BERKLEY Re DIRECT
a W. R. Berkley Company

RANSOMWARE:
THE EQUAL OPPORTUNITY CRIMINAL VENTURE

Congratulations 2016! Security experts from around the world have declared you "The year of ransomware and digital extortion!" It is no surprise given the fact that since 2014, according to Kaspersky and other industry publications, incidents of data that are being held for ransom have increased as much as 500% on a year over year basis.[1] Additionally, we have seen incidents occur in every revenue threshold of business from small business to Fortune 500 and every industry from financial services to healthcare, even governmental services. Furthermore, not to raise additional concern, but cyber criminals have adapted their practices to evade law enforcement and security firms meaning this trend doesn't appear to be subsiding anytime soon. With attention surrounding this threat increasing, clients of all sizes will be asking the following questions which we will explore:

1. What is Ransomware?
2. Can this happen to us?
3. What can we do to protect ourselves?

1 WHAT IS RANSOMWARE?

Essentially, Ransomware is a type of malware (virus). It infects computer systems by locking the victim out of their computer network entirely until a ransom is paid. What it typically does is encrypt sensitive data on a computer so the victim may be able to access their system but not the sensitive data. According to Kaspersky and FBI experts, on average it takes less than three minutes from infection time until a victim's data is entirely encrypted.[2] This creates a fast, simple and totally anonymous transaction for the criminal. Payments are often required to be in the form of untraceable currencies such as bitcoin and the perpetrators are in other parts of the world.

2 COULD EXTORTION HAPPEN TO YOU?

UNEQUIVOCALLY THE ANSWER IS YES

Regardless of industry and size of the operation.

Ransomware attacks are unique because the profitability of the assault is derived from inconvenience and fear and not necessarily the financial means of the victim. The loss of the electrician's employee protected health information or the small flower shop's customer records are just as important to them as an entire server is to a large Fortune 500 company. Additionally, according to the ICIT Ransomware Report, demands on average range in the $300–$1,000 range, and the cost of infecting each operation can be as little as $150, still providing criminals with an attractive return on equity regardless of who they are targeting.[3] Furthermore, the pain doesn't end there for most victims. Data restoration and replacement costs can average as much as $10,000 and victims have reported being without access to their network for as long as five days![4]

3 WHAT CAN WE DO TO PROTECT OURSELVES?

Now that there is panic amongst friends, this is the question your clients are asking. The answer, unfortunately, is not an easy one and requires customers to employ a combination of active IT Controls, a conscientious employee and management culture, and prudent risk management vehicles:

→ ***Strong IT Controls:*** Secure IT Controls: This is, of course, the first line of defense. Making sure you have segregation of servers for data, encryption, firewalls, daily virus scans, and a dedicated IT manager (can even be a third party vendor) all reduce the threat of a ransomware attack. However, since the FBI reports as many as 100,000 variants of ransomware are in distribution daily[5], it is nearly impossible to eliminate the threat through active controls.

→ ***Conscientious Employee and Management Culture:*** This is very important! According to the 2016 Net Diligence Cyber Claims Survey, over 50% of compromised data was a result of some sort of employee error (lost laptops, failure to update IT software, employee negligence in internet practices, etc.).[6] This human element can be hard to control, but it is so important. Everyone needs to own network best practices from the owner right down to the part time employee or intern.

→ ***Prudent Risk Management Vehicles:*** This is where insurance comes in. The insurance market is consistently trying to keep up with internal threats facing clients, making critical the latest version of cyber insurance policies that include coverage for extortion and ransomware. While ransomware has been around for over a decade, this latest trend started to appear around 2014, so many policies may NOT include this coverage. Additionally, insurance policies can assist with pre-claim risk management, including incident response plans, business continuity plans, and best practice surveys.

Ransomware is clearly a leading threat to the well-being of business in any industry of any size. It is imperative that all our clients are not only aware of their exposures but that they take steps to reduce their risk as much as possible and consider binding an insurance policy that has up-to-date coverage to handle such claims. This is a trend in cyber security that is consistently evolving and isn't going away anytime soon.

[1] http://usa.kaspersky.com/about-us/press-center/press-releases/2016/Crypto-ransomware_attacks_rise_five-fold_to_hit_over_700000_users_in_one_year

[2] http://usa.kaspersky.com/about-us/press-center/press-releases/2016/Crypto-ransomware_attacks_rise_five-fold_to_hit_over_700000_users_in_one_year

[3] 2016 Ransomware report: http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report2.pdf

[4] MacAfee Report 2016: https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf

[5] Net Diligence 2016 Cyber Claims Study: https://netdiligence.com/portfolio/cyber-claims-study/

[6] Net Diligence 2016 Cyber Claims Study: https://netdiligence.com/portfolio/cyber-claims-study/