February 9th, 2021

TLP White

This week, *Hacking Healthcare* begins with another look at ransomware. Specifically, we analyze trends that emerged throughout the past year, data from the last quarter of 2020 and what it tells us about where things are headed, and why ransomware becoming less lucrative for cyber criminals may actually be harmful to the healthcare sector. We wrap up by breaking down a non-traditional cyber 'threat' that has the potential to harm vaccination roll-out, and why solutions may not be so easy to come by. Welcome back to *Hacking Healthcare*.

1. 2020 Ransomware Review

It seems like a safe bet that ransomware will continue to be a scourge in 2021, but some newly released information suggests that evolving methods and tactics will help ensure the situation will remain fluid. A number of recent reports has helped to put the scale of the issue into context, and the outsized impact ransomware has had on the healthcare sector is no surprise. There are several noteworthy takeaways from this data, including potentially encouraging news that suggests that ransomware attacks are becoming less lucrative for perpetrators. However, our analysis section will explore why that may not signal a benefit for the healthcare sector.

Recap

First, let's quickly recap where things stand. The challenges faced by the healthcare sector have been enormous over the past year, and cyber criminals certainly did not make dealing with COVID-19 any easier. VMware Carbon Black reported 239.4 million attempted cyberattacks against its own healthcare clients alone in 2020, culminating in the almost unbelievable statistic that "healthcare entities saw 816 attacks per endpoint last year, an incredible 9,851 percent increase from 2019."[1] This information comes just weeks after cybersecurity firm Emsisoft reported that at least 560 healthcare provider facilities were hit by ransomware in 2020.[2]

Discouragingly, the most prevalent ransomware hitting the healthcare sector appears to have been Cerber. Rampant in 2017, Cerber had dropped off considerably by 2018, before taking off once again last year and accounting for 58% of ransomware attacks against VMware Carbon Black's healthcare sector customers.[3] While Carbon Black noted that Cerber had undergone updates and adaptations, some of the variants' successes in

2020 are almost certainly linked to unpatched vulnerabilities, once again highlighting an added difficulty of cybersecurity in the healthcare sector.[4]

A Positive Sign with Dangerous Potential

Ending with potentially good news, ransomware response and recovery firm Coveware released their *Quarterly Ransomware Report* for Q4 of 2020 last Monday. The most significant takeaway appears to be their reporting that ransomware payments have significantly dropped off. By their numbers, the average ransomware payment fell by roughly 34% from Q3 2020, down to $154,108 from $233,817.[5] Additionally, the median ransomware payment made in Q4 saw an even bigger drop of roughly 55%, down to $49,450 from $110,532.[6]

Prior to this newest report, Coveware had previously reported steady increases in average and median ransomware payments going back to Q4 2018.[7] Coveware attributes the recent decline partially to the erosion of trust that ransomware actors who exfiltrate data will actually delete it upon receiving a ransom. Numerous examples of "deleted" data being resold on the black market or being used to hold an organization for ransom a second time, have altered the risk calculus for ransomware victims.

While the full report contains much more information, a few interesting notes caught our eye. First, email phishing continues its upward climb as an attack vector, breaking the 50% mark and overtaking RDP compromise. Second, roughly 70% of ransomware attacks in Q4 involved a threat to leak exfiltrated data, an increase of 20 percentage points over Q3.[8] Furthermore, Coveware reports that malicious actors are going so far as to "fabricate data exfiltration in cases where it did not occur." However, the most concerning bit of information may be Coveware's reported uptick in "the increase in the incidence of irreversible data destruction as opposed to just targeted destruction of backups or encryption of critical systems."[9]

Action & Analysis
H-ISAC Membership Required

2. Healthcare faces a non-traditional cyber 'threat'

While healthcare sector cybersecurity and IT teams already face the daunting challenge of maintaining the privacy and security of their networks and data in the face of all sorts of traditional state and non-state threats, there may be another non-traditional technical challenge where their skills could be useful.

In the rush to get entire countries vaccinated, healthcare organizations are confronting the unprecedented administrative and logistical task of organizing appointments for patients while striving for the smallest possible waste of precious vaccine doses. To aid in this effort, many organizations have been using some form of online portal or scheduler. The US Department of Health and Human Services (HHS) even released a

notice of enforcement discretion for *Online or Web-Based Scheduling Applications*.[10] Unfortunately, these schedulers have become the victim of 'bot' attacks orchestrated by scalpers.

According to Reuters, "U.S. retailers and pharmacies like Walgreens and CVS Health are preparing for a fresh round of "bot" attacks by scalpers hoping to snap up COVID-19 vaccine appointments."[11] While this kind of behavior is familiar to anyone trying to purchase quantity-limited items, like the newest tech gadget or sporting event tickets, both of those circumstances are more easily categorized as an annoyance. The same cannot be said if such behavior begins to significantly impact vaccination rollouts.

According to Reuters, "[i]n recent weeks, people shared on social media networks horror stories of attempting to secure vaccination appointments from government sources, with some blaming bots for site crashes and stolen slots." Both Walgreens and CVS have indicated they are aware of the issue and have instituted multiple defenses for detection and prevention.

Action & Analysis
H-ISAC Membership Required

Congress –

Tuesday, February 9th:
- No relevant hearings

Wednesday, February 10th:
- House of Representatives – Committee on Homeland Security Hearing: *Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience*

Thursday, February 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://healthitsecurity.com/news/70-ransomware-attacks-cause-data-exfiltration-phishing-top-entry-point
[2] https://healthitsecurity.com/news/560-healthcare-providers-fell-victim-to-ransomware-attacks-in-2020
[3] https://www.zdnet.com/article/this-old-form-of-ransomware-has-returned-with-new-tricks-and-new-targets/

[4] https://www.zdnet.com/article/this-old-form-of-ransomware-has-returned-with-new-tricks-and-new-targets/
[5] https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
[6] https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
[7] https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
[8] https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
[9] https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
[10] https://www.hhs.gov/sites/default/files/hipaa-vaccine-ned.pdf
[11] https://www.reuters.com/article/us-health-coronavirus-scalpers-focus-idUSKBN2A524S