AIR UNIVERSITY | AIR FORCE CYBER COLLEGE

WIZARD SPIDER: Lethally Poisonous Ransomware

Joshua A. Sipper, Air Force Cyber College

Narrative

October 1, 2019 at 11:03 AM CDT – "Three hospitals in the DCH Health System are not taking patients right now unless they are critical cases. The three hospitals, DCH Regional Medical Center, Northport Medical Center and Fayette Medical Center are under a ransomware attack"[1]. Critical cases are being diverted to other hospitals until the attack can be mitigated. This is a major blow to the Tuscaloosa, Alabama area as these hospitals are responsible for the healthcare of over 200,000 people. Current patients are being cared for and are not expected to be transferred unless under emergency circumstances. Emergencies will be accepted, but will be transferred immediately once stabilized. The ransomware attack forced DCH to revert to emergency procedures; implementing paper and pencil records in place of digital. Robert Hill, a cybersecurity expert believes that the attack, as others of its type, is maliciously targeted and will likely force DCH to pay the ransom quickly. "This will take out their ability to take care of patients and an organization like that is much more willing to pay ransom to get their systems back rapidly," Hill said[2]. The FBI and Secret Service have been called in to investigate as well, but generally, ransomware attacks inevitably end in payment of the ransom according to Hill[3].

October 7, 2019 at 11:35 AM CDT – "The Alabama hospital group DCH Health Systems has paid an undisclosed sum to the attackers who perpetrated a ransomware attack on its three hospitals in Tuscaloosa, Fayette and Northport"[4]. DCH has paid an undisclosed amount to a hacker for the encryption key to unlock and restore patient files and other vital medical system data. The hackers used the "Ryuk ransomware code, a malware that contains several bugs, resulting in damage about one in every eight files that it encrypts"[5]. Following the reception and use of the encryption key, DCH began the restoration of files and other system

1 WBRC Staff, (2019). Tuscaloosa hospitals crippled due to ransomware attack, ***WBRC News Report***, accessed 4/29/2020: https://www.wtvy.com/content/news/Tuscaloosa-hospitals-crippled-due-to-ransomware-attack-561974121.html

2 Ibid.

3 Ibid.

4 Eddy, N. (2019). Alabama hospital system DCH pays to restore systems after ransomware attack, Healthcare IT News, accessed 4/29/2019: https://www.healthcareitnews.com/news/alabama-hospital-system-dch-pays-restore-systems-after-ransomware-attack

5 Eddy, N. (2019). Alabama hospital system DCH pays to restore systems after ransomware attack, ***Healthcare IT News,*** accessed 4/29/2019: https://www.healthcareitnews.com/news/alabama-hospital-system-dch-pays-restore-systems-after-ransomware-attack

continued...

data in order to return to normal operations. "This will be a deliberate progression that will prioritize primary operating systems and essential functions for emergency care. DCH has thousands of computer devices in its network, so this process will take time," officials said in the statement[6]. Further analysis from cybersecurity experts revealed the probable origin of the attack. "A California-based cybersecurity firm believes the group of hackers who use the particular ransomware software found on DCH Health System computers work from Russia"[7]. This is based on signature data obtained through analysis of the "Ryuk" attack which was first spotted in August of 2018. "The cybersecurity firm Crowdstrike believes the Ryuk ransomware attacks emanate from a hacker group in Russia known as "WIZARD SPIDER" and that the Russian group has netted about $3.7 million in bitcoins since August 2018"[8].

****

December 23, 2019 – "Four patients of the DCH Health System filed a federal class-action lawsuit Monday alleging that the three west Alabama Hospitals violated health information privacy laws and disrupted their medical care when the system was hit with a ransomware attack in October"[9]. The patients cited negligence, invasion of privacy, breach of contract and breach of fiduciary duty in the lawsuit due to the effects of the ransomware exploitation. The negligence claim was related to health care workers being unable to address patient needs due to a lack of adequate data protection[10]. Invasion of privacy was related to the same lack of data protection which led to medical records being open to unauthorized parties[11]. Breach of fiduciary duty was purely related to the absence of care provided by medical personnel because of the lack of access to proper data, stemming from the lack of data and access protection incumbent upon the DCH Health System[12]. The patients also commented that several, critical healthcare benefits were denied them during the attack including: lost access to prescription medications and medical files, compromised medical files, disruption of healthcare, and lost access to necessary healthcare. "Sheneka Frieson, who filed as a plaintiff on behalf of a 7-year-old girl, claimed the girl went to Northport Medical Center for a severe allergic reaction that caused the girl's eyes to swell shut. A nurse allegedly told Frieson that the hospital was only taking emergency room patients and it would be a four to five-hour wait to be seen because of the ransomware attack. Frieson's, whose only options were to drive to Walgreens or go to Birmingham for medical care, claimed in the lawsuit that the girl's swelling took three days to go down 'as a consequence

6 Landi, H. (2019). Alabama health system pays hackers responsible for ransomware attack as FBI warns more to come, ***Fierce-Healthcare***, accessed 4/29/2019: https://www.fiercehealthcare.com/tech/alabama-based-dch-health-system-pays-hackers-responsible-for-ransomware-attack-as-fbi-warns

7 Burkhalter, E. (2019). DCH Hospital System pays Russian hackers in ransomware attack, ***AlabamaReporter.com***, accessed 4/29/2019: https://www.alreporter.com/2019/10/05/dch-hospital-system-pays-russian-hackers-in-ransomware-attack/

8 Ibid.

9 Koplowitz, H. (2019). DCH Health System patients file federal suit over ransomware attack, ***AL.com***, accessed 4/29/2019: https://www.al.com/news/tuscaloosa/2019/12/dch-health-system-patients-file-federal-suit-over-ransomware-attack.html

10 Koplowitz, H. (2019). DCH Health System patients file federal suit over ransomware attack, ***AL.com***, accessed 4/29/2019: https://www.al.com/news/tuscaloosa/2019/12/dch-health-system-patients-file-federal-suit-over-ransomware-attack.html

11 Koplowitz, H. (2019). DCH Health System patients file federal suit over ransomware attack, ***AL.com***, accessed 4/29/2019: https://www.al.com/news/tuscaloosa/2019/12/dch-health-system-patients-file-federal-suit-over-ransomware-attack.html

12 Koplowitz, H. (2019). DCH Health System patients file federal suit over ransomware attack, ***AL.com***, accessed 4/29/2019: https://www.al.com/news/tuscaloosa/2019/12/dch-health-system-patients-file-federal-suit-over-ransomware-attack.html

continued...

of this disruption to her medical care'"[13]. This is all in addition to a growing list of institutions whose data has been ransomed or exfiltrated as a result of hacks. "DCH is just the latest in ongoing health data breach lawsuits in the last year. Most recently, Solara Medical Supplies was hit with a class-action lawsuit, following a months-long breach that impacted about 114,000 patients"[14].

The attacks were also followed by analysis from law enforcement agencies, espousing the need for attention to tracking down malicious hackers and bringing them to justice. "The FBI issued a warning Oct. 2 that ransomware attacks are becoming 'more targeted, sophisticated and costly, even as the overall frequency of attacks remains consistent'"[15]. The sophistication is likely a result of the frequency of attacks as hackers will undoubtedly learn more and they repeat the process of the attack. "Cybercriminals are increasingly targeting software commonly used by managed and other third-party service providers…as was the case in the August incident in which 22 cities and towns in Texas were impacted, according to Emsisoft, a security firm involved in the investigation. The average ransom demand also has continued to increase in 2019. If one organization is willing to pay $500,000, the next may be willing to pay $600,000, Emsisoft said in its report"[16]. Regardless of the consequences, law enforcement is generally against paying ransoms. "The FBI does not advocate paying a ransom, the agency said, 'in part because it does not guarantee an organization will regain access to its data.' In some cases, victims who paid a ransom were never provided with decryption keys"[17]. Ransomware shows no sign of slowing, with at least 621 government entities, healthcare service providers, school districts, colleges and universities affected by ransomware in the first nine months of 2019, with 491 of those attacks against healthcare providers[18].

Background: Ransomware Analysis

Hackers have at their disposal an arsenal of cyber weaponry ready for immediate deployment. While some attacks can take weeks, months, and even years to plan and execute, malware attacks are available and ready for immediate release, causing 20 billion dollars in lost revenue annually[19]. Ransomware carries with it the capacity for multiple levels of damage including monetary, psychological, reputational, legal, and even physical effects. Each of these are explored in the Narrative above and will be covered throughout this analysis section. Obviously, the monetary damage results from loss of revenue from having to pay the ransom as well as the inability to operate as well as ensuing lawsuits. The psychological effects stem from the damage done to reputation as well as the health and welfare of patients and potentially employees as

13 Koplowitz, H. (2019). DCH Health System patients file federal suit over ransomware attack, ***AL.com***, accessed 4/29/2019: https://www.al.com/news/tuscaloosa/2019/12/dch-health-system-patients-file-federal-suit-over-ransomware-attack.html
14 Davis, J. (2020). DCH Health Faces Federal Lawsuit After 10-Day Ransomware Attack, ***HealthITSecurity.com***, accessed 4/29/2020: https://healthitsecurity.com/news/dch-health-faces-federal-lawsuit-after-10-day-ransomware-attack
15 Landi, H. (2019). Alabama health system pays hackers responsible for ransomware attack as FBI warns more to come, ***FierceHealthcare***, accessed 4/29/2019: https://www.fiercehealthcare.com/tech/alabama-based-dch-health-system-pays-hackers-responsible-for-ransomware-attack-as-fbi-warns
16 Landi, H. (2019). Alabama health system pays hackers responsible for ransomware attack as FBI warns more to come, ***FierceHealthcare***, accessed 4/29/2019: https://www.fiercehealthcare.com/tech/alabama-based-dch-health-system-pays-hackers-responsible-for-ransomware-attack-as-fbi-warns
17 Ibid.
18 Ibid.
19 Arezina, L (2021). Ransomware statistics in 2020: From random barrages to targeted hits," DataProt, Accessed 2/16/2021: https://dataprot.net/statistics/ransomware-statistics/

continued...

well. The legal ramifications are vast as denial of healthcare and the potential loss of life are paramount. Also, the physical effects of anything from chronic illness to dismemberment can potentially occur. This cyber attack vehicle is virtually ubiquitous, being used by hackers from nation-state actors all the way down to the range of petty criminals. With these facts in mind, let us explore the meaning, mode, methods, and malefactors of this vicious cyber tool.

Ransomware Meaning

Morse and Ramsay (2017) define ransomware as "malware that encrypts data in a host computer or mobile device with the intent to exchange a ransom payment for the decryption key"[20]. As we saw in the narrative above, hackers often use ransomware to extort hundreds of thousands of dollars in cryptocurrency from unsuspecting individuals and organizations (e.g., DCH Healthcare Systems). Ransomware is usually delivered through phishing emails with seemingly benign attachments such as Microsoft Word documents. However, when the recipient opens the attachment, embedded code is released and searches out files which it then encrypts. "Once encryption is complete, the ransomware will display an image on-screen with instructions for how the victim can remit a ransom to obtain a decryption code"[21]. The data that has been encrypted is still present. However, the code is necessary for complete restoral. While some data may be able to be restored from back-ups, it takes vast amounts of time for large entities like hospitals, health systems, and government agencies to restore the information. Even if the information is available for restoral, it might not be up-to-date or referenced properly, making retrieval and restoration impossible.

Several ransomware packages have been released over the years with varying levels of disruption. One of the most widely destructive ransomware attacks was(??) WannaCry. "WannaCry leveraged the EternalBlue vulnerability, which took over the news in May 2017 as a result of its inclusion in data leaked by the criminal syndicate known as The Shadow Brokers—a hacking group that has published several leaks of sensitive hacking tools originally developed by the National Security Agency (NSA)"[22]. With the combinatory power of EternalBlue and another malicious hacker tool named DoublePulsar, WannaCry spread extremely rapidly through the internet, infecting millions of users across 150 countries; a global ransomware phenomenon. Ransomware is an extremely powerful, albeit simple, tool that can be used widely and very effectively for illegal financial gain at the expense of innocents.

Ransomware Mode

Surprisingly, ransomware is not a tool relegated to only the hacker elite. Although the more potent forms are built by technically savvy hackers, there are numerous versions available to practically anyone with the money and the will to use them. "To expand their reach and operations, ransomware specialists offer their code and expertise to novice hackers online for a nominal fee, for no fee at all, or with a cut of any ransom

20 Morse, E. and Ramsey, I. (2017). Navigating the Perils of Ransomware, ***The Business Lawyer***, Vol. 72, No. 1 (WINTER 2016-2017), pp. 287-294.
21 Harkins, M. and Freed, A. (2018). The Ransomware Assault on the Healthcare Sector, ***Journal of Law & Cyber Warfare***, Vol. 6, No. 2 (Winter 2018), pp. 148-164.
22 Ibid.

continued...

obtained"[23]. Thus, the mode of ransomware hacking can start at a very low entry threshold with petty cybercriminals using it for fun, extortion, revenge, or smaller electronic payments. Coined Ransomware as a Service (RaaS), one such tool created for this purpose is Satan. "Satan's developers have posted the ransomware online, making it available for free to the public. Any would be cybercriminal with absolutely no programming skills can download and deploy Satan in just three easy steps, while also managing their ransomware campaigns in a central console hosted on the Satan developer page"[24]. These tools aren't just effective, but sophisticated, allowing their users to get more money and cause more damage quite rapidly.

Regardless of who commits ransomware attacks, the goal is almost always the same: money. But, how do the transactions between novice ransomware criminals and their elite counterparts take place without being tracked? How do the ransomware hackers receive their payments without being found and arrested? "Ransomware attacks often present a clear business case for payment. For example, hackers have targeted hospitals, effectively shutting down their operations by cutting off access to electronic patient records. In one case, system control was restored for the modest payment of $17,000 worth of bitcoin"[25]. Bitcoin and other cryptocurrency operate on an encryption scheme called blockchain which offers layers of obfuscation for monetary transfer. Additionally, cryptocurrency can be transferred within Dark Web spaces such as The Onion Router (TOR) so named to indicate its multiple layers of obscuring encryption.

Ransomware Methods

The methodology used by transmitters of ransomware all basically come down to the principles of denial, disruption, and degradation of information. However, the effects of these malicious attacks can travel the spectrum of harm and engagement from petty theft all the way to the loss of infrastructure and human life. Case in point is the Tuscaloosa hospital attack which is considered by most cyber professionals to be an infrastructure attack[26]. The concept of operations for ransomware use generally revolves around centers of sustainment, power, and opportunity such as infrastructure. But, attacking a hospital or other healthcare organization directly is another level of danger since patients are involved. Some hospital shutdowns have gone on for weeks at a time as in the case of the Hollywood Presbyterian Hospital in Los Angeles[27]. The pressure put on hospital staff and administrators during an event such as this is enormous, including loss of revenue, reputation, and potential lawsuits from patients and their families, not to mention potential loss of life as a result of the ransomware attack. "Successful attacks have effectively provided a diagnostic for failed practices and systems, and ransom payments may be viewed as a small price to pay for this diagnosis.

23 Harkins, M. and Freed, A. (2018). The Ransomware Assault on the Healthcare Sector, ***Journal of Law & Cyber Warfare***, Vol. 6, No. 2 (Winter 2018), pp. 148-164.
24 Ibid.
25 Morse, E. and Ramsey, I. (2017). Navigating the Perils of Ransomware, ***The Business Lawyer***, Vol. 72, No. 1 (WINTER 2016-2017), pp. 287-294.
26 Pfeifer, J. (2018). Preparing for Cyber Incidents with Physical Effects, ***The Cyber Defense Review***, Vol. 3, No. 1 (SPRING 2018), pp. 27-34.
27 Woods, B. (2017). Confronting Transatlantic Cybersecurity Challenges in the Internet of Things, ***Atlantic Council***

continued...

When risks to human life and to firm reputations are at stake, future failures are not an option"[28]. Of all the malware and cyber attacks available and in use currently, ransomware is the only known cyber attack to actually claim human lives[29].

Other methods used in ransomware attacks are more about the efficiency and technology associated with the attacks themselves. "Crowti and CrowtiA, which use JavaScript embedded in spam e-mails to encrypt files on a computer and direct the owner to a webpage requesting payment in bitcoin in order to unlock those files"[30]. As ransomware code and systems become more popular and efficient, the frequency of ransomware could rise. The criminals who produce and use ransomware are widespread and very good at what they do and extremely difficult to catch making ransomware attacks all the more dangerous and destructive.

Ransomware Malefactors

Basically anyone can be a ransomware hacker. If one has the money and the will, one needs only purchase a tool like Satan to do one's dirty deeds. However, someone had to create the tool and make it available. Not to mention, they probably learned how to create the tool from others who were ransomware elites, passing the information along, sometimes purposefully, often unwittingly. "[I]n 2016 an executive for the computer security firm Kaspersky Labs revealed that around 75% of the ransomware his firm had examined was written by Russian or Russian-speaking hackers"[31]. In fact, Russia has been a leading producer of malware including Ransomware for some time. Groups like The Shadow Brokers, for instance are known to have Russian ties. The Russian modus operandi flows well with this association as Russia often supports disruptive criminal cyber operations against its adversaries. "High-capability adversaries, such as Russia, showed growing willingness to engage in cyberattacks. Meanwhile, high-intent adversaries, such as cyber-criminal groups and the Islamic State of Iraq and al-Sham (ISIS), have access to increasingly sophisticated toolkits to strengthen their capabilities"[32]. With a mounting list of adversaries with access to ransomware and other malicious attacks, understanding what attacks like ransomware are capable of becomes increasingly important.

28 Morse, E. and Ramsey, I. (2017). Navigating the Perils of Ransomware, ***The Business Lawyer***, Vol. 72, No. 1 (WINTER 2016-2017), pp. 287-294.
29 Eddy, M. and Perlroth, N. (2020). Cyber Attack Suspected in German Woman's Death, New York Times, Accessed 2/16/2021: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html#:~:text=BERLIN%20%E2%80%94%20The%20first%20known%20death%20from%20a,it%20hostage%20until%20the%20victim%20pays%20a%20ransom.
30 Ibid.
31 Eoyang, M., Farkas, E., Freeman, B., and Ashcroft, G. (2017). The Last Straw: Responding to Russia's Anti-Western Aggression, ***Third Way***
32 Woods, B. (2017). Confronting Transatlantic Cybersecurity Challenges in the Internet of Things, ***Atlantic Council***