Legal Issues of
Data Held Hostage

Overview of Ransomware

Robert Underwood

4/10/2016

Abstract

Data held hostage has become a recent technology trend with computers and with these types of attacks in which crooks take a victim's data and hold it for ransom demanding money to release our data back to us, which seems to be clearly a violation in law but how do we prosecute these criminals and what can we do to prevent these types of attack. A similar attack vector used like ransomware restricts a victim's access to their computer functionality by popups and annoying spawning programs in which money is leveraged from the victim to stop the attack.

There is another type of ransomware that is also part of this debate, but in this case raises questions about legality because of the question about ownership. There are some instances an organization who maintains a customer's data, such as a cloud service, will restrict use from the customer for non-payment of services so when this situation occurs is it legal, does an organization have the legal right to restrict a customers access to their data. This paper will explore the legal discussions that peruse this type of ransom situation and what is currently being discussed in recent events.

As in kidnapping the object of the word is kid and the verb of the word is napped, or taken. So the author of this paper defined a word for this paper as a conventional word, in jest, called datanapping, which serves two purposes. The fist purpose is to bring a personal feeling to an impersonal action, restricting access to data seems very impersonal with no real threat involved as where datanapping has both personal and urgency overtones. The second purpose was to be clever about the meaning as to make the reader think about the word and its relation to their data.

Who are these Datanappers

Criminals have found a way through technology to get your money and these so called attackers, referred to as datanappers, take our data hostage and ask for money. Recent attacks on computers using ransomware are on the rise with ransomware where it is used to restrict users from their data and then extort money from their victims as a promise that they will regain access to their data. According to PC world in 2014 there were as many as 600,000 computers infected with a specific type of ransomware called CrytoWall which once activated on a user's computer encrypted their files and restricted the user from accessing their data (Constantin, 2014).

Another type of ransomware attack does not encrypt a user's data but causes their system to become non-functional by using a type of scareware that uses ads to cover portions of your internet browsing in addition to instant popup windows that block your computer screen in which one screen will be an attackers billboard screen giving instructions on who to contact to remove this malware. Another flavor of billboard say they are anti-virus vendors seeking to help you remove the user's current popup dilemma. Although the user's data is not locked up the functionality of their computer is severely diminished by messages that force a user to pay the malware evokers (Veracode, 2012).

According to a major antivirus vendor Norton, ransomware is on the rise and customers need to take precautions to prevent these types of attacks. Also Norton quotes the FBI, that

ransomware has gained in popularity and is earning criminals $150 million a year, and with these numbers there is more motive for datanappers to grab our data (Constantin, 2014).

Norton says that if a user gets attacked there is little hope that the user will get their data back, in addition the FBI is noted as saying that there is very little chance that a victim can get their data back so a victim should just pay the ransom and hope for the best (Roberts, 2015). It would appear that reacting to an incident without being prepared is going to end badly, so how can we prepare ourselves for this type of attack?

Preventing Data Loss

Norton (Constantin, 2014) says there are several actions to which we can take that will help prevent data loss, Norton lists these actions on their website as:

1. Antivirus protection from a reputable vendor. Research which vendors are good, current, and not listed as scam.
2. Firewall. Maintain a firewall by activating it on Microsoft Operating Systems which comes as default software on most new Microsoft Operating Systems (OS). You can also install a reputable software based firewall from a vendor. Or you can purchase a firewall network device and install it on your network.
3. Enable your popup blocker on your browser. Popup buttons are often reprogrammed by criminals so don't click them.
4. Backup your data often. In many cases a computer backup can save the day. Make sure your back up method is solid that you know how to restore your data and what it takes to restore it. In some cases a data backup is only the data and not the OS, so in these cased you need to have your OS disks available to reinstall before you can restore your data.

5. Exercise caution. Don't click on links inside emails. Avoid suspicious websites, avoid responding to urgent email messages that your account has been compromised by clicking on a link.

Take precautions and protect your data but if you should become compromised follow this advice from (Constantin, 2014) of Norton, use another computer to research the problem, and seek professional help from reputable vendors. Disconnect your computer from the internet to prevent further attack and turn the computer off. If you are experiencing a ransomware attack and being asked for money alert the authorities. Ransomware is a serious crime and law enforcement will want to know about it (Constantin, 2014).

More than One at Risk

Recently an entire organization's operations were brought to a standstill as cybercriminals shut down their internal computers. The Presbyterian hospital in Hollywood California was the organization that was held hostage by cybercriminals who shut down their systems. These datanappers demanded $17,000 as a ransom to have the hospital's data released. In this situation people's lives could have been put at risk, although the Presbyterian hospital says there was no risk to patients, the extent of operational interference is not revealed, only the fact that administrational functions were deprecated. When the hospital said deprecated they mean tossed back to the proverbial Stone Age, for everything went to paper and pencil, which brought operations to a substantial slow down. According to hospital authorities the ransom was paid and the services were restored (CBS SF Bay Area News, 2016), which leaves a lingering question, if the operational impact was limited to only administrative operations why did the hospital pay the ransom? In speculation the impact could have involved some important medical

devices that are controlled by the network and limited lifesaving abilities of the hospital or there was a risk similar to that nature that caused the hospital to make payment.

Whatever the reason for payment the datanappers were successful in extorting money for data. Datanapping may not be as successful as datanappers expect due to FBI response. With cybercrime stealing more than 38% more money than bank robbers, according to (Krebs on Security, 2010) the FBI has started making a substantial shift in resources to cybercrime. The FBI has been successful at catching criminals with investigations related to bank robbery with as much as 80% of the bank robbers caught (Center for Problem-Oriented Policing, N.D.). The FBI Cybercrime division site is a great resource for its new initiatives against cybercrime, the site provides training and information for customers (Federal Bureau of Investigation (FBI), N.D.).

Legal Efforts

According to the Cybersecurity Docket, who delivers important news and current developments about cybersecurity to Lawyers, executives and other professionals, states the overwhelming growth of cybercrime puts the onus of defense on the customer. (Stark & Fontaine, 2015) of Cybersecurity Docket say that "companies that experience a cyber-attack should not expect any assistance or even compassion from governmental bodies. In fact, for a variety of reasons, companies need to anticipate and plan for just the opposite:

1) U.S. government agencies are overwhelmed with protecting the nation's own infrastructure and do not have a SWAT team or a rescue team standing-by to assist individual U.S. companies in the defense or response to a cyber-attack;

2) given the forty-seven or so separate state privacy statutory regimes and a growing range of federal agency jurisdiction (each wielding its own unique set of rules, regulations, laws

and enforcement tools), instead of a helping hand, cyber-attack victims should expect subpoenas, enforcement actions and an onslaught of litigation; and 3) the public's view of cyber-attack victims is a skewed one, often defined by anger, vilification and blame-casting, instead of understanding and recognition regarding the extent and nature of this very real threat to all types of companies (Stark & Fontaine, 2015)."

In summary of this section it is apparent that we as individuals and we as businesses need to take the precautionary advice of professionals about securing our systems to the best or our ability that we also need to become better educated about the types of cybercrimes that are occurring and how to defend against them.

Whose Data is it?

Regarding this type of datanapping we discuss a more legally gray area in which we as a customer have our access to data restricted by a vendor to whom we have entrusted with our data. As an example we as individual or we as a business may keep our data on a cloud service such as Foggy Cloud Services. If our fictitious Foggy Cloud Services turns off our data access for some reason do they have the right to do so?

There are several reasons that Foggy Cloud could restrict our access to our data:

a) Foggy Cloud Services goes out of business and closes its doors.
b) Foggy Cloud Services is seized by legal authorities and locks down all data, such as an FBI investigation.
c) Foggy Cloud Services comes under attack of ransomware and all their data is locked up including yours.

d) Foggy Cloud Services makes an accounting error and believes their customer did not pay their monthly fee causing Foggy Cloud Service to restrict the customer's access.
e) Customers do not pay Foggy Cloud Services which causes restricted access.

Each one of these issues have some type of legal and ethical obligation involved with them so how are they defined. Most companies who provide this type of service, cloud services, have a Service Level Agreement (SLA) which spells out the scope of services they deliver. At the website of (Cloud Standards Customer Council, 2015) contain documents that outlines services that need to be defined in the SLA such as; Data Preservation and Redundancy which includes backups, restores, and integrity checks; Data Location, where the data is stored in relation to other customers data; Data Privacy, who can see your data; Data Availability, events that can cause interruption in service and how long those events are expected to last such as maintenance; Data Seizure, when law enforcement may seize your data, when a provider goes out of business, billing disputes, or security issues such as ransomware events at the provider (Cloud Standards Customer Council, 2015).

In most of these cases it is clear that the data restriction was due to an issue that would be consider unforeseen and unavoidable and their resolves would involve no loss of data but what about those issues that are caused by billing disputes, can we ever get our data back. Even if the SLA says that the provider can restrict access for billing disputes is this a legal position, can a provider take your data even if they spell it out in a contract. Situation, what if a hospital said, sorry, you cannot pay the bill we are keeping your child until you pay what is owed, now that seems as an extreme example because your data is not a child or a person but your business could be built on or dependent on data access. The success of a business may depend on the access to data, so what about then, would it be legal to shut down a business?

According to the American Bar Association (ABA) article posted by (Nelson & Simek, N.D.) most Lawyers do not know who the data belongs to. For a Lawyer the need to know ownership is very important because lawyers are required to keep their clients' information confidential and with the professional rules about technology for Lawyers, all Lawyers are required to be competent with their technology (Nelson & Simek, N.D.). So how is it possible for legal representatives such as Lawyers, who cannot define who owns the data, to legally support a customer once they agree to put their data in the cloud?

Cloud Caution

Cautions to know about the cloud are those risks that we need to consider before we place our data on the cloud. Before we continue we need to consider data as opposed to dataset, the fact that all data is not the same that some data is important and some data is not. An organization usually has both types of data which industry defines as datasets. In our analysis of our datasets we first we need to ask what we can lose if the cloud restricts access to our dataset and if the answer is, yes we can lose it, then we need not worry about the dataset. If no, we cannot lose it, is the answer about the dataset in question, let's say a Lawyers confidential files, then we need to make sure we can positively restrict access to that data, if there is any question about the cloud keeping our dataset safe then the cloud would be a bad choice for storage. If you need absolute access to your dataset at all times then if your cloud service cannot guaranty access, then cloud service would be a bad choice. If there is no exit strategy for blowing the cloud away for another type of service then the cloud service would be a bad choice. If your datalink to the cloud service provider does not require encryption then your data transfers could be intercepted and data taken, this cloud vendor is probably a very bad choice. If the market

analysis reveals financial instability or very poor market performance then the vendor may be a poor choice. (Nelson & Simek, N.D.).

A note about exit strategy for cloud service, the format that a cloud service stores you data may be encoded by an optimizing program so that all the data received by the cloud service is condensed into smaller files. If you decide to leave a cloud service the provider may give you your data back in the encoded form to which you might not be able to decode in (Nelson & Simek, N.D.).

Meeting all the requirements stated above may be difficult to achieve but with a little investigation and a little effort most people and business can find a cloud service that meets their needs and requirement. The most important part of this effort is understanding the roles and rules that your datasets will fall under so you can identify the correct service. In those circumstances where you cannot find what you need then you will need to hire a professional service that provides the type of IT analysis for dataset protection to make the best recommendations available.

For those risks that you do not want to take by using a cloud service then the risks can be mitigated through some careful planning, this type of planning is called business continuity planning. With this type of plan you can develop cost effective techniques at your site or in concert with cloud services that protects your data and provides the mitigation techniques needed to ensure the risk has been limited to your comfort level. The business continuity plan involves business impact analysis, recovery strategies, plan development, test, and exercises which provides the necessary feedback about the success of the plan.

Conclusion

Not all datanappers are the same as we have seen some are just plain criminals who lock up our data and demand payment for release of your data (Constantin, 2014) which also showed the cost to industry with 600,000 computers affected. We looked at another type of ransomware restricted the functionality of our computer and demanded payment for the return of fuctionality (Veracode, 2012). As to the impact of datanappping we observed that it can also people's lives in harm's way as we examined the hospital datanapping caper (CBS SF Bay Area News, 2016). We examined the efforts of law enforcement and how efforts have increased and continue to increase in this realm but is over taxing the system and causing industry to implement their own protection mechanisms (Stark & Fontaine, 2015).

We took a look at the gray area around vendors who provide data storage services and how these cloud service like our fictional Foggy Cloud Service could restrict access to our data. In this context we examined the legal confusion with who owns the data legally where many Lawyers were quoted as not knowing who the data belong to as stated by the ABA's (Nelson & Simek, N.D.) which compounds the issues around selecting cloud service.

Finally we examined cloud services and the risks associated with them and possible solutions that can educate the customer and reduce the risks associated with cloud service providers.

References

Center for Problem-Oriented Policing. (N.D.). *Factors Contributing to Bank Robbery*. Retrieved from Center for Problem-Oriented Policing: http://www.popcenter.org/problems/robbery_banks/2

Cloud Standards Customer Council. (2015, April). *Practical Guild to Cloud Service Agreements Version 2.0*. Retrieved from Cloud Standards Customer Council: http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Cloud-Service-Agreements.pdf

Constantin, L. (2024, August 29th). *CryptoWall ransomware held over 600K computers hostage, encrypted 5 billion files*. Retrieved from PC world: http://www.pcworld.com/article/2600543/cryptowall-held-over-halfamillion-computers-hostage-encrypted-5-billion-files.html

Federal Bureau of Investigation (FBI). (N.D.). *Cyber Crime*. Retrieved from Federal Bureau of Investigation (FBI): https://www.fbi.gov/about-us/investigate/cyber

Krebs on Security. (2010, March 10th). *Cyber Crooks Leave Traditional Bank Robbers in the Dust*. Retrieved from KrebsonSecurity: http://krebsonsecurity.com/2010/03/cyber-crooks-leave-bank-robbers-in-the-dust/

Nelson, S. D., & Simek, J. W. (N.D.). *How to Select a Law Firm Cloud Provider Volume 40 Number 2*. Retrieved from American Bar Association: http://www.americanbar.org/publications/law_practice_magazine/2014/march-april/hot-buttons.html

Roberts, P. F. (2015, October 22nd). *FBI's Advice on Ransomware? Just Pay The Ransom*. Retrieved from They Security Ledger: https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/

Stark, J. R., & Fontaine, D. R. (2015, April 9th). *Cyber Insurance: A Pragmatic Approach to a Growing Necessity*. Retrieved from Cybersecurity Docket: http://www.cybersecuritydocket.com/2015/04/09/cyber-insurance-a-pragmatic-approach-to-a-growing-necessity/

Veracode. (2012, October 12th). *Common Malware Types: Cybersecurity 101*. Retrieved from Veracode: https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101