Just last week Methodist Hospital in Henderson Kentucky was hit with Ransomware, they are latest in a string of different organization who are being forced to seriously consider paying attackers in hope they will regain control of vital data on their own network. “The attackers are demanding a mere four bitcoins in exchange for a key to unlock the encrypted files; that’s a little more than USD $1,600 at today’s exchange rate.” (Clerix, 2016) This is the modus operando of attacker who use Ransomware, they demand payment that are well within the means of those being attacked.

As a result of this attack the hospital was forced to “placed a scrolling red alert on its homepage this week, stating that “Methodist Hospital is currently working in an Internal

State of Emergency due to a Computer Virus that has limited our use of electronic web based services. We are currently working to resolve this issue, until then we will have limited access to web based services and electronic communications." (Clerix, 2016) As seen in the graphic below. As of the final writing of this paper the banner had been removed which indicates that either the ransom had been paid of the hospital was able restore their systems from unaffected backups.

"Ransomware is a type of malware that prevents or limits users from accessing their system." (Trend Micro, 2015) Ransomware is able to accomplish this by encrypting the data on computer systems usually with a private key that only the attacker knows. The attack usually includes a message that instructs the user to send payment through a minimally traceable means such as Bitcoin, Western Union or PayPal. "While ransomware criminals used to accept prepaid cards and other familiar forms of payment, they're now moving into so-called "cryptocurrency." Some rings only take Bitcoin, the electronic cash that's popular among hedge fund investors and online drug traders." (Shahani, 2015). In most cases once the attacker verified payment they provide instructions as how to unlock the encrypted data or provide encryption key.

The attacks also include a countdown clock which instructs the victim to pay within a certain timeline they data will permanently lock and because the private key used to encrypt the victim's data is destroyed. Some attacks focus on individual computers but others are designed to propagate throughout a network seen high value targets such as servers. Servers are targeted because they usually store large amount of data. Since the gold of Ransomware is to take control of data hostage until payment is made, servers are rich targets. Figure 1

below illustrates the intent of ransomware, essentially they lock some or all devices on a victims network crippling their ability to access data.

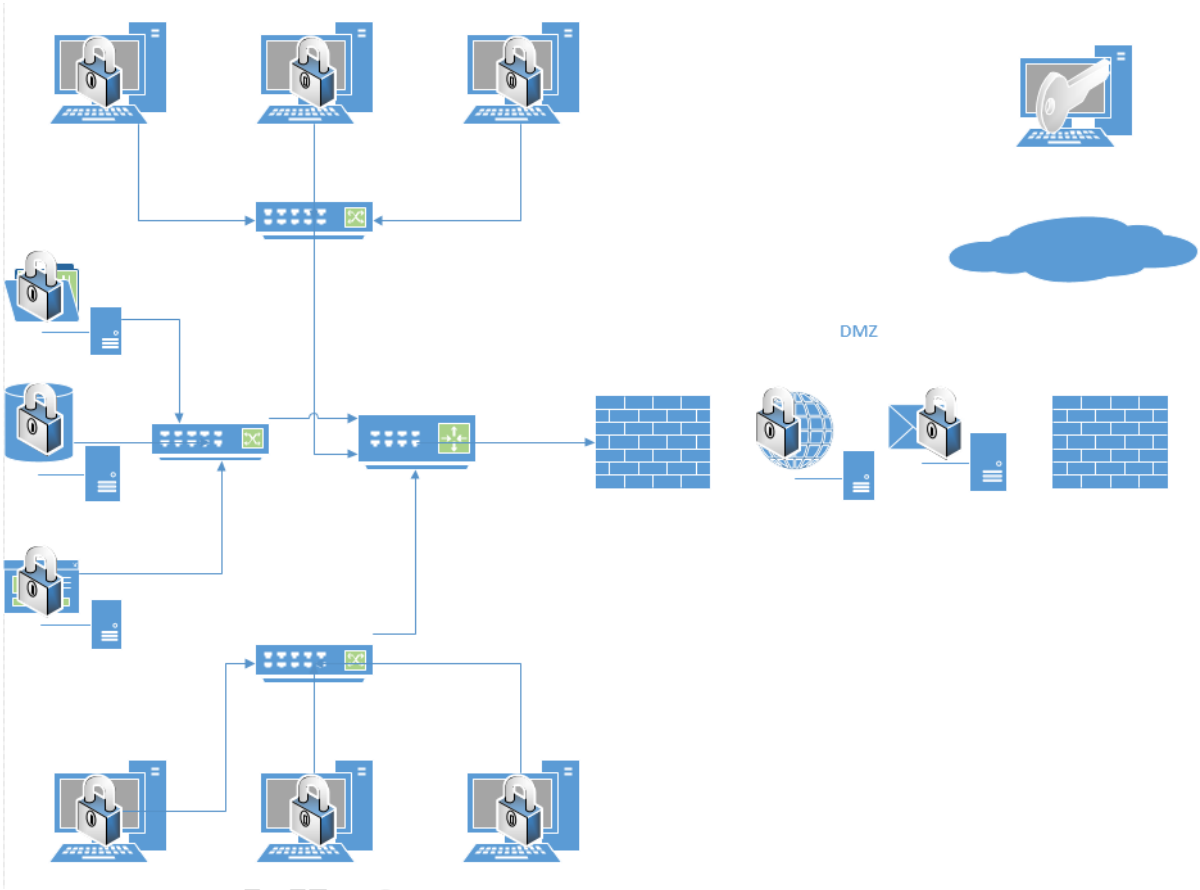

Figure 1

The mechanism for the initial infection of Ransomware varies. "These aggressive assaults begin in a similar manner to scareware." (Boatman, 2015) Some users are tricked with pop ups, others are laced at waterholes such as porn sites or even frequently visited sites. A large majority of computer systems fall victim to Ransomware attacks because users do not properly patch the operating systems or applications with the latest updates. In some cases especially for large companies, attackers may employ a zero day exploit, by attacking a

system vulnerability for which a patch was not yet released. Another area of attack and exploitation is evident in the ever evolving use of TeslaCrypt a version of Ransomware which "once the malicious code is run, the attackers can extract even more data than before from the local machine. The harvested data is then compiled into a unique key, while, at the same time, the ransomware will recruit the affected PC into a central botnet." (Wilson, 2015) TelsaCrypt has represents a leap from simple encrypting the data on a user's systems and storing it locally to actually moving data to systems controlled by the attacker.

Despite the terrible prospect of data being held hostage, there are ways to protect our data and our computers systems from Ransomware. Practice defense in depth, which means, "protecting a computer network with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack." (McGuiness, 2015) Backing up data often and to redundant sites will allow reduce the effect of having to pay ransoms for data. However, in some case such as TeslaCrypt and its variants users may still be subject to information being released on the internet by the attackers. Backing up data to redundant sites will allow administrators to clean up the systems that were attack and return the users to full functionality. Another important means of slowing down attackers is by efficiently updating systems. Most large organizations have a change management process that includes updates to system and testing of patches and updates in a non-production environment prior to deploying changes to the production system. However, the process may not be dynamic enough to keep up with changes in malware and an alternative means to patching might be prudent. One of the best methods of prevention is user education, if users are aware of the dangers it may limit the action ransomware. Quarantining infected system may also help to slow the spread of ransomware.

Bibliography

Boatman, K. (2015, March 2). *Your Security Resource Beware the Rise of Ransomware*. Retrieved from Your Security Resource Norton: http://us.norton.com/yoursecurityresource/detail.jsp?aid=rise_in_ransomware

Clerix, K. (2016, March 16). *Hospital Declares 'Internal State of Emergency' After Ransomware Infection*. Retrieved from KrebsonSecurity : http://krebsonsecurity.com/2016/03/hospital-declares-internet-state-of-emergency-after-ransomware-infection/

McGuiness. (2015, March 20). *Defense In Depth Version 1.2E*. Retrieved from SANS Institute InfoSec Reading Room: https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525

Shahani, A. (2015, February 13). *Ransomware: When Hackers Lock Your Files, To Pay Or Not To Pay?* Retrieved from NPR : http://www.npr.org/sections/alltechconsidered/2014/12/08/366849122/ransomware-when-hackers-lock-your-files-to-pay-or-not-to-pay

Trend Micro. (2015, March 02). *Definition*. Retrieved from Ransome : http://www.trendmicro.com/vinfo/us/security/definition/Ransomware

Wilson, M. (2015, March 19). Retrieved from Betanews: http://betanews.com/2016/03/19/teslacrypt-4-unbreakable-encryption/