KPMG

Ransomware:

To pay or not to pay..... Is it a question?

By **Corey Fotheringham**
Partner, Forensic Technology
KPMG in Canada
416-218-7974
coreyfotheringham@kpmg.ca

Cybercrime is a nasty, sophisticated, and, for many people, a crime of which there is little knowledge. It is also a crime that everyone should be prepared for, both personally and professionally. There are many types of cybercrime and one such digital crime, although rather simple and unsophisticated, can levy a significant financial burden. This new-age, 'hostage-taking' digital crime is known as Ransomware. Ransomware can present itself in several forms such as an account takeover (i.e. personal online bank account, email account such as Yahoo or Gmail, etc.), holding confidential and embarrassing material hostage (i.e. corporate information, photographs, etc.) or it can be the injection of malware (malicious software) that is harmful to a computer system.

Ransomware, as defined by a large antivirus and online security software company, 'is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and force users to pay the ransom demanded through certain online payment methods in exchange for an encryption key, which will allow the system to resume operation.'

A frightening scenario

In order to demonstrate, let's consider the following fictitious scenario. Mr. Smith is a very busy 'mover and shaker' in his company. He can always be found on the phone making deals, out at meetings, and having client lunches; well you get the picture. One day Mr. Smith receives an email that appears to be sent by a client with the subject line: Here is the deal we spoke of for your review. No further details are provided in the body of the email, just an attachment of a Microsoft Word document labeled '2019 Expansion Proposition.docx'. Mr. Smith does not hesitate to click on the document to begin his review. When the file does not open on the first click, he clicks on the document again in another attempt to open it but is once again unsuccessful. What he does not notice is the brief flash of a window opening and closing on his computer – this sort of thing happens all the time. Although a little confused as to why the document wouldn't open, he thinks nothing of it and continues on with his scheduled calls and meetings. He will follow up with the client later.

The next day Mr. Smith wakes up and while sitting, having his morning coffee, he logs onto his computer only to discover that all of his critical business files, deal documents, personal data, etc. cannot be accessed. What he does not realize is the files on his computer have been encrypted as a result of clicking and attempting to open the earlier email attachment that he thought was a business deal. Encryption is usually a legitimate security process that secures data so only authorized parties are able to access it with the proper credentials (password) or encryption keys. However, Ransomware refers to an encryption process used with malicious manner to 'lock' people out of their own data. This is a crisis for Mr. Smith, as his meeting notes along with his presentation for his 2:00 PM board meeting are on his computer. He immediately picks up the phone and calls his IT department. After being on hold for 10 minutes, IT responds to Mr. Smith's call. However, instead of being able to assist him in accessing his data, they inform Mr. Smith that a large portion of the company's data, including Mr. Smith's files, has been encrypted and are inaccessible to them.

As described above, all Mr. Smith did was click on what he thought was a legitimate attachment from an email that appeared to be sent by a client. As a result, not only is Mr. Smith's computer system's data inaccessible, but a vast majority of the company's data has been encrypted. This type of event could just as easily have happened if Mr. Smith visited an unknown website and clicked on an advertisement, downloaded free software (i.e. freeware) to make and edit videos, organize music, or play a simple game.

Mr. Smith's IT department desperately tries to access and repair the data while trying to respond to the numerous employee requests being received as a result of not being able to access their data. They are now aware that the computer screens of the affected systems within Mr. Smith's organization begin to change and are updated with display messages stating the company has fallen victim to a Ransomware attack. The unidentifiable and anonymous parties claiming responsibility for the Ransomware attack are demanding $250,000 CAD in Bitcoin (which is approximately 52 Bitcoin at the time of writing this article). Along with the amount of Bitcoin demanded are instructions on how to transfer the Bitcoin once obtained and assurance the key to unlock the encryption will be provided once payment has been received.

What is Bitcoin? Bitcoin is a digital currency created in 2009 that has a fluctuating value. For example, at the time of writing this article, one Bitcoin is worth $4,768.65 CAD, however, in December 2017 the value was approximately $20,000 CAD. Bitcoin is believed to be untraceable due to the technology involved and hence a preferred method of receiving illegal proceeds from cybercrime such as Ransomware. Ironically, Bitcoin as a method of ransom payment, is now proving to not be quite so attractive a technology as software and forensic specialists are catching up to assist law enforcement in apprehending these 'Cyber Bandits'. Stay tuned for a future article describing advancements in this area.

Critical questions after an attack

The first of many questions that should be considered when responding to a Ransomware attack is where can Bitcoin be purchased? Bitcoin is almost as elusive as the infamous Dilithium crystals that Captain Kirk and Mr. Spock were always desperately searching for in the 1960's TV series Star Trek! Once the Bitcoin has been identified, how is the purchase transaction brokered? At this point, Mr. Smith's company must start to weigh the various options. The following questions should be considered in this event, such as:

1. How important is the data in question?
2. How long can the business operate without the data before profits or reputation are impacted?
3. Are there any backups of the data and if so, are they also encrypted?

Along with the operational questions come some moral and ethical considerations:

1. If I do pay the Bitcoin Ransomware demand, where exactly is the money going? Is it funding organized crime, terrorism, or some other illegal activities?
2. How do I know the attackers will honour the agreement and provide the encryption key upon receiving payment and what stops them from attacking the company again?

To pay or not to pay

So what is the right answer? Unfortunately, there really is no right answer in the above scenario and many like it. Each situation will involve different factors, with relevant weighting for each, in making the appropriate decision to pay or not to pay. From a personal perspective, I am conflicted on what path should be taken given my background in law enforcement and my current role as a Partner in a large business practice. Although the decision 'to pay or not to pay' will be yours and yours alone, there is help available and options to be considered. Cybercrime experts and 'breach coaches' can assist you in narrowing down options that make sense for you.

In addition, as the above scenario illustrates, it is imperative to educate the workforce in the prevention of Ransomware attacks in order to mitigate the risks of future occurrences. Cybercrime experts can tailor a program to fit your needs.

kpmg.ca/rethinkrisk
#rethinkrisk