesting a friendly relationship with Russian law enforcement agencies.[8]

- A screenshot of a Conti control panel showing "a number of compromised hosts and a breakdown of the operating systems, antiviruses, user rights, and detailed information about the infected assets."[9]

- Evidence that Conti appears to have had more than 100 salaried employees at some points in time; however, staffing levels appear to vary significantly.[10]

- Internal communications that detail the sophistication and damage related to the National Security Agency's (NSA) sabotage of the Trickbot malware in 2020.[11]

- Conti communications that suggest it specifically targeted American healthcare organizations during COVID-19 that coincided with a U.S. government warning to the healthcare sector in October 2020.[12]

- Conti communications that show the group spent significant funds on intelligence tools to ascertain "how much insurance a company maintains; their latest earnings estimates; and contact information of executive officers and board members."[13]

- Conti communications that shed some light on how ransomware negotiators interact with ransomware groups.[14]

- Conti communications that show that members were involved in numerous other criminal schemes beyond ransomware, including a variety of cryptocurrency scams.[15]

Despite the significance of the leaks, it appears that Conti's leadership has not been successful at determining who is responsible. Several leaks have been posted since February 27th, alongside messages of support for Ukraine. However, for those hoping that the leaks would lead to long-lasting damage, some experts have noted that compromised infrastructure has already been largely replaced and the group has rebounded swiftly.

Action & Analysis
Membership required

Congress

Tuesday, March 8th:
- No relevant hearings

Wednesday, March 9th:

March 9, 2022

- No relevant hearings

Thursday, March 10th:
- Senate – Intelligence Committee: Hearings to Examine Worldwide Threats

International Hearings/Meetings –

- No relevant meetings

EU –

Thursday, March 17th:
- European Parliament – Public Hearing: General Data Protection Regulation implementation, enforcement and lessons learned

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.congress.gov/bill/117th-congress/senate-bill/3600?r=3&s=1

[2] https://www.congress.gov/bill/117th-congress/senate-bill/3600/text?r=3&s=1#toc-id1E3C7124ACBA4C4986D04F51AD1E8045

[3] https://www.rapid7.com/blog/post/2022/03/01/conti-ransomware-group-internal-chats-leaked-over-russia-ukraine-conflict/

[4] https://arstechnica.com/information-technology/2022/03/conti-cybergang-gloated-when-leaking-victims-data-now-the-tables-are-turned/

[5] https://www.rapid7.com/blog/post/2022/03/01/conti-ransomware-group-internal-chats-leaked-over-russia-ukraine-conflict/

[6] https://www.rapid7.com/blog/post/2022/03/01/conti-ransomware-group-internal-chats-leaked-over-russia-ukraine-conflict/

[7] https://www.rapid7.com/blog/post/2022/03/01/conti-ransomware-group-internal-chats-leaked-over-russia-ukraine-conflict/

[8] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/

[9] https://www.rapid7.com/blog/post/2022/03/01/conti-ransomware-group-internal-chats-leaked-over-russia-ukraine-conflict/

[10] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/

[11] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/

[12] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/

[13] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/

[14] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/

[15] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iv-cryptocrime/