HACKING HEALTHCARE

Cybercriminals Find Value in Holding Data Hostage As Alternative to Putting it Up For Sale

FLASHPOINT

Introduction

In the wake of several high profile ransomware attacks on hospitals, Flashpoint analysts have observed relevant discussions by cybercriminals surrounding the targeting of hospitals and healthcare networks. Quick to capitalize on such publicity, cybercriminals have begun utilizing the successful attacks as marketing material to advertise ransomware for sale on Deep & Dark Web forums and marketplaces. As cybercriminals evaluate which targets will bring them the highest return, the healthcare industry continues to be perceived as a lucrative source of potential income.

On February 5, 2016, a hacker installed a piece of ransomware on the Hollywood Presbyterian Medical Center (HPMC) network, encrypting the data housed on several computers and effectively knocking them offline. Ransomware is malicious software installed on a computer that encrypts the contents of the computer with a key that only the perpetrator holds. The illicit actor then "ransoms" access to the encrypted data, promising that the data will be decrypted once the victim has paid the actor, usually through online remittance via bitcoin. Once paid, the ransomer provides the victim with the decryption key, restoring access to the files—usually. There are certainly cases of victims paying ransoms with the perpetrators simply taking payment and disappearing, leaving the victim without data and less rich.

Along with grabbing headlines, the attack on the hospital successfully extorted a $17,000 ransom to decrypt the computers' files and restore access to the institution's systems. While it does not appear that any patient data was compromised in the attack, these computers were nonetheless used for hospital operations and administration. Soon after the news of payment, two German hospitals were also hit by ransomware, rendering them unable to access patient data email or critical business operations systems.

Targeting the healthcare industry as a rich source of data is nothing new for cybercriminals. "Fresh" and detailed patient data continues to be sold on underground marketplaces without showing signs of abatement, suggesting intrusions and a persistent presence in many medical facilities and insurers. More concerning, however, is that the news of these successful, high-value ransomware attacks is inspiring at least some cybercriminals to rethink their business models.

Those who profit from selling patient data stolen from medical facilities are realizing that institutions may be willing to pay substantial ransoms worth much more than the value of the data itself on the black market in order to regain control over the functionality of critical systems and data. This reassessment of how to profit the most from the healthcare industry's data could pose a substantial threat to hospitals and healthcare providers.

As these ransomware campaigns and related software become more widespread and accessible to lower level cybercriminals, the healthcare industry must work to understand how these actors are seeking to exploit their systems in order to prepare themselves to mitigate and respond to this new kind of threat.

Honor among Thieves

On February 12, 2016, Fox 11 Los Angeles reported that a piece of malware known as "CryptoLocker" paralyzed Hollywood Presbyterian's computer systems, preventing access to all patient records and forcing the hospital to revert its day-to-day operations to pen and paper. While ransomware campaigns in general are not unique and have been steadily spreading around the globe, the preferred attack vector historically has been predominantly large-scale infections via spam campaigns. In these campaigns, the victim would be demanded to pay a ransom of anywhere between $250 and $500 to decrypt the files. For a ransom demand to be in the tens of thousands of dollars is highly unusual, since the price is set prior to malware deployment and can generally not be altered once installed. In other words, extorting a hospital for such an astronomical sum suggests a purposeful and targeted attack against this specific victim.

Although the unwritten code of conduct amongst Eastern European cyber criminals strictly prohibits any malicious activity directed against citizens of the Commonwealth of Independent States (CIS), the targeting and exploitation of Westerners – and in particular United States citizens – is highly encouraged. Nevertheless, Eastern European cybercriminals reacted coldly to the news of the attack against Hollywood Presbyterian which was regarded as a reckless and unacceptable move. With the exception of a handful of supporters, the general consensus within this segment of the underground was highly negative, condemning the unknown assailants.

One highly reputable member of a Russian cybercrime forum expressed his frustration, writing:

> *From the bottom of my heart I sincerely wish that the mothers of all ransomware distributors end up in the hospital, and that the computer responsible for the resuscitation machine gets infected with it [the malware].*

The actor's post received immediate support from another respected member:

> *Dirt bags, the move is completely unethical. Do not touch hospitals!*

In response to another member concerned that the attack was a precursor to more large-scale operation in the future, a notorious ransomware developer affirmed that similar attacks were likely to occur in the future:

> *I am afraid it is…[They] scored. It means everything was done properly.*

When Opportunity Knocks

While many cybercriminals scorned the ransomware attack on the hospital, others saw opportunity. On the prominent illicit marketplace AlphaBay, members began discussing how the hospital attack might have been perpetrated. One member noted:

> *I'm sure there's many ways this may have got onto their machines. Employees love to open other attachments from other employees, superiors, etc. on work computers. Once a machine is compromised, priv escalate, laterally move and infect all network drives/shares.*
>
> *I believe the easiest way would be to have physical access to a computer on hospital grounds. Heck even finding where the IT department is and see if a hardware keylogger is possible. Depends on what you're comfortable with.*

Others discussed techniques they had used to infiltrate hospital networks successfully, with one user noting:

> *I compromised an entire clinic group recently by pulling RDP credentials out of cleartext while being on the guest wifi. Gained RDP access in off hours, escalated privlidges [sic], hit everything else on the network, got rootkits in their nice expensive printers, and even had to setup a dedicated server just to offload the huge amounts of data I was pulling.*

Infiltrating hospital networks and exploiting their vulnerabilities is only one part of a ransomware scheme. The malicious actor necessarily needs software that can encrypt data and effect a ransom. To this end, some prominent illicit actors have developed ransomware that is being marketed specifically to extort the healthcare industry.

One put up for sale his ransomware product, called "BitcoinBlackmailer," taking advantage of the recent headlines and marketing it as follows:

> *Hacker holds Hollywood Hospital to ransom for $3.6 million in Bitcoin in Ransomware Cyber Attack" What if you was that hacker? I bet he was just a 16 years old kid in the right place at the right time. Just like you are now.*
> *This time I have reinvented the classic ransomware method, I call it BitcoinBlackmailer.*
> *....*
> *Just like in my previous works I hopefully dumbed down every nitty-gritty technical details to a clear, easy-to-follow, comprehensive, step-by-step guide. There is absolutely no risk or further investment needed.*
>
> *Furthermore the only things you need are a computer and the ability to follow clear instructions.*
>
> *If you can do that you will never have to worry about your finances again.*

Despite malicious actors promoting the sale of ransomware targeting hospitals specifically, Flashpoint assesses that cybercriminals are likely using any such tools across a wide spectrum of industries.

Conclusion

Highly publicized ransomware attacks on hospitals and health networks have resulted in large payouts to regain access to operations as well as retrieval of confidential data and critical files. Though our research suggests some cybercriminals have scruples over the targeting of hospitals and medical facilities, it is clear that some members of this illicit community are seeking to capitalize on the publicity surrounding the ransoming of hospitals' data and systems.

While certainly ransomware is applied indiscriminately across industries and individuals, a shift in criminal business tactics recognizing that access to the data can be more valuable than the data itself exposes corporations more broadly to this type of threat. To defend themselves as effectively as possible, companies need to remain aware of the current trends in the cybercriminal community to understand how these actors are likely seeking to profit from their data and invest in appropriate security to stymie such attacks.

About Flashpoint

Flashpoint helps companies and individuals understand the threats looming in the Deep & Dark Web in order to mitigate and prevent both cyber and physical attacks.

We provide data, tools, and expertise to security and intelligence teams across the Fortune 500 and government to both obtain actionable intelligence, as well as gain critical awareness of threatening actors and their relationships, behaviors, and networks prone to malicious activity.

Contact

web: www.flashpoint-intel.com
Email: info@flashpoint-intel.com