September 8th, 2021

TLP White

This week, *Hacking Healthcare* begins by highlighting a notice for the National Institute of Standards and Technology's (NIST) new telehealth cybersecurity project, which is presently open for industry comment. Next, we briefly examine a new healthcare sector cybersecurity study that emphasizes how malicious actors are increasingly targeting smaller outpatient and specialty clinics. We then break down how a disgruntled ransomware affiliate leaked a ransomware playbook and what security researchers have gleaned from investigating it. Finally, we wrap up with a report on insider threats, and we put a spotlight on the need for interdepartmental collaboration to help mitigate such threats effectively.

Welcome back to *Hacking Healthcare*.

1. **NIST Releases Telehealth Cybersecurity Draft Project**

   The NIST National Center of Excellence (NCCoE) has released a new draft project entitled *Mitigating Cybersecurity Risk in Telehealth Smart Home Integration*.[1] Recognizing that telehealth technology has evolved in tandem with IoT to the point that individuals now often use consumer-grade IoT devices to access and interact with their health information, NIST is looking to create guidance that will help bolster the security of the home environments and networks through which such interactions take place.

   The 21-page draft will be used to help "further identify project requirements, scope, along with hardware and software components for use in a laboratory environment," and NIST is seeking comments from interested parties to better shape the project going forward. Those interested should submit comments on or before October 4th.[2, 3]

2. **Outpatient and Specialty Clinics Increasingly Targeted**

   A new report from Critical Insight, a managed IT service provider for healthcare, is calling attention to the targeting of outpatient facilities and specialty clinics by malicious cyber actors. Their analysis of the first half of 2021 raises some interesting questions and reiterates some assumptions about healthcare sector cyberattacks and the malicious actors that carry them out.

The 23-page *Healthcare Breach Report Jan-June 2021* examines who in the healthcare sector is getting breached and how the healthcare sector is being targeted.[4] Perhaps the most interesting finding in the report is that "[o]utpatient facilities and specialty clinics were breached nearly as much as hospitals in H1 2021."[5]

Critical Insight points out that its natural for malicious actors to target organizations with weaker defenses, and smaller outpatient and specialty organizations typically don't have the ability to spend as much on cybersecurity as larger hospital systems.[6] This makes these smaller organizations especially attractive targets as healthcare data routinely tops the charts as the most valuable to criminals and most costly to victims. These same reasons for increased cyber risk likely apply to Business Associates, as defined by HIPAA, as the report noted that they accounted for 43% of healthcare breaches, a "continuation of a 3-year upward trend."[7, 8]

Action & Analysis

3. Ransomware Playbook Spills Conti Secrets

From our "No Honor Among Thieves" department, we reveal that last month, an affiliate of the Conti ransomware group leaked information on the group's own infrastructure and 113MB of tools and training documents.[9] Unconfirmed reports suggest that the individual in question released the documents in retaliation after being banned by Conti for luring business away from them to another group.[10] Since then, the Russian language documents have been translated, and they now provide a window into how Conti affiliates are instructed to act.

According to Bleeping Computer, an unnamed security researcher alleged the files contained "a manual on deploying Cobalt Strike, mimikatz to dump NTLM hashes, and numerous other text files filled with various commands."[11] Other researchers have since confirmed that the documents match well with known Conti methods and attacks, likely confirming their legitimacy.[12]

Vitali Kremez, CEO of Advanced Intel and a self-described ethical hacker, told Bleeping Computer that "[t]he implications are huge and allow new pentester ransomware operators to level up their pentester skills," and that "[t]he leak also shows the maturity of their ransomware organization and how sophisticated, meticulous and experienced they are."[13]

Recently, Cisco Talos researchers provided an updated and corrected translation of the documents.[14] A review of the new translation confirms the thoroughness of the instructions to the point that "[s]ome adversaries who are very new to the malware scene could follow this playbook to compromise a major, enterprise network with

relatively little experience."[15] Furthermore, Cisco Talos stated the documents "display a familiarity with corporate network environments, such as where prized assets are located and how to access them. This is particularly true for U.S. and European networks, which they note have enhanced documentation that provides for easier targeting."[16]

Actions & Analysis

4. Don't Forget Insider Threats

How prepared are you for insider threats? According to new research from the Ponemon Institute sponsored by the cybersecurity company DTEX Systems, there is a good chance you have room for improvement.

Citing recent data breach reports and high-profile incidents at Tesla and Verkada as "[demonstrating] a need for additional education around how to identify and mitigate risks associated with insider threats," the Ponemon Institute carried out a survey of 1,249 IT and IT security professionals in North America, Western Europe and Australia/ New Zealand.[17] The resulting 6-page report, *The State of Insider Threats 2021: Behavioral Awareness & Visibility Remain Elusive,* underscores the difficulty of adequately defending against insider threats.

The report indicates that organizations may be able to do more and that many "are missing the early warning signs of insider threats and the desired endgame or intent of the perpetrators."[18] According to Ponemon, "the vast majority of security threats follow a pattern or sequence of activity leading up to an attack, and insider threats are no exception." As such, DTEX has proposed an *Insider Threat Kill Chain* that they believe helps frame the vast majority of insider threats.

According to DTEX, the five step kill chain includes:

- Reconnaissance – to include researching where useful data is and testing security controls
- Circumvention – to include attempts to bypass security controls
- Aggregation – to include the aggregation of data in a place for extraction
- Obfuscation – to include attempts to hide malicious activity
- Exfiltration – to include routs to exfiltrate data

Through this lens, the report states that 49% of organizations find recognizing malicious reconnaissance to be very difficult to impossible to detect. This level of difficulty extends to recognizing warning signs in Circumvention (47%), Aggregation (53%), Obfuscation (42%), and Exfiltration (40%) as well.[19] The report concludes with recommendations for organizations to improve their security posture, fill gaps in

monitoring controls and practices, and designate an ultimate authority for addressing this type of risk. The report is freely available for those interested in reviewing it.

Action & Analysis

Congress –

Tuesday, September 7th:
- No relevant hearings

Wednesday, September 8th:
- No relevant hearings

Thursday, September 9th:
- No relevant hearings

International Hearings/Meetings –
- No relevant meetings

EU –

Thursday, September 9th:
- European Parliament: Committee on the Environment, Public Health and Food Safety – Committee Meeting

Conferences, Webinars, and Summits –

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

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

[1] https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-shi-project-description-draft.pdf
[2] https://www.nccoe.nist.gov/webform/comments-draft-project-description-mitigating-cybersecurity-risk-telehealth-smart-home
[3] https://content.govdelivery.com/accounts/USNIST/bulletins/2ee5ab0
[4] https://cybersecurity.criticalinsight.com/2021_healthcare_data_breach_report
[5] https://cybersecurity.criticalinsight.com/2021_healthcare_data_breach_report
[6] https://cybersecurity.criticalinsight.com/2021_healthcare_data_breach_report

[7] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html
[8] https://cybersecurity.criticalinsight.com/2021_healthcare_data_breach_report
[9] https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/
[10] https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/
[11] https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/
[12] https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/
[13] https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/
[14] https://www.bleepingcomputer.com/news/security/translated-conti-ransomware-playbook-gives-insight-into-attacks/
[15] https://blog.talosintelligence.com/2021/09/Conti-leak-translation.html
[16] https://blog.talosintelligence.com/2021/09/Conti-leak-translation.html
[17] https://www2.dtexsystems.com/ponemon-state-insider-threats-2021-report
[18] https://www2.dtexsystems.com/ponemon-state-insider-threats-2021-report
[19] https://www2.dtexsystems.com/ponemon-state-insider-threats-2021-report