OneBeacon
TECHNOLOGY INSURANCE

A Member of OneBeacon Insurance Group®

Minimizing the Impact of Ransomware

Authors: Tushar Nandwana, OneBeacon Technology Risk Control and Joe Budzyn – OneBeacon Insurance Group

Published: July 2018

[1]

Ransomware – A Growing Threat

Ransomware has featured prominently in the news over the last few years. Hospitals, municipalities, businesses, law enforcement agencies, individuals and even entire regions of the world have been affected by it. Some have paid the ransom and recovered their computer data; others have lost their data forever.

- In March 2018, the city of Atlanta, Georgia was hit by SamSam ransomware which prevented city residents from paying their bills and accessing court information online. The demand was for $51,000 but it ultimately cost the city several million dollars from other costs to rectify. SamSam also infected the Colorado Department of Transportation twice in February 2018. Numerous other U.S. municipalities and healthcare organizations have been hit by this ransomware[2].

- WannaCry wreaked havoc on the world in May 2017. With its worm-like, self-propagating behaviour, it spread to thousands of systems within hours using the Eternal Blue exploit to target Windows machines. WannaCry resulted in an estimated $4B in economic losses to the affected businesses and infected 30,000 machines worldwide[3].

- In June 2017 we also saw Petya and NotPetya which used the same exploit as WannaCry, but were more intent on destruction rather than ransom. NotPetya targeted systems specifically in the Ukraine[4]. FedEx ended up reporting a $300M loss, not from the ransom payout but due to the downtime and economic loss sustained by its Ukrainian subsidiary, TNT Express[5]. Petya caused Danish shipping giant AP Moller $300M in lost revenue[6]. Other large global enterprises sustained similar types of economic losses.

- Global economic loss in 2017 was estimated at $5B, up from $325M in 2015[7], and is predicted to be about $11.5B in 2019[8]. Attacks on the healthcare sector are estimated to quadruple by 2020[9]. Average ransomware payouts have decreased to $549 per infected machine in 2017 from $1,071 in 2016[10]. However, since hundreds of machines can be involved, the total ransom payout can range from $2,500 to $50,000 or more.

Understanding Ransomware

Ransomware is malicious software that infects a computer similar to a computer virus. A virus may simply destroy all of the data on the computer or use the computer to send unsolicited email. Ransomware takes the attack further by making the data inaccessible by the owner, then demanding payment before returning the data.

Ransomware has a long history, dating back to 1989[11]. Ransomware has varied in the particular method used to prevent access to files from hiding them, replacing them or encrypting them, to simply lying about the files being unavailable. In early versions of ransomware, flaws in the malicious software sometimes allowed the victim to recover their files without paying the ransom. There are two types of modern ransomware – Crypto and Locker:

- Crypto - File encrypting ransomware that rose to prevalence in 2013 with the rise of CryptoLocker[12]. It was promptly shut down in 2014 but numerous other families of file encrypting ransomware have propagated since then including Goldeneye, Jaff, Erebus and numerous others. Crypto ransomware is the most prevalent.

- Locker - This ransomware family is lock screen ransomware. This version pops up a window or in some other way "locks" the computer or mobile device to prevent its usage. Sometimes the lock message will claim to be from some branch of law enforcement and accuse the user of a crime. Typically the files are not encrypted during this attack. If the lock screen ransomware is removed, the files are typically untouched. Ransomware families includes Ransoc, YeeScrLocker and others.

Ransomware initially started gaining popularity among criminals in Russia. Once it was found to have a lucrative business model, it quickly spread worldwide. Today there are even readymade low-cost ransomware systems that can be purchased for $39[13]. A would-be cyber-criminal doesn't need experience or a large investment to begin infecting computers.

Ransomware is now available as a service (RaaS) to allow criminals with little technical knowledge to attack with ease. These services are available in marketplaces on the dark web and some even include online technical support. A firm called RainMakers Lab has two RaaS products called Philadelphia ($389) and Stampado ($39). Other vendor products include RaasBerry which is a subscription model, and Satan which is a free, commission-based product where the owners take a 30% cut of any ransom the criminal user generates[14].

Ransomware Infiltration

So far in 2018, Ransomware threats were found in 39% of malware-related data breaches – double the level as compared to 2017[15]. Ransomware can arrive via several mechanisms. It can be in a malicious email attachment, attached to a

phishing email, embedded in a malicious website download or even a web link that can automatically download the ransomware when it is clicked.

Currently, email remains the primary distribution channel for ransomware malware.

Ransomware infections have even been linked to legitimate website advertisements that were poisoned in what is known as a "drive-by" infection[16]. Some drive-bys require the user to click on something. However if the computer is missing security patches, simply loading an infected advertisement on a web page can start the infection.

In some cases, attackers will rely on vulnerabilities in the user's system to attack and upload the ransomware malware – for example WannaCry exploiting Windows' SMB while SamSam exploiting a remote desk top vulnerability.

Once the file-encrypting ransomware is active on a computer, it begins the process of rendering data inaccessible. Unknown to the user, the ransomware encrypts their files. If the user tries to open an encrypted file, the computer will indicate that the file is damaged. Once all of the user's files are encrypted, the ransomware typically displays a ransom message prominently.

17

At this point the user is typically given instructions on how to pay the ransom. If the ransom is paid in a timely manner, the criminals say they will provide the user the decryption key necessary to recover their files. The payment is usually some

method that is fairly convenient, yet difficult to trace back to the criminals such as wire transfers, pre-paid payment cards, premium cost SMS services or a digital currency such as Bitcoin.

According to Norton Cybersecurity, globally 34% and in the U.S. 64% of victims pay the ransom[18]. It is important to understand that even if the ransom is paid in the timeframe required, there is no guarantee that the data will be recovered. Some versions of ransomware have flaws that make it impossible to decrypt the data. Others are simply scams where the data is encrypted and the criminals take the money but don't deliver the decryption key. Yet other versions have "customer service" to provide additional means to recover the data. Criminals know if victims don't believe they will recover their data, they will stop paying the ransom.

Paying the ransom to recover files does not prevent reinfection with the same or different ransomware and the cycle repeating. In the end, the transaction is with a criminal and the outcome is unpredictable.

Minimizing ransomware impact:

- Maintain an offline current backup copy of important data. This backup should be disconnected from the computer. Some versions of ransomware can encrypt data stored on network drives or in cloud services when they are connected to the infected computer.
- Apply vendor security patches to the operating system and to applications. Ransomware often takes advantage of software flaws to infect the computer or mobile device.
- Use anti-virus software to detect and prevent infection. Be sure to apply security patches and signature updates to this software as well.
- Use web and email filtering software to reduce exposure to the ransomware in the first place. Be cautious about opening email attachments.
- Train your employees in cybersecurity best practices. Make them aware of phishing attacks and remind them not to click on unknown/potentially malicious attachments and emails.
- Establish a process so employees can communicate and forward suspicious emails, attachments or encounters to appropriate IT staff in your organization for further investigation.

- Encourage ongoing use of strong passwords and two-factor authentication when accessing systems.
- Ensure your disaster recovery plan includes ransomware as a threat condition. The plan should address handling a server infected with ransomware, how best to disconnect servers to limit the spread of malware, how to recover files and resume operations, and how to determine whether paying the ransom is even a viable option. Be suspicious of a computer that has been infected with ransomware. Even if the data is recovered, other malicious software may be present on the computer.
- Even if a computer is infected with ransomware, having current offline backups available means data will not be lost. As a bonus, the backup is also useful if the computer is lost, stolen or breaks.

Contact Us

To learn more about how OneBeacon Technology Insurance can help you manage online and other technology risks, please contact Dan Bauman, VP of Risk Control for OneBeacon Technology Insurance at dbauman@onebeacontech.com or 262.623.6558.

[1]

Reference

[2] Crowe, Jonathan. (March 2018). "City of Atlanta hit with SamSam ransomware: 5 key things to know." Barkly. Accessed June 2018. https://blog.barkly.com/atlanta-ransomware-attack-2018-samsam

[3] Staff Writer. (September 25, 2017). "Total WannaCry losses pegged at $4 billion." Accessed June 2018. https://www.reinsurancene.ws/total-wannacry-losses-pegged-4-billion/

[4] Bing, Chris. (June 28, 2017). "Global ransomware attack was meant to be destructive, not collect money." Cyberscoop. Accessed June 2018. https://www.cyberscoop.com/petya-ransomware-destructive-microsoft-windows-master-boot-record/

[5] Shoorbee, Zaid. (September 20, 2017). "FedEx attributes $300 million loss to NotPetya ransomware attack." Cyberscoop. Accessed June 2018. https://www.cyberscoop.com/fedex-attributes-300-million-loss-notpetya-attack/

[6] O'Brien, Dick. (July 2017). "Internet Security Threat Report Ransomware 2017." Symantec. Accessed June 2018.

https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf, page 18

[7] Morgan, Steve. (May 23, 2017). "Ransomware damages rise 15x in 2 years to hit $5 billion in 2017." Accessed June 2018. https://www.csoonline.com/article/3197582/leadership-management/ransomware-damages-rise-15x-in-2-years-to-hit-5-billion-in-2017.html

[8] Morgan, Steve. (January 23, 2018). "Top 5 cybersecurity facts, figures and statistics for 2018). Accessed June 2018. https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

[9] ibid 7. Accessed June 2018

[10] ibid 5. page 17. Accessed June 2018

[11] Wikipedia "Ransomware" Accessed September 2016 https://en.wikipedia.org/wiki/Ransomware

[12] Ibid 10. Accessed September 2016

[13] Brenner, Bill. (December 13, 2017). "5 ransomware as a service (RaaS) kits – Sophos Labs investigates. " Naked Security by Sophos. Accessed June 2018. https://nakedsecurity.sophos.com/2017/12/13/5-ransomware-as-a-service-raas-kits-sophoslabs-investigates/

[14] ibid 14. Accessed June 2018

[15] Nisco, Aliso De. (April 9, 2018). "Ransomware reigns supreme in 2018, as phishing attacks continue to trick employees." Tech Republic. Accessed June 2018. https://www.techrepublic.com/article/ransomware-reigns-supreme-in-2018-as-phishing-attacks-continue-to-trick-employees/

[16] Goodin, Dan. (March 15, 2016). "Big-name sites hit by rash of ads spreading crypto ransomware." ArsTechnica. Accessed June 2018. http://arstechnica.com/security/2016/03/big-name-sites-hit-by-rash-of-malicious-ads-spreading-crypto-ransomware/

[17] Ransomware – Definition – Trend Micro USA. Accessed June 2018. http://www.trendmicro.com/vinfo/us/security/definition/ransomware#The_Evolution_to_CryptoLocker_and_Crypto-ransomware

[18] Ibid 5. page 18. Accessed June 2018