March 9th, 2021

TLP White

This week, *Hacking Healthcare* begins by drawing your attention to the latest publication in the H-ISAC's own ongoing series of white papers designed to introduce CISOs to an identity-centric approach to cybersecurity. Next, we briefly examine a comprehensive report from the New York Cyber Task Force (NYCTF) that highlights the United States' need to invest in a whole-of-nation response to plausible cyber crises. Finally, we detail concerns that Ryuk ransomware is evolving some dangerous new capabilities. Welcome back to *Hacking Healthcare*.

1. **H-ISAC Publishes "All About Authentication: A Health-ISAC Guide for CISOs"**

   Within the healthcare sector, keeping an organization secure from cyber threats is a continuous and increasingly difficult task under the best of circumstances. In response, the H-ISAC began a series of white papers to introduce CISOs to an identity-centric approach to cybersecurity. Designed to be an approachable and holistic guide to assist CISOs in the health sector, the series provides an explanation of key concepts, outlines a framework, investigates various solutions, and highlights aspects of implementation. The most recent addition to this series is *All About Authentication: A Health-ISAC Guide for CISOs*.[1]

   If you've ever been lost in a whirlwind of unfamiliar authentication acronyms, been confused about how to weigh the pros and cons of various authentication technologies, or just wanted to know where to begin on the subject in general, this free and publicly available guide is for you.

   The guide helpfully:

   - Contains a breakdown on authentication's basics;
   - Extolls the importance of usability;
   - Details a framework for how to view various authentication technologies;
   - Gives an overview of various authentication technologies;
   - Discusses the transition from static multi-factor authentication (MFA) to continuous authentication; and

- Explores two case studies from healthcare organizations that recently transitioned to modern authentication solutions.

It is our hope that the paper will help empower healthcare sector CISOs to take steps to ensure their organization has implemented an appropriate solution for their particular use cases.

Action & Analysis
H-ISAC Membership Required

2. Report Calls for Whole-Of-Nation Approach to Meet Potential Major Cyber Crises

At the end of last month, a report from the New York Cyber Task Force was published that called for "a whole-of-nation approach to enable enhanced cyber readiness through operational collaboration."[2] The 64-page report makes the case that the nation is unprepared to respond to a major cyber crisis, and that the United States "must reduce its vulnerability to strategic disruption by adversaries acting through cyberspace."[3] Central to the findings and recommendations of the report is the need to create "a public-private network of empowered nodes to provide effective crisis response to strategic cyber contingencies."[4]

The report notes that existing geopolitical and social tensions, technological dependencies, and "inherent advantages for ever-more capable cyber attackers" make the threat of a major cyber crisis all the more likely.[5] In turn, these plausible crises have the potential to cause "significant adverse effects on public safety, the economy, and national security."[6]

For the report, the NYCTF brought together a group of more than 40 individuals from a variety of industry sectors including cybersecurity, finance, academia, and government to construct "severe" but plausible near-future scenarios to assess the nation's readiness to defend itself. They concluded that the "United States must undertake a focused, urgent cyber readiness effort through improving operational collaboration."[7] The report ultimately offered up 5 recommendations and corresponding enabling actions that include:

1. Identify National Cyber Crisis Contingencies;
2. Establish a National Cyber Response Network (NCRN);
3. Operation of the NCRN;
4. Assess National Cyber Response Capabilities to Ensure Readiness; and
5. Ensure National Cyber Readiness Through Training and Exercises.

The report is available for free online by the initiative's sponsor, Columbia University's School of International and Public Affairs. Interested parties are encouraged to review the full report.

Action & Analysis
H-ISAC Membership Required

3. Ryuk Ransomware Demonstrates New Capabilities, Raising Threat

Last week, France's cybersecurity agency, the National Agency for the Security of Information Systems (ANSSI), released an analysis concluding that a new sample of the Ryuk ransomware strain appeared to have worm-like or self-replicating abilities.[8] ANSSI stated in their report:

> *"A Ryuk sample with worm-like capabilities allowing it to spread automatically within networks it infects, was discovered during an incident response handled by the ANSSI in early 2021."*[9]

Ryuk is one of the most widespread ransomware strains in the world and has particularly plagued the healthcare sector since it was first discovered in 2018. The newly detected capabilities will allow Ryuk to spread from machine to machine without input from the ransomware operator. It is expected that this capability would automate lateral movement within an infected network, and thus make containment and remediation more costly and difficult.

As many are already aware, ransomware attacks against the healthcare sector have risen significantly during the COVID-19 pandemic, and Ryuk is a large part of that trend. A recent report found that at the end of 2020 Ryuk was used in 75% of the ransomware attacks on the healthcare sector in the U.S.[10] Additionally, in October 2020, the FBI, Department of Homeland Security, and Department of Health and Human Services issued an alert specifically citing Ryuk as a threat to the healthcare sector.[11] The alert detailed the tactics, techniques, and procedures used by cybercriminals capitalizing on Ryuk and further detailed the technical details Ryuk uses so an entity can check if they have been infiltrated.

However, Ryuk ransomware is not just a problem in the U.S. Ryuk ransomware attacks thought to be carried out by a Russian or North Korean actor and have targeted companies and hospitals across Europe – including in France, the U.K, and Germany.

Action & Analysis
H-ISAC Membership Required

March 9th, 2021

Congress –

Tuesday, March 9th:
- No relevant hearings

Wednesday, March 10th:
- No relevant hearings

Thursday, March 11th:
- No relevant hearings

International Hearings/Meetings –

- No relevant hearings

EU –

- No relevant hearings

Conferences, Webinars, and Summits –

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

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

---

[1] https://h-isac.org/authentication-a-health-isac-guide-for-cisos/
[2] https://www.sipa.columbia.edu/sites/default/files/embedded-media/NYCTF%20-%20Enhancing%20Readiness%20for%20National%20Cyber%20Defense%20through%20Operational%20Collaboration.pdf
[3] https://www.sipa.columbia.edu/sites/default/files/embedded-media/NYCTF%20-%20Enhancing%20Readiness%20for%20National%20Cyber%20Defense%20through%20Operational%20Collaboration.pdf
[4] https://www.sipa.columbia.edu/sites/default/files/embedded-media/NYCTF%202020%20Executive%20Summary.pdf
[5] https://www.sipa.columbia.edu/sites/default/files/embedded-media/NYCTF%202020%20Executive%20Summary.pdf
[6] https://www.sipa.columbia.edu/sites/default/files/embedded-media/NYCTF%202020%20Executive%20Summary.pdf
[7] https://www.sipa.columbia.edu/sites/default/files/embedded-media/NYCTF%202020%20Executive%20Summary.pdf
[8] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf
[9] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf
[10] https://www.cyberscoop.com/ryuk-ransomware-develops-worm-like-capabilities-anssi-france/
[11] https://us-cert.cisa.gov/ncas/alerts/aa20-302a