February 17th, 2021

Hacking Healthcare

TLP Amber

This week, *Hacking Healthcare* begins with a breakdown of some high-level findings from the Cyber Threat Intelligence League's (CTIL) first ever *Darknet Report*. We analyze the report and extrapolate it into a discussion about indirect threats to the healthcare sector. Next, we examine some alarming news that a malicious entity's remote access to a water treatment facility in Florida could have resulted in making the water toxic. Finally, we emphasize that healthcare organizations should ensure they are appropriately securing their health apps by detailing a new report that found significant vulnerabilities in a number of widely used mobile health apps and APIs.   Welcome back to *Hacking Healthcare*.

1. Cyber Threat Intelligence League Releases 2021 Darknet Report

As the COVID-19 pandemic kicked off, it quickly became clear that cyber criminals and even nation-state actors would not refrain from targeting the healthcare sector, despite some early suggestions that they might. With healthcare sector security and IT already stretched thin, and with various governments overwhelmed from the fallout of COVID-19, a group of cybersecurity researchers and law enforcement personnel came together to form the CTIL. The organization's stated goal is to provide "support [for] its healthcare and law enforcement partners" and "reduce the likelihood and impact of cybersecurity-related issues so that caregivers can continue serving global public health goals."[1] To this end, they have recently released their first *Darknet Report*, "cataloging criminal activity related to healthcare and the COVID pandemic."[2]

The 26-page report provides key insights, CTIL's assessment of what to expect going forward, and a breakdown of seven specific threats: Ransomware, Initial Access Brokers, Opportunistic Cybercriminals, Disinformation Campaigns, Scammers, Phishing, and Databases. CTIL's top level insights include:[3]

- The top five ransomware variants that impacted healthcare in 2020 are Maze, Conti, Netwalker, REvil, and Ryuk, affecting over 100 organizations that they are aware of.
- Nearly two-thirds of healthcare cybercrime victims were in North America and Europe, though victims spanned every continent.

- Threat actors moved to target the healthcare industry with ransomware because of healthcare organizations' increased prominence during the pandemic and their high susceptibility to attacks.
- The proliferation of dark markets and supply chains significantly lowered the barrier to entry for cybercriminals to affect healthcare.
- The threat actors that deploy ransomware as part of their attack method will almost certainly increasingly target the healthcare sector as it has emerged as one of the most vulnerable industries during the pandemic.
- The business of Initial Access Brokers (IAB) has boomed in the year 2020. From Q2 2020 to Q4 2020, the number of IABs compromising and selling access to healthcare organizations and other life-saving organizations has more than doubled.

While not much of the information provided by CTIL is groundbreaking, the *Darknet Report* does provide another data point confirming emerging cyber threat trends targeting the healthcare sector. The breakdown provided in the report is also useful due to its broad approach. By examining not just the criminal and nation-state threats that directly target healthcare organizations, but also those that target the general population, the report does an admirable job of providing context for just how varied malicious cyber activities against the healthcare sector can be.

2. Hacker Breached Florida Water Treatment Facility

On February 5th at a water treatment plant in Oldsmar, Florida, a yet-to-be-named hacker broke into a water treatment plant's computer system and temporarily increased the amount of sodium hydroxide (lye) in the water to a dangerous level. Luckily, no one was harmed in the attack, as the lye levels were quickly reversed by astute personnel at the plant. While the entire population of Oldsmar (15,000 people) was at risk from this attack, Sheriff Bob Gualtieri stated the following in a press release: "At no time was there a significant adverse effect on the water being treated. Importantly, the public was not in danger."[4] City officials have also noted that even if the increased lye levels had not been caught immediately, the toxic water would have taken 24 to 36 hours to reach the city's population, and an automated PH testing safeguard would have caught the increased level of lye, triggered an alarm, and notifying personnel of the change before anyone could be harmed.

The bad actor was able to infiltrate the Oldsmar Water Treatment Facility's computer system through remote access software typically used by operators for IT maintenance. The remote access software, TeamViewer, has since been disabled.[5] Attributing the attack to a specific bad actor has been a challenge; currently, it is unknown if the attack was carried out by a domestic or foreign actor. Oldsmar is conducting a forensic investigation on the attack in conjunction with the Federal Bureau of Investigation (FBI) and Secret Service.

The attack was mentioned during a federal Committee on Homeland Security hearing titled "Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience" last week. Hearing witness Chris Krebs, Former Director of the Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security, stated during the hearing that this attack could be an insider or disgruntled employee, but it is also possible it was a foreign actor. Another hearing witness, Michael Daniel, President and CEO of the Cyber Threat Alliance, said he thought the attack came from overseas due to the commonalities between this attack and a previous attack on Israel's water system by Iran. Krebs underlined at the hearing that tens of thousands of water treatment facilities across the country need to invest in software updates.

Action & Analysis

While luckily no one was harmed as a result of this attack, a successful infiltration of critical infrastructure is a dire reminder of the consequences of insufficient cybersecurity practices. After initial reports of the compromise, it was revealed that even though TeamViewer had not been used in six months, it was still installed on the computer system. Additionally, all computers shared the same password for TeamViewer, and a state advisory further detailed that the water treatment plant computers were connected to the Internet directly without firewall protection.[6] Given the details currently available, the attack on the Oldsmar water treatment facility does not appear to be a sophisticated one. Instead, it appears as though several poor cybersecurity practices created a relatively easy path for the attacker to exploit.

As Krebs mentioned in his comments to the Committee on Homeland Security, it is imperative that critical infrastructure facilities across the U.S. invest in software updates to prevent attacks like this in the future. Remote access tools, especially during the current work-from-home increase, could be exploited in the healthcare and public health sector just as much as any other sector. On a positive note, this attack could help incentivize critical infrastructure providers to examine their current security measures and invest in stronger cybersecurity practices where appropriate.

There are a few essential lessons organizations can take away from this event. First, it is of critical importance to routinely assess whether a system needs to be Internet connected, and if so, to quantify the inherent risk and potential mitigations.

Next, and we really shouldn't have to say this anymore, but you should be examining your password policies and assessing whether they are being properly implemented and enforced. Strong password policies generally include requirements for the following: different passwords for each employee, and multi-factor authentication where possible (which TeamViewer supports).

Third, if you aren't already, we suggest you consider applying the principle of least privilege to ensure user accounts are only able to access parts of the network that are essential to perform that user's duties.

And finally, don't leave software running that you don't need. To be fair, you can't always know when you might need remote access or other legacy services, but this reality only reinforces the importance of taking the other steps noted above in an effort to mitigate critical risks.

None of this is new, nor does it require any special tools or a large budget. It does, however, require spending the time to make sure these fundamental practices are in place for your organization. Additionally, these recommendations align with U.S. government best practice recommendations. The National Institute of Standards and Technology (NIST) has a helpful resources page for all sectors, including healthcare,[7] and CISA has a healthcare-specific sector plan through the National Infrastructure Protection Plan available online.[8] And, of course, sharing information and learnings with your H-ISAC colleagues is a great way to get help and suggestions. No matter how big or small your organization is, you really don't have to go it alone.

The last point we will make on this is that it highlights an important aspect of incident response that can sometimes be overlooked by security teams who are focused on dealing with the latest ransomware or data breach. What if this attack had been successful and your healthcare organization suddenly didn't have any safe water to use? What if wastewater treatment were impacted? Electricity? Now is as good a time as any to make sure your incident response policies and procedures consider these elements. Unfortunately, they are likely to continue.

3. Report Raises Healthcare Mobile Health App Security Concern

During 2020, COVID-19 underscored how vital it is for individuals across the globe to have access to digital products and services. Unfortunately, the rush to capitalize on that need led to some high-profile instances of cybersecurity and privacy best practices becoming less of a priority (or even ignored altogether). While communication applications like Zoom grabbed early headlines for less than stellar security, the healthcare sector has had its own mishaps. A recent report on healthcare app security is a sobering reminder that achieving adequate security and privacy is not an easy task for even the most highly resourced and well-intentioned organizations.

The healthcare sector is increasingly looking to digital products and services to reach both patients during the response to COVID-19 as well as underserved communities for whom in-person healthcare is a logistical challenge. This fact is partially responsible for the estimated 318,000 mobile health applications that exist in major app stores today.[9] The growing popularity of such applications led mobile app API security company *Approov* to sponsor cybersecurity marketing firm *Knight Ink* to investigate the security of 30 such health apps for vulnerabilities that could expose sensitive health and identity information.[10] The apps tested were not limited to small, unknown entities, and while the identities of those tested were kept anonymous, the average number of downloads for the apps tested was 772,619.[11]

The report's findings were disheartening, but also useful in underscoring just how difficult the task of securing health apps can be and what kinds of problems organizations should ensure they address. Key findings included:[12]

- Out of all thirty mHealth apps tested, 77% contained hardcoded API keys, some which don't expire, and 7% even contained hardcoded usernames and passwords.
- Out of the API endpoints tested, 100% of them were vulnerable to Broken Object Level Authorization (BOLA) attacks leading to unauthorized access to full patient records, downloadable lab results and x-ray images, blood work, allergies, and personally identifiable information (PII).
- 27% of the apps tested were not secured against reverse engineering through code obfuscation.
- 100% of the apps tested failed to implement certificate pinning, man-in-the-middle attacks against the app.
- 50% of the APIs tested allowed access to the pathology, x-rays, and clinical results of *other* patients.

The author of the study concluded that "mHealth companies need to implement more of a zero-trust approach to the security of their apps and APIs" and that "[t]here is a clear lack of static code analysis and penetration testing that would have mitigated many of the 'low hanging fruit'."[13]

Action & Analysis

The highly regulated nature of the healthcare sector is generally a good incentive to ensure that security and privacy efforts are appropriately resourced. However, this report suggests that even more can and should be done to secure mobile healthcare apps. Some of the report's identified flaws, like hardcoded passwords, violate basic security-by-design principles that should be regarded as accepted best practice by now. Other issues, such the high rate of BOLA vulnerabilities and failure to implement certificate pinning, appear to suggest some vulnerability vectors may not be covered by current testing policies and procedures.

While organizations will always have to balance security and business needs, the ramifications of failing to adequately secure mobile health apps can be enormous. Laws and regulations can impose significant monetary penalties for a lack of reasonable security measures, and the loss of patient trust can impact customer retention. We would advise all organizations that operate a mobile health app, or are considering developing one, to assess if security and privacy considerations are being given the proper amount of prioritization. For those interested, the full *Approov/Knight Ink* report provides significantly more detail around the types of vulnerabilities that were found.

Congress –

Tuesday, February 16th:

- No relevant hearings

Wednesday, February 17th:

- No relevant hearings

Thursday, February 18th:

- 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://cti-league.com/blog/darknet-report-2021/
[2] https://cti-league.com/blog/darknet-report-2021/
[3] https://cti-league.com/blog/darknet-report-2021/
[4] https://www.cyberscoop.com/florida-hacker-water-plant-sodium-hydroxide/
[5] https://www.cyberscoop.com/florida-hacker-water-plant-sodium-hydroxide/
[6] https://www.cnn.com/2021/02/11/us/florida-water-plant-hack/index.html
[7] https://www.nist.gov/cyberframework/critical-infrastructure-resources
[8] https://www.cisa.gov/healthcare-and-public-health-sector
[9] https://www.mobius.md/2019/03/20/11-mobile-health-statistics/
[10] https://www.mobihealthnews.com/news/report-patient-info-risk-due-rampant-api-vulnerabilities-among-major-mobile-health-apps
[11] https://approov.io/mhealth/hacking/
[12] https://approov.io/mhealth/hacking/
[13] https://approov.io/mhealth/hacking/