1-1-2017

Ransomware: Evolution, Mitigation and Prevention

Ronny Richardson
Kennesaw State University

Max M. North
Kennesaw State University

Ransomware: Evolution, Mitigation and Prevention

Ronny Richardson and Max North
Management & Entrepreneurship Department
Information Systems Department
Coles College of Business
Kennesaw State University, GA USA

[Abstract] Ransomware is a rapidly growing threat to the data files of individuals and businesses. It encrypts files on an infected computer and holds the key to decrypt the files until the victim pays a ransom. This malware is responsible for hundreds of millions of dollars of losses annually. Due to the large amounts of money to be made, new versions appear frequently. This allows bypassing antivirus software and other intrusion detection methods. In this paper, we present a brief history of ransomware, the arguments for and against paying the ransom, best practices to prevent an infection, and to recover from an infection should one happen.

[Keywords] Crypto, Locker, Malware, Ransomware

Overview of Ransomware

Ransomware is malware that locks your computer or prevents you from accessing your data using private key encryption until you pay a ransom. That ransom is usually paid in Bitcoin. Data based extortion has been around since about 2005 but the development of ransom encryption software and Bitcoins have greatly facilitated the scheme (Zetter, 2015).

While ransomware attacks on personal computers are the stories that generally make the news, ransomware have also been developed to attack mobile phones by changing the PIN number of the device and then requiring a ransom to obtain the new PIN (Zetter, 2015). Ransomware is big business. The computer security firm Symantec conservatively estimates that ransomware extorts hundreds of millions from victims each year. Symantec also notes that paying the ransom is no guarantee that the decryption key will be provided and, in many cases, it is not (Zetter, 2015).

Ransomware can be divided into two basic types. The most common is crypto ransomware, which encrypts files and data. The second type is locker ransomware. This version locks the computer or other device, preventing the victims from using it (Savage, Coogan, & Lau, 2015). Locker ransomware only locks the device; the data stored on the device is typically untouched. As a result, if the malware is removed, the data is untouched. Even if the malware cannot be easily removed, the data can often be recovered by moving the storage device, typically a hard drive, to another functioning computer. This makes locker ransomware much less effective in extorting ransom payments (Savage, Coogan, & Lau, 2015).

Crypto ransomware, on the other hand, encrypts the data, so even if the malware is removed from the device or the storage media is moved to another device, the data is not accessible. Typically, crypto ransomware does not target critical system files, enabling the device to continue to function in spite of being infected—after all, the device could be needed to pay the ransom (Savage, Coogan, & Lau, 2015).

In late 90's and up until 2005, online payment methods were not so readily available. Victims were instructed to pay ransoms via SMS text messages or by mailing pre-paid cards. Another common payment method was having the victim call a premium rate telephone number that earned money for the attacker (Zetter, 2015).

All of these payment methods were risky, since a determined investigator could trace them back to the attacker. Ransomware really took off when in 2008 Bitcoin came into use. Bitcoin is electronic currency that is much harder to trace and thus helped anonymize the transactions. That made it difficult or even impossible to track the attacker by following the payment (Rosenberg, 2015). While Bitcoins have the advantage of being difficult to impossible to trace, they do have risks. The two major risks are massive exchange rate swings and hacking of major Bitcoin exchanges (Savage, 2015).

In general, crypto ransomware prefers Bitcoin, while locker ransomware prefers payment voucher systems. That makes sense: the infected computer remains fully functional after a crypto ransomware infection, so the user is free to use the computer to purchase Bitcoins. With locker ransomware, the computer is locked and, therefore, unusable, making the purchase of Bitcoins more difficult. It is therefore easier for the victim to buy payment vouchers locally and enter a payment code (Savage, 2015).

Ultimately, the criminals need to convert the ransomware they receive into cash they can spend. The methods used to laundry the ransom depend on the type of ransomware. Locking ransomware, which tend to use payment voucher systems, use online betting services in a variety of legal jurisdictions that accept the voucher codes as payment. The money is then transferred to prepaid debit cards and "money mules" are used to withdraw cash (Savage, Coogan, & Lau, 2015). Payments in Bitcoin can be used directly due to the privacy of cryptocurrency. However, many criminals are worried about law enforcement. As a result, a number of Bitcoin-laundering services have become available for criminals to use. There are also Bitcoin anonymizers that criminals can use (Savage, Coogan, & Lau, 2015).

Evolution of Ransomware

The following timeline was created with approximate dates based on what is known about the ransomware. Due to the illegality of ransomware, the authors fully expect that details are missing. Nevertheless, it does show the general evolution and growth of ransomware over time. It is also important to note that sources are not consistent in the names used for the various versions of ransomware, though they do tend to be similar.

1989. The first ransomware virus, called the AIDS Trojan (and also known as the PC Cyborg), was created by Joseph L. Popp. Popp was a Harvard-trained evolutionary biologist. It was distributed by floppy disk at the World Health Organization's International Aids conference. It used simple symmetric cryptography to encrypt file names and tools were soon available to decrypt them (Sjouwerman, 2015b).

2005. The first modern ransomware was Trojan.Gpcoder, also known as GP Code and GPCoder. It was released in May 2005 and initially used a custom symmetric encryption technique that was weak and easily overcome. Its authors continued to improve the malware (Savage, Coogan, & Lau, 2015). Trojan.Gpcoder was spread via a spam email attachment claiming to be a job application (Sjouwerman, 2015b).

The bulk of the early ransomware was developed in Russia by Russian organized criminals. It was mostly aimed at Russian victims and those in neighboring countries, like Belarus, Ukraine, and Kazakhstan (Cawley, 2016).

2006. In early 2006, ransomware was starting to gain traction, and more attackers started to try their hand. Trojan.Cryzip appeared in March 2006. It copied data files to password-protected archive files and deleted the originals. The code for the malware included the password, so recovering it was straightforward.

Trojan.Archiveus also came on the scene in 2006. It operated much like Trojan.Cryzip, except instead of asking for a ransom, it required victims to buy medication from specific online pharmacies and submit the order ID to get the password (Savage, Coogan, & Lau, 2015).

2007. Locker ransomware began to appear. Early versions struck Russia and displayed a pornographic image on the machine and demanded payment to remove it, either by SMS text message or calling a premium-rate phone number. Attacks soon spread to Europe and the US (Zetter, 2015).

2008. A variant of Trojan.Gpcoder called GPcode.AK first appeared. It used a 1024-bit RSA key. It left a text file with instructions in each subdirectory where it encrypted files. It asked for payment of $100 to $200 in e-gold or Liberty Reserve (Tromer, 2008).

2011. Mid 2011 saw the first large-scale outbreak of ransomware, mainly due to emerging anonymous payment services. There were about 30,000 new ransomware samples in quarter one and another 30,000 in quarter two. By quarter three, there were 60,000 new samples (Sjouwerman, 2015b).

2012. A toolkit called Citadel was released at a cost of about $3,000. Citadel made it simple to produce and distribute ransomware (Segura, 2016). Another toolkit, called Lyposit, also came out in 2012. It was designed to produce ransomware that pretends to come from law enforcement with the exact agency depending on the computer's regional settings ("Lyposit Malware | win32/Lyposit.A," n.d.). One version

created with Lyposit was known as Reveton. It displayed a pop-up message saying the machine had been involved in child porn activity, downloading copyrighted material, or some other criminal activity, and had been locked by the FBI or Justice Department (Sjouwerman, 2015b; Savage, 2015). Another early ransomware was Trojan.Randsom.C. It spoofed a Windows Security Center message and asked the user to call a premium-rate phone number to reactivate their Windows license (Savage, Coogan, & Lau, 2015).

Deficiencies in locker ransomware, as well as other extortion schemes not discussed here, lead to a pivot back to crypto ransomware in 2013. A typical attack requests payment of around $300, and the attacks became much more capable (Savage, Coogan, & Lau, 2015).

2013. The most famous piece of ransomware, CyptoLocker, was released in August 2013 by a hacker named Slavik. It used public and private cryptographic keys to encrypt, and later decrypt, a victim's files. It was originally distributed via the Gameover ZeuS banking Trojan botnet. Later, it was distributed via an email that appeared to come from UPS or FedEx (Zetter, 2015). The original version of CryptoLocker encrypted about 67 different file types, including all Microsoft Office data files (Cannell, 2016).

CyptoLocker gave victims three days to pay. Prices were around two Bitcoins, or $100 at that time. Other payment methods included CashU, Ukash, Paysafecard, and MoneyPak. With some versions, if the three-day deadline was not met, victims could pay a much higher ransom to retrieve their files. The amount varied with the version (Sjouwerman, 2015b).

In November, the value of the two Bitcoin ransom increased to about $460. Missing the original deadline raised the price to ten Bitcoins. By December, 250,000 machines were infected. It was found that 41,928 Bitcoins of ransom had been paid (Sjouwerman, 2015b). In December, a copycat called Locker emerged. Its ransom was $150, with payment by Perfect Money or QIWI Visa Virtual Card number. Later in December, CryptoLocker 2.0 was released. It was written in a different language than CryptoLocker and so likely was released by different attackers (Sjouwerman, 2015b). During 2013, Symantec estimates that the number of attacks grew from 100,000 in January to 600,000 in December. They also estimated that three percent of infected users paid the ransom (Rosenberg, 2015).

2014. From September 2013 to May 2014, it is estimated that more than 500,000 victims were infected with CryptoLocker. An estimated 1.3 percent of victims paid the ransom (Cannell, 2016). In June, Operation Tovar, a coalition of law enforcement agencies, security vendors, and academics, took down the CryptoLocker distribution servers. Two vendors, FireEye and Fox-IT, found the database of decryption keys for all the CryptoLocker victims and released a service that allowed for free decryption by all victims (Cawley, 2016). In February, CryptoDefense was released. It was a fairly weak piece of ransomware, but still earned $34,000 in its first month. An improved version called CryptoWall was released in April. It used Java vulnerability and was delivered via malicious advertising. This version generated more than $1,000,000 in ransom (Sjouwerman, 2015b).

2015. By the end of 2015, the FBI estimated that victims had paid $27 million in ransoms to the attackers behind CryptoLocker (Cannell, 2016). CryptoWall passed Cryptolocker as the leading version of ransomware (Sjouwerman, 2015b).

A study by Kaspersky found that for 2014-2015, ransomware attacks increased by 17.7 percent but crypto ransomware attacks increased by 448 percent (Townsend, 2016). In May, ransomware-as-a-service arrived. Using a TOR website, attackers could create ransomware for free. The site handles payment and takes a 20 percent cut of the ransom (Sjouwerman, 2015b). In September, LockerPin was released. It infects Android systems and changes the PIN. It charges a $500 ransom. In October, a new report from the Cyber Threat Alliance reported total ransomware damage at $325,000,000 (Sjouwerman, 2015b). In November, Linus.Encoder.1 was discovered by Dr.Web, a Russian computer security firm. As the name implies, it targets Linux systems. It encrypts both data files and files associated with web applications (Cawley, 2016). In November, the fourth iteration of Cryptowall surfaced. It includes a modified protocol to help avoid detection. Additionally, it alters the file names when it encrypts files, making it harder to determine what files were actually encrypted (Pauli, 2015).

2016. In January, a JavaScript-only ransomware-as-a-service was discovered. Using JavaScript allows for a multi-platform attack, including Linus and MacOS X. In February, ransomware infected thousands of WordPress sites. WordPress is a popular blogging platform. In April, a ransomware called Petya came out.

Petya makes the whole hard disk inaccessible until the ransom is paid (Fitzpatrick & Griffin, 2016). It does this by overwriting the master boot record (MBR) of the infected computer. Without the MBR, the operating system cannot reconstruct the unencrypted files (Constantin, 2016). Apple had to release an update to block the KeRanger ransomware. KeRanger is believed to be the first ransomware attack targeting Apple computers. Once installed, KeRanger takes three days to activate and is designed to encrypt more than 300 file types (Kirk, 2016a).

In February, malware called Xbot was found to be targeting Android devices in Australia and Russia. Not only does it encrypt files, it also tries to steal online banking details (Kirk, 2016b). In July, the Locky ransomware added a failsafe mechanism that begins encrypting files even if the ransomware cannot request a unique encryption key from the criminals' servers due to the target computer either being offline or blocking the communications (Constantin, 2016c).

The FBI estimates that ransomware generated $209,000,000 in the first three months of 2016 and is on track to be a one-billion-dollar crime this year (Fitzpatrick & Griffin, 2016). During the first quarter, McAfee Labs measured 1.2 million ransomware attacks. This was a 24-percent increase over the fourth quarter of 2015 (McAfee Labs Threats Report, 2016). The three top versions currently in the wild are CryptoWall, CTB-Locker, and TorrentLocker. CryptoWall is an improved version of CryptoDefense. It not only encrypts files on the infected computer, but also targets any external storage or shared drives connected to the target. CTB-Locker is short for curve-Tor-Bitcoin. Both CryptoWall and CTB-Locker have affiliate sales programs. TorrentLocker harvests email addresses when it infects a computer in order to spam other users (Zetter 2015).

More Than Software is Required

Having ransomware software infect a machine is not enough. The ransomware must communicate with a server to get an encryption key and report its results. This requires a server hosted by a company that will ignore the illegal activity and guarantee the attackers anonymity. These hosting companies are called Bulletproof Hosting. Most are located in China or Russia. Attackers also use a proxy or VPN services to further disguise their own IP addresses (Segura, 2016).

Today, ransomware is a worldwide problem. Since different parts of the world have different abilities to pay, ransomware like CryptoWall uses dynamic geographical pricing. When a computer is infected, CryptoWall checks with its command-and-control (C&C) server. It reports the IP address of the infected computer. The C&C server checks a database and returns a price for the country associated with that IP address (Savage, 2015).

Likewise, some criminals target businesses rather than individual users. Criminals know they can charge businesses a much higher ransom than individuals. While businesses rarely report infections and the ransom paid, there is some antidotal evidence. In 2012, several Australian businesses reported paying ransoms of up to AU$5,000 (US$4,750) and in 2015, a US online financial database received a demand of $50,000 (Savage, 2015). According to Liam O'Murchu, a security executive at antivirus software maker Symantec Corporation, the business attacks are focused on small businesses. Larger firms have more comprehensive backups, networks that are compartmentalized by departments and knowledgeable technical support personnel (Rosenberg, 2016).

Researchers believe that criminals have found that about $10,000 is the optimal ransom for a business. It is low enough that businesses are willing to pay it and also low enough that law enforcement is reluctant to want to investigate it (Savage, 2015). For consumers, there is some good news. According to cybersecurity journalist Bob Sullivan, the ransoms seem to be dropping, with $300 being the more recent average price in the US. The criminals seem to be learning that lower ransoms make it much more likely that victims will pay (Wiles, 2016).

To Pay or not to Pay, That is the Question

Individuals and businesses face the decision whether to pay when they lack adequate backups to recover from the ransomware. As such, the decision boils down to two related questions. First, is the data worth

more than the ransom? And, if so, what is the level of confidence that the criminal will decrypt the data if the ransom is paid. Additionally, there is always the concern that paying the ransom will encourage the criminals. Given the statistic quoted above that the FBI believes ransomware will become a billion-dollar business in 2016, victims are clearly deciding to pay the ransom and take their chances.

Ransomware criminals seem to have enough business sense to realize that if word gets around that they do not deliver the decryption code once the ransom is paid; their business model will fail and victims will stop paying. Some ransomware schemes try to build trust by decrypting a few files before the ransom is paid. For example, Trojan.Cryptolocker.G has the option to decrypt five randomly chosen files for free. In other cases, business victims have been able to negotiate for a lower fee (Savage, Coogan, & Lau, 2015).

Nevertheless, in 2016, Kansas Heart Hospital paid the ransom when they were infected with an undisclosed ransomware. Rather than decrypting the files, the criminals demanded a second ransom, which the hospital refused to pay (Lemos, 2016). Trust is hard to build and easy to lose. It will not take many reports like this to strongly discourage businesses from paying the ransom if they are infected. In 2016, an Arkansas sheriff's office paid $2,400 to recover their files (Press, 2016). Sometimes, it makes sense to negotiate before paying. In 2016, Hollywood Presbyterian Medical Center was hit with ransomware that shut down their computers for more than a week. Rather than pay the initial $3.7 million ransom, the hospital went back to paper records until they were able to negotiate the payment down to 40 bitcoins or about $17,000 (Wolff, 2016).

Paying a ransom to get needed files back can make economic sense. Nevertheless, experts give four reasons not the pay the ransom. First, you become a bigger target. Criminals talk and tell each other who paid and who did not. Second, as discussed above, you cannot trust criminals to decrypt your data. CryptoWall has a reputation for excellent "customer service." Other malware families do not. Third, your next ransom will be higher. Perhaps the criminals demand a second ransom before decrypting your data or perhaps you are infected a second time. Either way, you will pay more. Fourth, your payment encourages the criminals to continue doing what they are doing (Rashid, 2016).

Data on Infection

According to Osterman Research, Inc., from June 2015 to June 2016, 59 percent of ransomware infections came via email, either as a link or an attachment. Another 24 percent came via a website or web application. Another eight percent came by social media, USB stick, or business application, and nine percent were of unknown origin. Once infected, only three percent of US companies pay the ransom, while 75 percent of Canadian companies pay (State of Ransomware, 2016). Symantec uses telemetry data to track ransomware infections by country. The rankings are shown in the table 1 below. For the most part, criminals are targeting large or affluent countries (Savage, Coogan, & Lau, 2015).

Table 1

Top 12 Countries Impacted by Ransomware

Rank	Country
1	USA
2	Japan
3	UK
4	Italy
5	Germany
6	Russia
7	Canada
8	Australia
9	India
10	Netherlands
11	Brazil
12	Turkey

Over the past 12 months, 64 percent of ransomware attacks have been crypto ransomware, while 36 percent has been locker ransomware. This is in line with the past several years (Savage, Coogan, & Lau, 2015).

Emerging Trends in Ransomware

Law enforcement and computer security vendors, like Symantec, are starting to pay attention to ransomware. This has forced the criminals to change the way they operate. More are using Tor and the Invisible Internet Project (I2P) to hide their tracks. Likewise, more are turning to cryptocurrencies like Bitcoin to hide the money trail. As the pressure on ransomware increases, the criminals will likely look for more ways to block and obfuscate attempts to track and understand their activities (Savage, Coogan, & Lau, 2015).

At first, ransomware was mainly a problem for the Windows platform. However, as discussed earlier, it has begun to move to Apple and Android systems. That trend is likely to continue. Researchers have written ransomware that can attack a smart thermostat (Fitzpatrick & Griffin, 2016). Already, locker ransomware that attacks smart watches has been seen in the wild. As the world moves to the Internet of Things (IoT), there is no doubt that ransomware will move to the IoT as well. While that might seem farfetched at first, researchers have already been able to take over the computer systems of a moving Jeep Cherokee. If researchers can do it, so can ransomware (Savage, Coogan, & Lau, 2015). At that point, the cost may not be money but your life.

The big money is to be made attacking businesses, and so far, crypto ransomware is a low-risk, high-yield endeavor with little to no fear of law enforcement prosecuting criminals in the rare event the infection is reported—and most infections go unreported. Companies do not report because they do not want to make things worse or become targets for other criminals (Gallagher, 2016).

From June 2015 to June 2016, according to a survey by Osterman Research, Inc., 79 percent of business organizations in the US suffered at least one ransomware attack and 22 percent suffered more than twenty. In these attacks, 78 percent reported that people were impacted, 12 percent reported the business stopped immediately, 11 percent reported that employees had to use personal equipment while corporate systems were down, and six percent lost revenue as a result. The top four industries attacked were healthcare, financial services, manufacturing, and governmental (State of Ransomware, 2016).

Currently, most ransomware quickly announces that it has encrypted data files in order to quickly collect the ransom. Some ransomware is moving to delayed announcements, all the while encrypting files in the background. That allows the encrypted files to quietly overwrite good files in backups, making it harder to recover from the ransomware using backups (Pauli, 2015). It is also becoming more common for ransomware to threaten to release files publically unless the ransom is paid. According to FireEye, one company paid over one million dollars to prevent sensitive data from being released. This has real potential for both cost and embarrassment. Consider a company that has emails from its general council compromised as part of a ransomware attack (Kirk, 2016c).

Criminals are also looking for alternative attack vectors. In late 2016, they begin using SVG (scalable vector graphics) files on social media as an attack method. SVG files allow computer code, such as JavaScript, to be embedded in the graphic. That code can be opened and executed via a browser (Rosenquist, 2016). In late 2016, the Locky malware was being prorogated via a Word macro (Gallagher, 2016c). One version of Popcorn Time allowed users to decrypt their files for free if they infected two other people with the ransomware (Abrams, 2016).

Ransomware are trending to become both localized and targeted at businesses, which can afford to pay the ransom and where the files are more critical. Researchers have found that most ransomware links are clicked on between 9am and 1pm: typical work hours. The criminals are adding detection evasion techniques, including CAPTCHA tests and versions that self-destruct (Constantin, 2015). Certainly, it seems likely that countries and other threat actors are looking at ransomware as a potential weapon. This was seen publicly when the North Koreans attacked Sony Pictures.

Preventing Ransomware

Experts have four recommendations for individuals and businesses trying to prevent a ransomware infection

and for dealing with the infection if it happens:

Step 1: Back Up. If the data is backed up, there is no need to pay a ransom to get the data back. Instead, it can be recovered from the backups (Zetter, 2016). Of course, the backups need to be current. Some ransomware attempts to encrypt locally connected backup systems, so either uses a cloud backup or a system that is only connected while the backup is being made. It is also important to keep multiple backups. As discussed above, ransomware is starting to delay announcing itself. It encrypts files in the background, and those encrypted files are then placed in the current backup, preventing that backup from being used to restore unencrypted files.

Step 2: Avoid Email Links and Attachments. Phishing attacks are the most common way to spread ransomware, so avoiding clicking on links or opening attachments in spam email will go a long way to avoiding ransomware. However, criminals have also started using compromised advertising (malvertising) to spread ransomware. These can target trusted websites. Ad blockers can protect against malvertising (Zetter, 2016). Turning off Java and JavaScript can also help. Business should train employees to avoid suspicious email, and corporate IT should consider standardizing ad blocking software.

According to a report by PhishMe, in March 2016, 93 percent of all phishing emails contained crypto ransomware. That is up from 56 percent in December 2015. PhishMe also estimates that 6.3 million phishing emails were sent in the first quarter of 2016 (Korolov, 2016). In addition to standard phishing, PhishMe is seeing an increase in targeted phishing emails. For example, the phishing email might contain what it claims to be a resume. Most recipients would either ignore it or forward it to HR, while an HR recipient might open it without thinking about it. Other categories are billing-, shipping-, and invoice-related phishing emails (Korolov, 2016).

Individual users can avoid most malicious email attachments by forwarding their email through Gmail, which does an excellent job of blocking suspect attachments. Corporate users can use application whitelisting, but that is not currently available for individual users (Bradley, 2015).

Step 3: Patch and Block. The operating system, browsers, and security software should always be kept patched and up-to-date. Likewise, third-party plug-ins, like Java and Flash, need to be kept patched if they are allowed at all. Business systems can also rely on whitelisting and limiting user rights to reduce the chance of a ransomware infection (Zetter, 2016). Of course, these steps will help reduce other types of malware infections as well. Unfortunately, ransomware is constantly evolving to stay ahead of antivirus software, so software alone cannot be depended on to block an attack (Rosenberg, 2015).

Step 4: Drop-and-Roll. At the first sign of an infection, the infected machine should be immediately turned off (or unplugged) to minimize the damage to files. If it is connected to a network, administrators should immediately shut down the network to minimize the propagation of the ransomware (Zetter, 2016). More on dealing with an infection is discussed below. The above applies to both individuals and organizations. For organizations, experts recommend the following best practices:

Understand the Risks. As this paper makes clear, ransomware is a very real danger to both data and the ability of the organization to continue operations and that danger is growing at an accelerating rate. Organizations cannot make good decisions regarding prevention and training expenditures without understanding the full extent of the threat that ransomware makes to the organization.

Develop Adequate Policies. Devices not owned by the organization are often connected to the organization's network. These would include, for example, cell phones and tablets owned by employees. This is sometimes called "shadow IT." Ransomware policies, protection, and response procedures need to include the entire network, including shadow IT (Best Practices, 2016).

Institute Best Practices for Users. These would include appropriate password management, ongoing security awareness training, backchannels for key employees dealing with finances or sensitive so requests for funds transfers can be double-checked, periodic testing of employees to make sure the training is effective, an appropriate social media policy, and making sure employees keep the software on their personal devices up-to-date (Best Practices, 2016).

The Federal Bureau of Investigation also recommends the following: make sure employees understand their role in protecting against ransomware, manage the use of privileged accounts so that work gets accomplished at the lowest privilege level possible, configure access controls, including file, directory, and

network share permissions appropriately, disable macro scripts, and implement software restriction policies or other controls to prevent ransomware from executing from commonly used locations ("Incidents of Ransomware on the rise," 2016).

Dealing with an Infected Machine

Dealing with ransomware is expensive; even if you have your data backed up and do not have to pay the ransom. According to the Cyber Threat Alliance, in eighteen months since CryptoWall in January 2015, victims have suffered $325 million in damages. This includes mainly restoring data from backups and purging systems of the ransomware, a process that can take days or weeks, during which the business may have limited abilities to operate (Zetter, 2016).

Ransomware does not destroy data. Rather, it locks up the data until a ransom is paid. Even if the ransomware infection is removed, the data remains encrypted (Bradley, 2015). While many versions of ransomware encrypt files in such a way that no recovery is possible without paying the ransom, many more versions have flaws that allow files to be recovered without paying a ransom. Often, the warning screen for crypto ransomware will give the name of the ransomware, which can serve as a starting point for research. Antivirus company AVG recommends the following steps:

Step 1: Run a full scan of the infected computer to find out the ransomware used.

Step 2: Copy the encrypted files to a USB drive so they can be decrypted on an uninfected computer. This also leaves the targeted computer in its infected state in case there is a need to pay the ransom to decrypt the files.

Step 3: Use a tool to decrypt the files on the USB drive. AVG provides free tools for decrypting six ransomware strains: Apocalypse, BadBlcok, Crypt888, Legion, SZFLocker, and TeslaCrypt (Buckingham, 2016).

Whether a tool is used to recover files, the files are recovered from a backup, or the ransom is paid, the ransomware software must be removed from the computer. Experts recommend that the data files be copied off the computer and then the hard drive reformatted and the operating system and files reinstalled fresh (Rosenberg, 2015).

Concise Concluding Inferences

Ransomware has become one of the most urgent problems in the digital world. The frequent attacks and the news they generate have shattered the illusion that firms have frequent backups and do an excellent job of protecting their digital resources. Clearly, protecting oneself from ransomware is hard. If firms find it challenging, what chance to individual users have of protecting themselves? And all of this is happening as both firms and individuals move more and more of their data, and lives, online. Unlike a mugger or burglar, these attackers are typically shadowy figures from other countries that have weak or nonexistent law enforcement, making it unlikely that law enforcement is going to make much of a dent in the wave of ransomware.

References

Abrams, L. (2016, December 8). New scheme: Spread popcorn time Ransomware, get chance of free Decryption key. *Bleeping Computer*. Retrieved from https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/

Barker, I. (2016, June 23). Crypto-ransomware attacks increase five fold. Retrieved from http://www.betanews.com/2016/06/23/crypto-ransomware-five-fold-increase/

Best Practices for Dealing with Phishing and Ransomware. (2016). Osterman Research, Inc.

Bradley, S. (2015, April 23). How to defend yourself from ransomware. Retrieved from Windows Secrets, http://windowssecrets.com/top-story/how-to-defend-yourself-from-ransomware/

Buckingham, A. (2016, July 1). *AVG announces 6 new tools to free your data from ransomware*. Retrieved from http://betanews.com/2016/07/01/avg-announces-6-new-tools-to-free-your-data-from-ransomware/

Cannell, J. (2016). *Cryptolocker Ransomware: What you need to know*. Retrieved from Malwarebytes, https://blog.malwarebytes.com/101/2013/10/cryptolocker-ransomware-what-you-need-to-know/

Cawley, C. (2016, August 30). A history of Ransomware: Where it started & where it's going. Retrieved from http://www.makeuseof.com/tag/history-ransomware-russia-reveton/

Chirgwin, R. (2016, May 3). Michigan electricity utility downed by ransomware attack. Retrieved May 3, 2016, from The Register, http://www.theregister.co.uk/2016/05/03/michigan_electricity_utility_downed_by_ransomware_attack/

Collier, K., Vovcuk, V., & Turgeman, M. (2016, August 26). Now you can buy your own custom Ransomware. Retrieved from http://www.vocativ.com/353523/shark-ransomware/

Constantin, L. (2015, September 24). Ransomware pushers up their game against small businesses. *PC World*. Retrieved from http://www.pcworld.com/article/2985826/security/ransomware-pushers-up-their-game-against-small-businesses.html

Constantin, L. (2015b, November 9). File-encrypting ransomware starts targeting Linux web servers. *PC World*. Retrieved from http://www.pcworld.com/article/3003098/business-security/file-encrypting-ransomware-starts-targeting-linux-web-servers.html

Constantin, L. (2016, March 28). This nasty ransomware overwrites your PC's master boot record. Retrieved from PC World, http://www.pcworld.com/article/3046626/security/petya-ransomware-overwrites-mbrs-locking-users-out-of-their-computers.html

Constantin, L. (2016b, May 24). New DMA locker ransomware is ramping up for widespread attacks. Retrieved from http://www.pcworld.com/article/3074823/security/new-dma-locker-ransomware-is-ramping-up-for-widespread-attacks.html

Constantin, L. (2016c, July 14). New Locky ransomware version can operate in offline mode. Retrieved from PC World, http://www.pcworld.com/article/3095865/security/new-locky-ransomware-version-can-operate-in-offline-mode.html

Destroying ransomware business models is not your job, so just pay up. (2016, May 17). Retrieved from http://www.theregister.co.uk/2016/05/17/pay_up_or_dont_ransomware_is_only_a_matter_of_money/

Enderle, R. (2016, June 9). Another Ransomware surprise and this One is a beast. Retrieved from http://www.tgdaily.com/enterprise/160786-another-ransomware-surprise-and-this-one-is-a-beast

Fadilpašić, S. (2016, November 3). Kaspersky tells ransomware victims not to pay up. Retrieved November from http://www.betanews.com/2016/11/03/dont-pay-ransom/

Fadilpašić, S. (2016b, September 12). New version of RAA ransomware only goes after business users. Retrieved from http://betanews.com/2016/09/12/new-version-raa-ransomware

Farrell, N. (2016, May 12). Ransomeware writers quickly adapt. Retrieved from Techeye, http://www.techeye.net/news/ransomeware-writers-quickly-adapt

Fitzpatrick, D., & Griffin, D. (2016, April 15). Cyber-extortion losses skyrocket, says FBI. *CNN*. Retrieved August 27, 2016, from http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security

Franceschi-Bicchierai, L. (2016, August 7). Hackers make the First-Ever Ransomware for smart thermostats. Retrieved from http://www.motherboard.vice.com/read/internet-of-things-ransomware-smart-thermostat

Francis, R. (2016, July 20). The history of ransomware: How PC hostage-taking has evolved over the years. Retrieved from PC World, http://www.pcworld.com/article/3098005/data-breach/the-history-of-ransomware-how-pc-hostage-taking-has-evolved-over-the-years.html

Gallagher, S. (2016, April 8). OK, panic—newly evolved ransomware is bad news for everyone. . Retrieved from http://www.arstechnica.com/security/2016/04/ok-panic-newly-evolved-ransomware-is-bad-news-for-everyone/

Gallagher, S. (2016b, July 13). Posing as ransomware, windows malware just deletes victims' files. . Retrieved from http://arstechnica.com/security/2016/07/posing-as-ransomware-windows-malware-just-deletes-victims-files/

Gallagher, S. (2016c, February 18). "Locky" crypto-ransomware rides in on malicious word document macro. *Ars Technica UK*. Retrieved from http://arstechnica.co.uk/security/2016/02/locky-crypto-ransomware-rides-in-on-malicious-word-document-macro/

Ginos, I. (2016, March 26). Petya ransomware reportedly encrypts hard drives, manipulates operating system boot process. Retrieved from https://www.neowin.net/news/petya-ransomware-reportedly-encrypts-hard-drives-manipulates-operating-system-boot-process

Goodin, D. (2014, June 7). We "will be paying no ransom," vows town hit by Cryptowall ransom malware. . Retrieved June 8, 2014, from http://arstechnica.com/security/2014/06/we-will-be-paying-no-ransom-vows-town-hit-by-cryptowall-ransom-malware/

Goodin, D. (2016, March 15). Big-name sites hit by rash of malicious ads spreading crypto ransomware [Updated]. Retrieved from http://arstechnica.com/security/2016/03/big-name-sites-hit-by-rash-of-malicious-ads-spreading-crypto-ransomware/

Harley, D. (2016, August 22). Ransomware: To pay or not to pay? Retrieved from We Live Security, http://www.welivesecurity.com/2016/08/22/ransomware-pay-not-pay-2/

Higgins, K. J. (2016, July 15). New HIPAA guidance tackles Ransomware epidemic in healthcare. Retrieved from http://www.darkreading.com/vulnerabilities---threats/new-hipaa-guidance-tackles-ransomware-epidemic-in-healthcare/d/d-id/1326291

Higgins, K. J. (2016b, July 11). New "Ranscam" Ransomware lowers the bar but raises the stakes. Retrieved from http://www.darkreading.com/threat-intelligence/new-ranscam-ransomware-lowers-the-bar-but-raises-the-stakes/d/d-id/1326223

Incidents of Ransomware on the rise. (2016, July 14). Retrieved from http://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise

Kan, M. (2016, August 3). Almost half of US businesses hit by ransomware, says study. *Computer World*. Retrieved from http://www.computerworld.com/article/3103489/security/almost-half-of-us-businesses-hit-by-ransomware-saysstudy.html

Kirk, J. (2016a, March 6). Apple shuts down first-ever ransomware attack against Mac users. Retrieved March 7, 2016, from *PC World*, http://www.pcworld.com/article/3040987/security/apple-shuts-down-first-ever-ransomware-attack-against-mac-users.html

Kirk, J. (2016b, February 19). A new Android trojan steals your banking info and holds your files ransom. Retrieved from PC World, http://www.pcworld.com/article/3035106/security/a-new-android-banking-trojan-is-also-ransomware.html

Kirk, J. (2016c, April 12). With few options, companies increasingly yield to ransomware demands. Retrieved from PC World, http://www.pcworld.com/article/3054591/security/with-few-options-companies-increasingly-yield-to-ransomwaredemands.html

Korolov, M. (2016, June 1). 93% of phishing emails are now ransomware. . Retrieved from http://www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-now-ransomware.html

Lemos, R. (2016, June 28). How greed could destroy the ransomware racket. Retrieved June 28, 2016, from *PC World*, http://www.pcworld.com/article/3083772/security/how-greed-could-destroy-the-ransomware-racket.html

Luna, J. (2016, June 24). Ransomware: What it is, and what you can do about it. Retrieved July 25, 2016, from https://www.neowin.net/news/ransomware-what-it-is-and-what-you-can-do-about-it

Lyposit Malware | win32/Lyposit.A. Retrieved August 28, 2016, from https://www.knowbe4.com/lyposit

MartinSlideshows, S. (2016, June 22). How to lock down so Ransomware Doesn't lock you out. Retrieved June 23, 2016, from http://www.darkreading.com/vulnerabilities---threats/how-to-lock-down-so-ransomware-doesnt-lock-you-out/d/d-id/1326009

McAfee Labs Threats Report, June 2016.

Pauli, D. (2015, November 9). Cryptowall 4.0: Update makes world's worst ransomware worse still. Retrieved November 9, 2015, from http://www.theregister.co.uk/2015/11/09/cryptowall_40/

Pre-packaged exploit kits for Microsoft office. (2016, July 19). Retrieved July 20, 2016, from Office Watch, https://office-watch.com/2016/pre-packaged-exploit-kits-for-microsoft-office/

Press, T. A. (2016, December 13). Arkansas sheriff's office hit by ransomware pays hackers. Retrieved December 13, 2016, from Salon, http://www.salon.com/2016/12/13/arkansas-sheriffs-office-hit-by-ransomware-pays-hackers/

Rashid, F. Y. (2016, March 14). 4 reasons not to pay up in a ransomware attack. Retrieved March 19, 2016, from http://www.infoworld.com/article/3043197/security/4-reasons-not-to-pay-up-in-a-ransomware-attack.html

Rosenberg, J. M. (2015, April 8). *A Q&A about the malicious software known as ransomware*. Retrieved April 8, 2015, from http://www.salon.com/2015/04/08/a_qa_about_the_malicious_software_known_as_ransomware/

Rosenberg, J. M. (2016, April 8). Computer users face hard choice _ pay ransom or lose files. Retrieved April 8, 2016, from Salon, http://www.salon.com/2015/04/08/computer_users_face_hard_choice___pay_ransom_or_lose_files/

Rosenquist, M. (2016, November 29). Beware: Scalable vector graphics files are A new Ransomware threat. Retrieved November 30, 2016, from Dark Reading, http://www.darkreading.com/partner-perspectives/intel/beware-scalable-vector-graphics-files-are-a-new-ransomware-threat/a/d-id/1327581?_mc=RSS_DR_EDT

Savage, K., Coogan, P., & Lau, H. (2015). The Evolution of Ransomware.

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016, June). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. In 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS) (pp. 303-312). IEEE.

Segura, J. (2016). *Citadel: A cyber-criminal's ultimate weapon?* Retrieved August 28, 2016, from https://blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/

Sheridan, K. (2016, August 30). New "Fantom" Ransomware poses as windows update. Retrieved November 6, 2016, from http://www.darkreading.com/attacks-breaches/new-fantom-ransomware-poses-as-windows-update/d/d-id/1326774

Sjouwerman, S. (2015a). *Ransomware on pace to be A 2016 $1 Billion dollar business*. Retrieved August 28, 2016, from https://blog.knowbe4.com/ransomware-on-pace-to-be-a-2016-1-billion-dollar-business

Sjouwerman, S. (2015b). *A short history & evolution of Ransomware*. Retrieved August 28, 2016, from https://blog.knowbe4.com/a-short-history-evolution-of-ransomware

Song, Y.-S. (2016, August 25). Ransomware: 3 seconds to encryption. Retrieved August 25, 2016, from Beta, http://betanews.com/2016/08/25/ransomware-3-seconds-to-encryption

Spadafora, A. (2016, June 27). New ransomware targets office 365 users. Retrieved June 27, 2016, from http://betanews.com/2016/06/27/office-365-ransomware/

Spector, L. (2016, May 6). How to stop ransomware: Backup can protect you, but only if you do it right. Retrieved May 6, 2016, from PC World, http://www.pcworld.com/article/3056907/security/how-to-stop-ransomware-backup-can-protect-you-but-only-if-you-do-it-right.html

State of Ransomware 2016: Understanding the Depth of the Ransomware Problem in the United States. (2016). Osterman Research, Inc.

Sutton, M. (2016, July 1). Big business Ransomware: A lucrative market in the underground economy. Retrieved July 3, 2016, from http://www.darkreading.com/vulnerabilities---threats/big-business-ransomware-a-lucrative-market-in-the-underground-economy/a/d-id/1326144

The nuts & bolts of Ransomware in 2016. (2016). Retrieved August 27, 2016, from http://www.titanhq.com/the-nuts-bolts-of-ransomware-in-2016

Thompson, C. (2015, June 10). What to do when Ransomware takes your computer hostage. Retrieved from http://www.slate.com/blogs/business_insider/2015/06/10/ransomware_a_form_of_malware_is_taking_over_the_internet_protect_yourself.html

Townsend, K. (2016, June 24). History and statistics of Ransomware. Retrieved from http://www.securityweek.com/history-and-statistics-ransomware

Tozer, N. (2016, March 30). How to mitigate ransomware risks. Retrieved March 30, 2016, from *Beta News*, http://www.betanews.com/2016/03/29/mitigate-ransomware-risks/

Tromer, E. (2008). Cryptanalysis of the Gpcode.Ak ransomware virus. Retrieved from rump2008.cy.yp.to/6b53f0dad2c752ac2fd7cb80e8714a90.pdf

Valach, A. P. (2016, November 8). Risk management – what to do after a Ransomware attack. Retrieved from http://www.rmmagazine.com/2016/06/01/what-to-do-after-a-ransomware-attack/

Valach, A. P. (2016, November 8). Risk management – what to do after a Ransomware attack. Retrieved from http://www.rmmagazine.com/2016/06/01/what-to-do-after-a-ransomware-attack/

Wiles, R. (2016, November 4). Hackers get smarter: They're lowering their ransom prices. Retrieved from http://www.usatoday.com/story/money/personalfinance/2016/11/04/ransomware-attack-ransom-price/92746524/

Wolff, J. (2016, February 18). Lessons from the Hollywood hospital that paid $17, 000 to free its computers from Ransomware. Retrieved from Slate, http://www.slate.com/articles/technology/future_tense/2016/02/hollywood_presbyterian_medical_center_paid_17_000_to_free_computers_from.html

Zetter, K. (2015, September 17). *Hacker lexicon: A guide to Ransomware, the scary hack that's on the rise*. Retrieved from Security, https://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/

Zetter, K. (2016, May 13). *4 ways to protect against the very real threat of Ransomware*. Retrieved from Security, http://www.wired.com/2016/05/4-ways-protect-ransomware-youre-targe