October 6th, 2020

TLP White

This week, *Hacking Healthcare* talks ransomware yet again. This pervasive threat continues to plague organizations across all sectors and the globe, and we believe it warrants continued attention.

We begin by exploring what cybersecurity reports from IBM and Microsoft have to say about the current state of ransomware and why new attack trends are specifically noteworthy for healthcare organizations. Next, we look at the just-released Europol report on Internet organized crime to get a sense of the European perspective on ransomware. Finally, we conclude by hopefully alleviating some concern around the recent United States Treasury Department advisory that raised an alarm for those that deal with ransomware remediation. ***Please give us a minute of your time to answer a few questions about this week's Hacking Healthcare topics. We'll publish the results in an upcoming issue. Survey link follows the articles below.***

Welcome back to *Hacking Healthcare*.

1. **Ransomware is Growing and Maturing.** According to separate reports released last week by IBM's Security X-Force Incident Response and Microsoft, ransomware is clearly still thriving, and some worrisome activities may be beginning to solidify into common practice. If you weren't already taking steps to prepare for a potential ransomware attack, hopefully what follows will convince you to get started.

   First, while the prevalence of ransomware is fairly obvious, it is worth reiterating the scale of the issue. IBM's report states that their incident response teams have remediated three times the number of ransomware attacks in Q2 2020 than in Q1, representing 32% of all incidents between April and June.[1] This was echoed by Microsoft, who reported that ransomware has been their most common incident response from October 2019 through July 2020.[2]

   However, what may be most concerning is what appears to be a maturation in ransomware tactics by malicious threat actors. IBM reports there is a notable "new emphasis on blended extortion-ransomware attacks."[3] This is the type of attack where threat actors attempt to steal information in addition to encrypting a target's files. Once stolen, this information can be used as added leverage to push for payment. And speaking of payment, IBM has also noted that ransom demands are trending upwards, with some examples topping the $40 million mark.[4]

A few additional statistics worth noting are:[5]

- 41% of ransomware attacks targeted operational technology networks.
- Ransomware threat actors appear to "[seek] out victims with a low tolerance for downtime."
- Asia and North America have been the regions where IBM's Security X-Force has responded to the most ransomware incidents in 2020 – at 33% and 30% respectively.

Action & Analysis
H-ISAC Membership Required

2. **Europe's Ransomware Perspective**. According to the newly released *Internet Organized Crime Threat Assessment 2020* report from Europol, Europe's ransomware experience is similar to the rest of the world. The annual report cited ransomware as a serious issue "for cyber investigators across the EU," and noted that ransomware was "one of the, if not the, most dominant threats."[6] However, Europol's report highlights an issue not mentioned by IBM or Microsoft: the underreporting of ransomware events by the private sector.

   At the start, the Europol report largely corroborates the figures from both Microsoft and IBM's reports. In addition to noting that ransomware attacks are becoming increasingly targeted and sophisticated, Europol points out that the higher payouts from ransomware attacks are at least partially related to the increased investment of malicious actors themselves. This investment includes more comprehensive reconnaissance of targets, broader and deeper collaboration with other criminal groups, and better tools.[7] Additionally, Europol notes the development of Ransomware-as-a-service, and credits it with lowering the barrier of entry to less sophisticated malicious actors.[8]

   However, one of the more interesting items that Europol notes is just how reluctant organizations in some EU states are to come forward to either the public or law enforcement when they are victimized by ransomware. According to Europol, several law enforcement authorities have only been able to identify ransomware attacks through notices in local media rather than direct reporting. Europol also stated that "victims prefer to engage with private sector security firms for investigating the attack or negotiating with the extortionists."[9] While this may be understandable to a degree, some of the hesitancy to report to government authorities presents a real cause for concern.

   Perhaps most worrisome is the announcement that "some of the companies that negotiate the ransom payment are working on the edge of legality, as they have developed a trusted business relationship with the ransomware actors."[10] This can include the perpetrator even referencing these companies directly to the victim with an offer to lower the ransom cost if they choose a preferred partner. Of course, by doing so, the "victims will not file an official complaint" with law enforcement.[11]

Action & Analysis
H-ISAC Membership Required

3. **United States Treasury Department Sends Ransomware Advisory Warning.** The Treasury Department made news last week with the release of an October 1st memo entitled *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*.[12] In the memo, the Treasury Department took a hard line by saying: "Companies that facilitate ransomware payments to cyber actors on behalf of victims… not only encourage future ransomware payment demands but also may risk violating [Office of Foreign Assets Control (OFAC)] regulations."[13]

   For those unfamiliar, OFAC is responsible for administering and enforcing "economic and trade sanctions based on US foreign policy and national security goals."[14] These sanctions can be targeted against numerous classifications of individuals and entities that are deemed to be a "[threat] to the national security, foreign policy or economy of the United States."[15] OFAC's interest in ransomware is partially due to how ransom payments are often a source of income for threat actors that have ties to antagonistic foreign governments.

   The five-page advisory begins by noting the recent increase in prevalence and sophistication of ransomware. In response, Treasury's OFAC has been routinely designating the developers and users of ransomware "under its cyber-related sanctions program and other sanctions programs."[16] As such, OFAC reiterated that it has, and will "continue to impose, sanctions on these actors and others who materially assist, sponsor, or provide financial, material, or technological support for these activities."[17]

   OFAC asserts that taking such actions is necessary as ransoms gained by these designated individuals could end up funding "activities adverse to the national security and foreign policy objectives of the United States," while also incentivizing further ransomware attacks.[18] As sound as that argument may be, the most critical section of the advisory might be the statement that "OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC."[19]

   Action & Analysis
   H-ISAC Membership Required

Survey:

Please take one minute to answer a few questions about this week's Hacking Healthcare by visiting this link: https://www.surveymonkey.com/r/Y673XSQ

October 6th, 2020

Congress –

Tuesday, October 6th:
- No relevant hearings

Wednesday, October 7th:
- No relevant hearings

Thursday, October 8th:
- No relevant hearings

International Hearings/Meetings –

EU – No relevant hearings

Sundries –

Foreign spies use front companies to disguise their hacking

https://www.cyberscoop.com/chinese-iranian-hackers-front-companies/

Chinese hacker group spotted using a UEFI bootkit in the wild

https://www.zdnet.com/article/chinese-hacker-group-spotted-using-a-uefi-bootkit-in-the-wild/

Conferences, Webinars, and Summits –

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

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

---

[1] https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/

2 Microsoft Digital Defense Report, September 2020

[3] https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/

[4] https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/

[5] https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/

[6] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

[7] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

[8] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

[9] file:///C:/Users/tcm03/Downloads/internet_organised_crime_threat_assessment_iocta_2020.pdf

[10] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

[11] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020
[12] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
[13] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
[14] https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information
[15] https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information
[16] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
[17] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
[18] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
[19] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf