Ransomware - Rising Menace to an Unsuspecting Cyber Audience

A Thesis

Presented to

the Faculty of the Department of Information and Logistics Technology

University of Houston

In Partial Fulfillment

of the Requirements for the Degree of

Master of Science

Information Systems Security

By

Pranav Narain

May 2018

Ransomware - Rising Menace to an Unsuspecting Cyber Audience

_____

Pranav Narain

APPROVED:

_____

Robert Christopher Bronk, PhD, Committee Chair
Assistant Professor, Information and Logistics Technology

_____

William Arthur Conklin, PhD
Associate Professor, Information and Logistics Technology

_____

Denise Kinsey, PhD
Assistant Professor, Information and Logistics Technology

_____

George Zouridakis, PhD
Associate Dean for Research and Graduate Studies, College of Technology

_____

Dan M Cassler
Interim Chair, Information and Logistics Technology

DECLARATION OF ORIGINALITY

I hereby certify that I am the sole author of this thesis and that no part of this thesis has been published or submitted for publication.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Copyright Act of 1976, I certify that I have taken measures to abide by the Act.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

ABSTRACT

Ransomware has quickly become one of the biggest threats, the public and enterprises in the cyber space, have ever had to face and continues to cement itself as a prominent threat with new variants being deployed periodically.

As the security community wises up to this issue and the security solutions incorporate advanced defense mechanisms to combat ransomware, the families also continue to evolve further by exploiting zero-day vulnerabilities and propagating itself in a much stealthier and creative way. Ransomware being combined with Advance Persistent Threats as well as the availability of Ransomware-as-a-Service (RaaS) is another big cause for concern.

This thesis highlights the latest developments in the security landscape to deal with the issue and ascertain whether the solutions currently available are feasible enough to eradicate the ambiguity caused by various ransomware families thus delaying an effective response to mitigate the attack on enterprise systems and Android devices.

To my amazing parents, Amit and Rashmi, infinitively supportive

ACKNOWLEDGEMENTS

The thesis I undertook over the course of the last couple of semesters at the College of Technology, University of Houston was a good opportunity to expand my knowledge base as well as for professional development. I am grateful for having a chance to meet so many wonderful people who led me through this research period.

I will use this opportunity to express my gratitude and special thanks to Dr. Robert Christopher Bronk, my guide and chair for the thesis, who in spite of being extraordinarily busy with his duties, took time out to hear, guide and keep me on the correct path and allowing me to carry out my project at this esteemed organization while extending a helping hand during the research. His constant support was a big factor during this entire journey.

I express my deepest gratitude to Dr. William Arthur Conklin, for taking part in decision making processes & giving necessary advice and guidance and partake actively in my work activities to make life easier. I choose this moment to acknowledge his contribution gratefully.

I express my deepest thanks to Dr. Denise Kinsey, Assistant Professor at University of Houston, for her guidance and constant supervision as well as for providing necessary information regarding the thesis & also for her moral support during this educational journey.

It is my radiant sentiment, to place on record my best regards and deepest sense of gratitude to my family for their support which was extremely valuable for constantly performing and excelling at the highest level.

I also extend a warm thank you to my peers at University of Houston for being there throughout and for being very cordial and accommodating to study and work with.
I perceive this experience as a big milestone in my career development. I will strive to use acquired skills and knowledge in the best possible way, and I will continue to work on their improvement, to attain desired career objectives. Hope to continue to grow with everyone in the future.

Table of Contents

LIST OF FIGURES

INTRODUCTION

With the advent of concepts that are aimed at accomplishing specific tasks and thus providing a positive impact in people's lives, there is always another aspect to it that aims at exploiting the concept for personal gain and thus disrupting the daily activities of the unsuspecting cyber audience. This is particularly visible when utilizing Cryptography for securing systems. According to Murray, W. H. (2008) in *What the Graduate Needs To Know About Cryptography*, "Modern systems have both increased the need and cost for cryptography." Yet, with no specific security measure in place for safeguarding the cryptographic elements of a system, specific vulnerabilities found in the system lead to exploitation of these elements. This is especially lacking at the hardware level and will be elaborated upon in further chapters. Improvement in technologies in the last decade in terms of Virtual Private Networks, Hash graphs and Blockchain, has created a perfect setup for malicious activities to be conducted on a large scale albeit a stealthy and evasive manner. Maintaining anonymity plays a pivotal role in a ransomware operation. Ransomware has been around since 1989, Gazet, A. (2010), but was never the perfect recipe for successfully exploiting people and getting away with it if performed at a large scale. It was an incomplete form of malware until recently and has seen a surge since 2013. Vanderburg, Eric. (2017)
With the recent introduction of Bitcoin as transaction units, it has ended up opening doors for potential threats to become active attacks with unique attack vectors and zero-day vulnerabilities making it harder to trace the malicious attacker. Liska, Allan and Gallo, Timothy (2016)

We will discuss more on how this came to be in further chapters as well as how it all fits into a perfect recipe for black hats to conduct exploits without fear of getting caught. Ransomware families continue to increase as variants are now being introduced for mobile devices apart from just home systems or portable devices like laptops. The protection for the same lies in the fact that the users are aware of the potential threat and are able to take necessary steps to avoid infection. Automatic key management, with no monitoring, often leads to quick demise of the system; once the exploit infiltrates the vaults or the key storage systems, making it an easy prey for attackers to encrypt and subsequently take over the system as a whole. Policies are essential for key management. Having strong cryptography schemes but weakly protected keys is another cause for concern as the aim these days is to bypass the schemes instead of breaking it due to time,

cost and resource factors. A much more efficient way to exploit from a black hat perspective. Murray, W. H. (2008)

But with increased focus on Ransomware and the classification of the variants based on similar traits, it has led to more reactive as well as proactive measures to surface utilizing deep learning algorithms and AI based detection techniques. The idea is to see how a commercially viable balance can be achieved while incorporating some of these measures into the system so that enterprises see it as an essential module instead of a cost add on and thus ensure that ransomware attacks can be blocked and eventually deemed as an infeasible form of exploitation. We will now explore and understand Ransomware at the basic level and build on the same while moving through its evolution across history. Chen, Y. C. et al. (2018)

WHAT IS RANSOMWARE?

In broad terms, a Ransomware is defined as a form of malware that disrupts user access to valuable resources via encryption and blocks any means of unlocking them until a ransom is paid to reestablish access. It is a means for extortion at both enterprise level and personal systems to achieve monetary gain. Mateiu, Monica. (2018). To further explain where Ransomware originates from, i.e., it is a form of malware, a piece of software or lines of code that is designed by an attacker to gain access and perform malicious actions like pilfering data, without the knowledge of the user, downloading them in the process. Legitimate users are denied access and in exchange for stolen functionality, are made to part with their money. This leads to large scale revenue generation for cyber criminals. Essentially it is the fear of losing data valuable to them and the lack of precautionary measures to preserve the data in a more secure location, that are exploited by the attacker. Vanderburg, Eric. (2017)

Cyber criminals tend to feed off the burgeoning market in a consistently evolving cyberspace. The reason such a large-scale extortion scheme has been successful is directly dependent on the multitude of approaches taken by each type of ransomware are quite different, thus, difficult to identify a generic one-for-all solution. The rise of health-based ransomware targeting devices

including pacemakers, health monitors or smart implants is a real issue and with the integration of smart technology such as smart television, security cameras, door locks and thermostats in our daily lives, it is evident that ransomware is here to stay. It is only bound to get even more lethal with every new variant introduced in the cyber space especially with Ransomware. Charette, N. Robert (2018)

Before we breakdown the different types of ransomware into their respective families, ransomware is pre-dominantly classified into two major types:

- Locker Ransomware
- Crypto Ransomware

With TOR based ransomware taking most of the RaaS market share, and a business succumbs to it, it generally means that important information has been lost. This equates to a major security breach, in addition to a significant financial hit to the business. These targeted businesses may not always be able to rely on computer backups or other safeguards that were supposedly protecting their crucial information. This could leave them at the mercy of the hacker with the understanding that they might or might not get the data back based on the nature of the infection. New ransomware tend to delete the data and only pretend to restore data upon payment of ransomware. Roccia, Thomas. (2018)

The key characteristics of these types of Ransomware along with classifying their variants in specific categories is essential to develop strategies to mitigate and effectively respond to each unique attack.

CRYPTOWARE – ORIGINS OF RANSOMWARE

To see what lies ahead for the future of ransomware and its integration with upcoming threats such as Crypto-jacking, it is important to delve into the past of both ransomware, and the advent of digital crypto techniques. Studying these events in the past allows us to figure out the most likely course of evolution and prepare for more advanced cybercrime.

Gazet, A. (2010) identifies that one of the first identified instances of ransomware, the virus was distributed on a floppy disk by the postal service. It sounds old-fashioned and outdated but was effective in its execution due to the surprise factor and not having seen an attack executed in this form and even more insidious than its modern descendants. Thus, dealing with the unknown and the surprise factor was a major element. Contemporary ransomware tends to bait victims using legitimate-looking email attachments—a fake invoice from Amazon and viruses in Microsoft software or Adobe Flash player updates. But the 20,000 disks dispatched to 90 countries in December of 1989, were masquerading as something much more unexpected - AIDS education software. Gazet, A. (2010),

Gazet, A. (2010) further mentions that the package that was delivered to victims abroad (they weren't distributed within the U.S.) was stamped with a fake company name called - PC Cyborg Corporation. Although the company was fake, the disk inside really did include a program that measured a person's risk of contracting AIDS based on their responses to an interactive survey. It also contained what came to be known as the "AIDS" Trojan, a virus that encrypted a victim's files after they had rebooted their computer a fixed number of times. The ransom demand came in the form of an analog note via a printer. Users were instructed to turn on their printers, which promptly asked for a "licensing fee" of $189 to be paid using the 20th century, black-box equivalent of Bitcoin: by sending money to a Panamanian PO Box. Mateiu, Monica. (2018).
Only then would the victim receive their decryption software. Extortion may be an age-old crime, but its sudden appearance in digital form caught the public completely unprepared. The virus was first reported in the UK, when there weren't even laws on the books for dealing with this brand of cybercrime. The 1968 Theft Act, at the time, held the closest semblance to anything that could be used in court at the time. Zaharia, Andra. (2017).

Young, A., and Yung, M. (1996) wrote "*Cryptovirology: Extortion-based security threats and countermeasures*", which shed light on the how to use crypto techniques for personal gain via unlawful ways as well as disruption of services. After AIDS Trojan was first unleashed by Popp, the two pioneering cryptographers—Adam L. Young and Moti M. Yung—patched the holes in Popp's programming by developing a class of algorithms known as public-key cryptography. The

two researchers created a proof-of-concept virus that encrypted files utilizing RSA and TEA algorithms, while denying access to the key used to encrypt the files.

In hindsight, "*Cryptovirology: Extortion-based security threats and countermeasures*", Young, A., and Yung, M. (1996), probably ended up being the primary source of knowledge for ransomware based attacks to come to fruition as the use of cryptology for malicious purposes is discussed in depth to the point of clearly highlighting the exact requirements to pull off an attack at such a large scale with crippling effects on its victims if not fully prepared or in most cases oblivious to this threat. It is important to state that this paper was ahead of its time as the tools and technology required for successfully administering such an attack only surfaced recently and the authors had no way of knowing that someday their idea would be practically implemented at a large scale even though it would be fair to say that is was predictable with the rapidly advancing technology in the 21st century.

According to Gazet, A. (2010), ransomware like Krotten, Archiveus, and GPCoder, came up in 2005 and multiple variants made an appearance subsequently. Out of the malware families noted here, GPCoder was an interesting instance of ransomware as it used 1024-bit RSA encryption when encrypting files, making file recovery via brute force difficult. At first it was believed that Cryptography wasn't an absolute necessity for ransomware in general, as social engineering techniques combined with moderate ransom price points could help facilitate a successful locker-ware (non-cryptographic ransomware) attack as it can use a simple JavaScript technique to take control of a browser, again with a ransom demand and revert control only after payment of it. The simplicity of mitigating these attacks ended up causing the unavoidable shift to cryptography techniques and stronger public key-based encryption as the base of all modern attacks. In hindsight, modern ransomware now depicts how crypto-ware is the only way to get close to an unbreakable denial-of-service extortion form of attack.

In 2009, crypto ransomware had forayed into the public key cryptography arena in force, and its use increased rapidly. Unlike locker-ware, there's no simple way to restore a critical resource and regain normal operation. The period between 2009 and 2012 became what we can now consider as the transition period where the emergence of blockchain technology and the use of ledgers for

anonymous transactions along with asymmetric cryptography techniques completed all the requirements for a true ransomware attack. Vanderburg, Eric. (2017).

Krebs, Brian. (2012) in his article mentions that during this time, Reveton, a major locker ransomware, took forefront due to lack of measure in place for ransomware-based attacks but was controlled by booting the system into Safe Mode, and deleting the file ctfmon.lnk that is present in the Startup folder. Despite that, with the new technology available and emergence of crypto based ransomware, it was almost inevitable that the preparation put in by cyber criminals, for the onset of the crypto era, would be set into the execution phase.

CryptoLocker, one of the earliest forms of crypto ransomwares, surfaced in fall of 2013, and remained amongst the most widespread of the crypto-ransomware families until mid-2014. Kotov, V. and Rajpal, M. S. (2012), explain that CryptoWall surfaced towards the end of 2013. New strains of CryptoWall appeared as recently as October 2014. Critroni acts similarly to CryptoWall, that is, they both require using the TOR browser to make payments, and they both were prominent during early 2014. According to Kotov, V. and Rajpal, M. S. (2012), the DirtyDecrypt outdates CryptoLocker, appearing in early 2013—a few months before CryptoLocker became prominent. It majorly targets and encrypts eight different file formats, which makes sense since it is among the earliest iterations of ransomware. The market size for ransomware substantially expanded in 2015 where Cisco Talos (2016) estimated that ransomware that was distributed through the Angler exploit kit was garnering criminals $60 Million annually. Since 2005, computation power has come a long way and systems have become relatively faster and many such early variants have been reverse engineered by various security researchers and firms and there are tools to prevent infection from these. But having said that, cyber criminals have come up with more ingenious ways to avoid detection which has led to introduction of AI into many real time detection mechanisms and hardware techniques for recognizing heavy encryption activities. We will be taking a closer look at these new detection and prevention mechanisms as well as post detection mitigation techniques in subsequent chapters. Chen, Y. C. et al. (2018)

Figure 1a and 1b are relatively current infographics, designed with respect to important events in the ransomware history leading all the way up to current incidents. The trend gets highlighted

better when taking a visual perspective especially in terms of migration to different types of attack vectors and targeted devices.

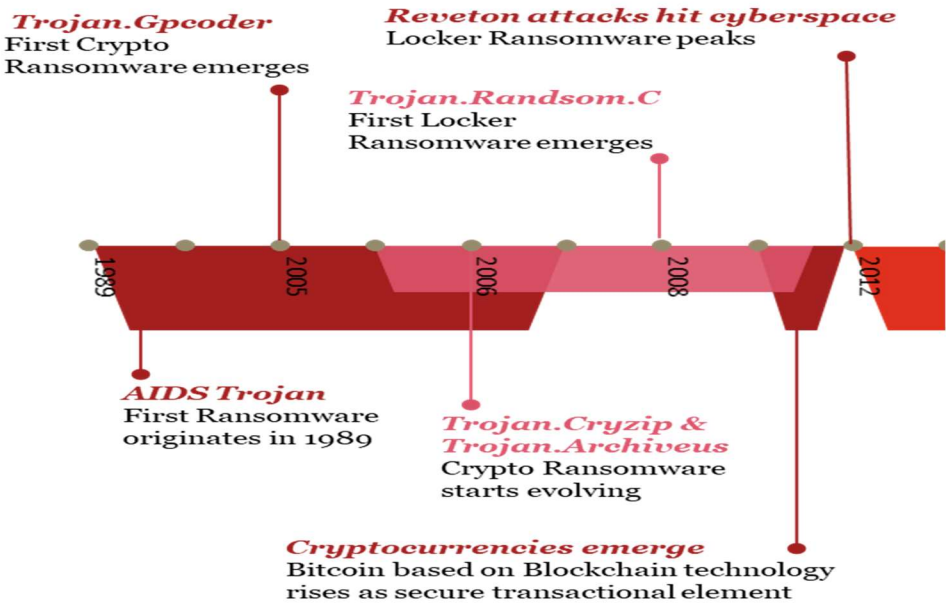

Figure 1a Timeline - Evolution of Ransomware

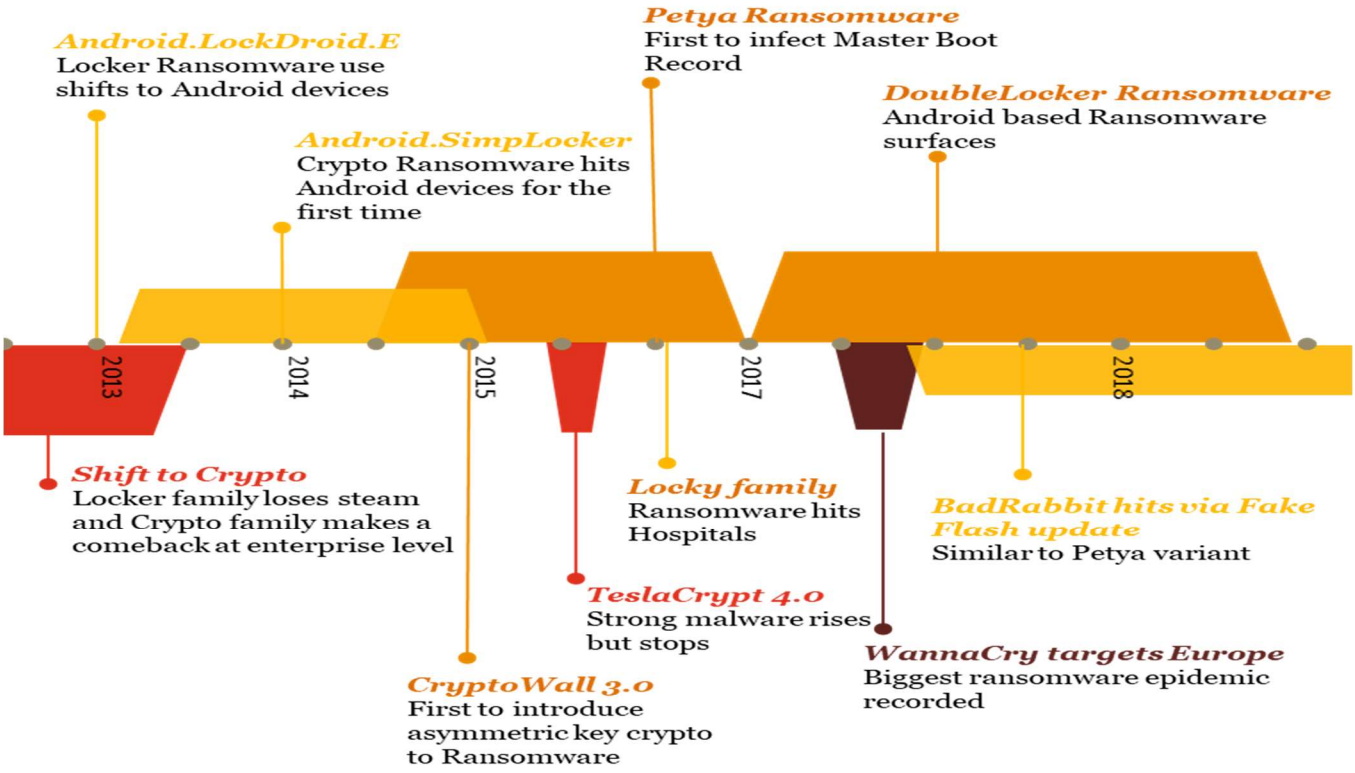

Figure 1b Timeline - Evolution of Ransomware

TYPES OF RANSOMWARE

Locker Ransomware typically locks the computer's or device's user interface and then asks the user to pay a fee to restore access to it. Locked computers will remain with limited capabilities. Locker Ransomware leaves the underlying system and files untouched. This type of ransomware often masquerades as law enforcement authorities and claims to issue fines to users for alleged online indiscretions or criminal activities. Zaharia, Andra. (2017). Since it is possible to remove most locker ransomware cleanly, the cyber criminals tend to go to great lengths to incorporate social-engineering techniques to pressure victims into paying. The idea is to use scareware tactics to create chaotic situations and time dependent effects to increase the chances of payment instead of a chance to conduct careful forensic analysis and mitigation. Although with continued effort through employee training and public awareness programs, the threat gets minimized as the panic factor is taken out of the equation and there are procedural steps that can be followed. Savage, K., Coogan, P. and Lau, H. (2015)

Locker ransomware can particularly be effective on devices that have limited options for users to interact with. This is a potential problem area considering the recent boom in wearable devices and the Internet of Things (IoT), where millions of connected devices could potentially be at risk from this type of ransomware. There are various cases of Locker ransomware being used on Android devices with easy integration to pre-installed services hence making it effective and a growing possible target for the future. Yang, T. et al. (2015)

Crypto Ransomware finds and encrypts valuable data stored on the computer, making the data useless unless the user obtains the decryption key. Crypto Ransomware noticeably searches for files and encrypts them. Its goal is to stay unnoticed only until it can find and encrypt all the files that could be important and valuable to the user. With Crypto Ransomware infections, mostly, the affected computer continues to work normally, and users can still use the computer apart from accessing encrypted data. The decryption key is stored on the attacker's server, so victims cannot recover their files without paying the ransom. There is an added risk with this type of ransomware in terms of potential backdoors being created and spreading the infection to multiple files that may be exchanged via the network to and from the compromised system. Kotov, V. and Rajpal, M. S. (2012)

RANSOMWARE FAMILIES

With multiple variants classified based on type of attack vectors, propagating tendencies and impact on data, a few families have taken center stage in the ransomware domain. Lanet, J., Guernic, C. Le and Legay, A. (2017) explain about CryptXXX, CTB Locker, TeslaCrypt. These strains have a specific target audience and the anatomy of the attack is devised with that in mind. Below is a historic review of the prominent families and how they have matured over multiple iterations.

Petya ransomware

The Petya ransomware family was first discovered in May 2016, and its trademark includes infecting the Master Boot Record to execute the payload and encrypt the data available locally.
It infects the hard drive partition table and prevents the operating system to be launched. Victims are redirected to a special boot screen asking for a ransom with persuasive font. Vanderburg, Eric. (2017)

Besides partition table overwriting which is not a new feature for malware, a special structure managed by the file system driver called Master File Table (MFT) is also encrypted preventing file recovery from a live cd. Based on research, it is the first significant ransomware to possess an entire offline cryptosystem design and which is placed at low-level. The disk encryption is performed with the stream cipher *salsa20*. Lanet, J., Guernic, C. Le and Legay, A. (2017)

WannaCryptor ransomware

The ransomware – also known as WannaCry, WCry, WannaCrypt and WannaCrypt0r – encrypted victims' files and changed the extensions to the following: *.wnry, .wcry, .wncry and .wncrypt*. WannaCry, searches for and encrypts 176 different file types and asks users to pay a US$300 ransom in Bitcoins. The ransom note indicates that the payment amount will be doubled after three days. If payment is not made after seven days, it claims the encrypted files will be deleted. Mills, Chris (2017)

The attack was apparently launched using NSA code leaked by a group of hackers known as the Shadow Brokers. National Health Service hospitals (NHS) in the UK suffered the brunt of the attack early on, with its phone lines and IT systems being held hostage. It resurfaced in early 2018 to hit the Boeing production unit in North Charleston in South Carolina although the damage was kept to a minimum due to faster remediation as compared to the first encounter with the WannaCryptor family in May 2017. Bisson, David. (2016)

Figure 2 WannaCry Pop-up upon file encryption

Source: Mills, Chris (2017)

The attack appears to exploit a Windows vulnerability Microsoft released a patch for in March. That flaw was in the Windows Server Message Block (SMB) service, which Windows computers use to share files and printers across local networks. Microsoft addressed the issue in its MS17-010 bulletin. Vanderburg, Eric. (2017)

Cerber ransomware

Cerber has been around for a while and its utilization has frequently gone up and down. A recent overhaul and new features have brought it back firmly into center stage. According to Lanet, J., Guernic, C. Le and Legay, A. (2017), in the first quarter of 2017, Cerber saw a rise to 90% market share among all the ransomware families. As of now, it ranks right up there with Not-Petya and WannaCry. Security researchers first identified Cerber in early 2016. The crypto based malware family has gone through at least six iterations. It's also sparked a ransomware-as-a-service (RaaS) platform that's resulted in more than a million dollars a year in ransom payments for its authors. Mateiu, Monica. (2018)

The ransomware has kept certain elements constant across its fast-paced evolution. Cerber uses Malspam with an attached file, for instance, and it still prefers Nemucod malware as its downloader. The malicious attacker now also targets saved passwords from Internet Explorer, Google Chrome, and Mozilla Firefox all before initiating its encryption routine. Cerber ransomware's latest monetization scheme is based on credential theft. The ransomware steals (and then subsequently deletes) a user's Bitcoin wallet files only. To make off with their Bitcoins, it requires the password that protects the stolen files. Burgess, M. and Ieraci, J. (2017)

Users can protect themselves against this updated ransomware variant by exercising caution around suspicious links and email attachments. Next, they should refrain from storing their passwords in a web browser and instead use a password manager to save their login credentials.

Locky ransomware

First seen in February 2016, Locky was reportedly sent to millions of users around the world, in an email scam which claimed to be an invoice or a receipt of order. The emails contained an illegible Word document, asked users to enable macros to view its content, then started downloading the malware. Mateiu, Monica. (2018) Files are being encrypted using RSA-2048 and AES-128 ciphers, and the private key available only with their servers and they are providing a

'.onion' website which is opened in TOR for further communications with C&C server of attacker.

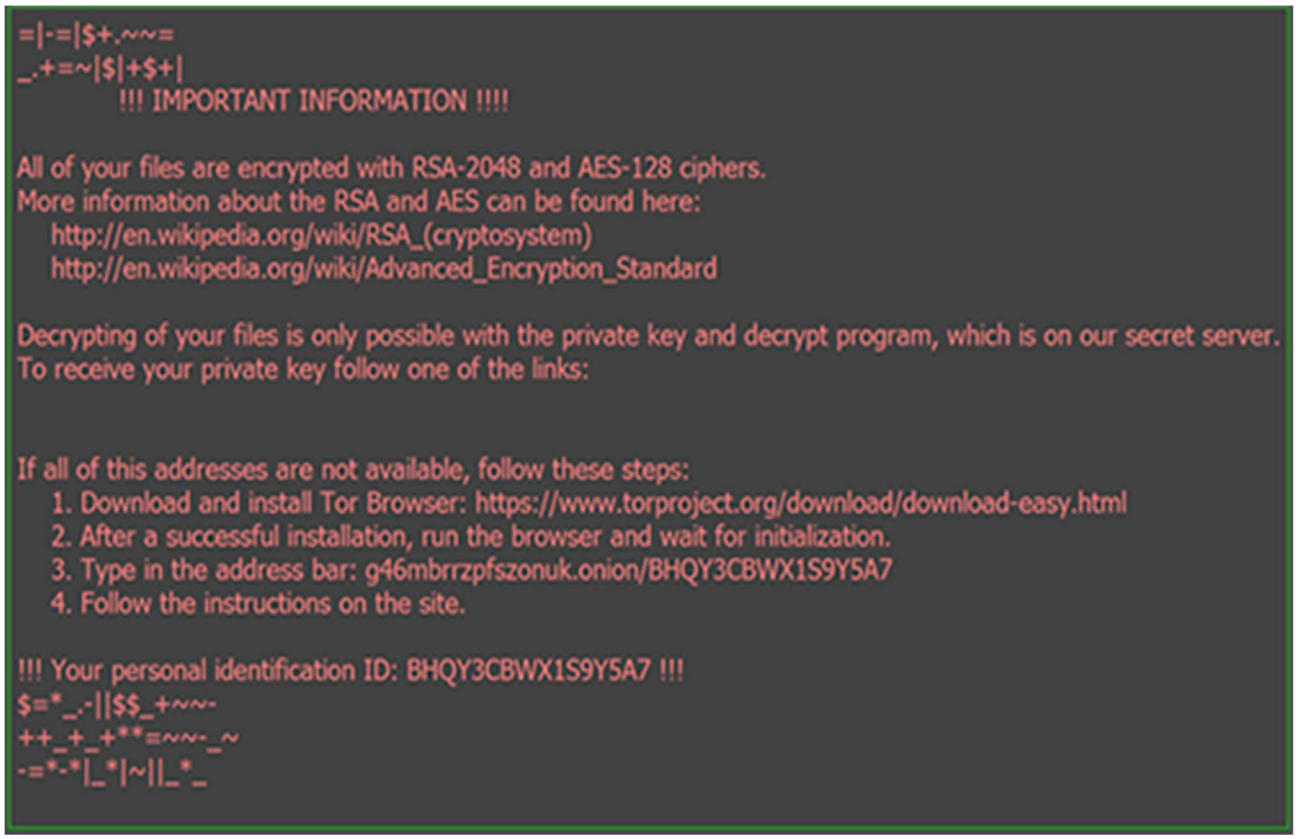

Figure 3 Locky Ransomware Pop-up asking for TOR browser install

Source: Moffitt, Tyler (2017)

The image in the word document is linked to run a PowerShell script, which tends to download another script from using Invoke-Expression which runs specific string as a command and return backs the expression. Then the second script executes and downloads the executable dropper into %temp% folder compiled with Microsoft VC 2013 and multiple layers obfuscation to trick the victims and from security to make the reversing process tedious. It has multiple unwanted strings including the one for system32\calc.exe, by including multiple strings attacker tries to mislead the victims and make them think as the legitimate file. Once it's made a new process it copies to "svchost.exe" and delete the first executable by creating a new process and then it will gather information about operating systems. Then later it passes information encrypted to the C&C servers along with the extent to retrieve the private key. Locky's descendant, Zepto, made its debut in early July 2016. Moffitt, Tyler (2017).

Torrent Locker

This file-encrypting malware emerged in early 2014 and relied almost entirely on spam emails for distribution. To increase effectiveness, both the emails and the ransom note were targeted geographically. Attackers paid attention to detail in their texts, which made their traps seem authentic to the unsuspecting victims. It adds captcha code and redirection to a spoofed site for infection. Mateiu, Monica. (2018)

At the beginning, AES encryption was performed on all files with the same key and Initialization Vector (IV) using Counter (CTR) mode. This can be exploited with one known plain-text and cipher-text in encrypted form. TorrentLocker creators released a new variant which featured stronger encryption and narrowed the chances for breaking it to zero. Its abilities to harvest email addresses from the infected PC are also noteworthy. Consequently, these emails were used in subsequent spam campaigns to further distribute the TorrentLocker. M. L´eveill´e, M.-E. (2014)

CryptoLocker

This family of ransomware encrypts files using AES with a random key which is then encrypted with a 2048-bits RSA public key. The corresponding private key, needed to decrypt the AES key, can be obtained by paying the ransom. Distribution was initially through spam messages containing malicious attachments. Then the main targets were the victims of the botnet Gameover ZeuS. It hit its peak around October 2013. Vanderburg, Eric. (2017). Post the attack, in June 2014, Deputy Attorney General James Cole, from the US Department of Justice issued out a large joint operation involving multiple law agencies and security companies wherein traditional law enforcement techniques and cutting edge technical measures were utilized to combat highly sophisticated cyber schemes targeting citizens and businesses. Zaharia, Andra. (2017).

It was coined Operation Tovar, and aimed to take down the Gameover ZeuS botnet, which authorities also suspected of spreading financial malware and CryptoLocker. Lanet, J., Guernic, C. Le and Legay, A. (2017)

Popular security blogger, Krebs, Brian. (2015) mentioned that "*The trouble with CryptoLocker is not so much in removing the malware — that process appears to be surprisingly trivial in most*

cases. The real bummer is that all of one's important files — pictures, documents, movies, MP3s — will remain scrambled with virtually unbreakable encryption"

CTB Locker

It is one of the first to use ECC to compute public keys and shared secrets based on secret keys generated at runtime. An active Internet connection is no longer required to begin the encryption process, moreover a complex cryptographic design is used. It is the first one which preceded AES file encryption by a compression step using ZLib. Communication with C&C is established by proxy websites like the Tor2web service which acts as a relay to the back-end infrastructure build on Tor hidden service. Lanet, J., Guernic, C. Le and Legay, A. (2017) further state that:

- C refers to Curve, that is Elliptic Curve Cryptography which encodes the affected files with a unique RSA key;
- T refers to TOR browser, because it uses the famous P2P network to hide the cybercriminals' activity from law enforcement agencies;
- B refers to Bitcoin transactions, the payment method used by victims to pay the ransom, also designed to hide the attackers' location.

A key characteristic specific to CTB-locker is that includes multi-lingual capabilities, so attackers can use it to adapt their messaging to specific geographical areas. If more people can understand what happened to their data, the bigger the payday. The CTB Locker spreads through spam campaigns, where the e-mail message appears as an urgent FAX message. Abrams, L. (2017)
CTB-Locker was one of the first ransomware strain to be sold as a service in the underground forums. Since then, this has become the norm, but two years ago it was an emerging trend. In 2014, malware analyst Kafeine managed to access one of these black markets and posted all the information advertised by online criminals. Abrams, L. (2017)

By taking a quick look at the malware creators' advertisement, we can see that the following support services are included in the package:

- Instructions on how to install the Bitcoin payment on the server;

- How to adjust the encryption settings to target the selected victims;
- Requested cost and the available localized languages;
- Recommendations on the ransom that can be set for the decryption key.

TeslaCrypt

TeslaCrypt stands out amongst the other ransomware families as it had a specific target audience. Surprisingly, it was a niche one albeit a very active set of people on the internet i.e. gamers. Out of the wide array of gamers that were targeted, including Call of Duty, World of Warcraft, Minecraft and World of Tanks, were among the worst hit. Zaharia, Andra. (2017). The primary reason for this was that most online versions of these games utilized Adobe Flash, which has been known for possessing multiple vulnerabilities and is a primary attack surface for ransomware infections. TeslaCrypt moves on to bigger targets, such as European companies, through websites that redirect victims to an exploit kit (drive-by download). Angler is one of them which takes advantage of Adobe Flash (CVE-2015-03116). Another interesting difference observed in TeslaCrypt was that it kept encryption keys on the disk during the attack. It is one of the first ransomware which specifically targets files used by video games. Closest to TeslaCrypt in terms of encryption is the CTB-Locker, both have encryption process occurring irrespective of any communication with the C&C, but their cryptosystem design differs ever so slightly. TeslaCrypt embeds an ECC public-key in its binary, shared across multiple samples which is used to compute a shared secret involved in the generation of an AES session key. The system has an ECC master private key which is used to decrypt files once ransom is paid.
It was surprisingly broadcast in May 2016 by the malware authors themselves during the ransomware shutdown process. Cyber security experts managed to find flaws in TeslaCrypt's encryption algorithm twice. TeslaCrypt 4.0 was released in March 2016, but after a period of two months, it was shut down by the malicious attackers themselves and they apologized after an apparent change of heart. ESET researchers managed to get the universal master decryption key from them and built a decryptor that one can use if they become a victim of TeslaCrypt. Zaharia, Andra. (2017).

CryptoWall

As explained by Lanet, J., Guernic, C. Le and Legay, A. (2017), it encrypts files using RSA encryption and uses the Onion Router (Tor) to obfuscate communications with the C&C. Each victim is registered and identified by a unique identifier and get from the C&C the corresponding RSA public-key. Infection vector was sent out initially via exploit kits and then moved to more traditional spam email campaigns. File encryption does not occur if the RSA public-key is not received. It is one of the first requiring payment in Bitcoin only, while deleting the Shadow Copy. Moreover, a list of all the encrypted files is stored in the registry to ease the decryption process. Cisco Inc. (2015) CryptoWall 3.0 upgraded to AES symmetric encryption with Cipher Block Chaining (CBC) mode for files and communication with C&C was done over the Invisible Internet Project (I2P) network. Due to the lack of reliability, they backed it up with a combination of compromised sites forwarding traffic to Tor server. Subsequently, in version 4.0, an additional step in disruption is made by renaming files, including extension, with random characters. To avoid encrypting the same file again following superinfection, a hash corresponding to the RSA public-key given to the victim, is attached to the beginning of the file. Vanderburg, Eric. (2017)

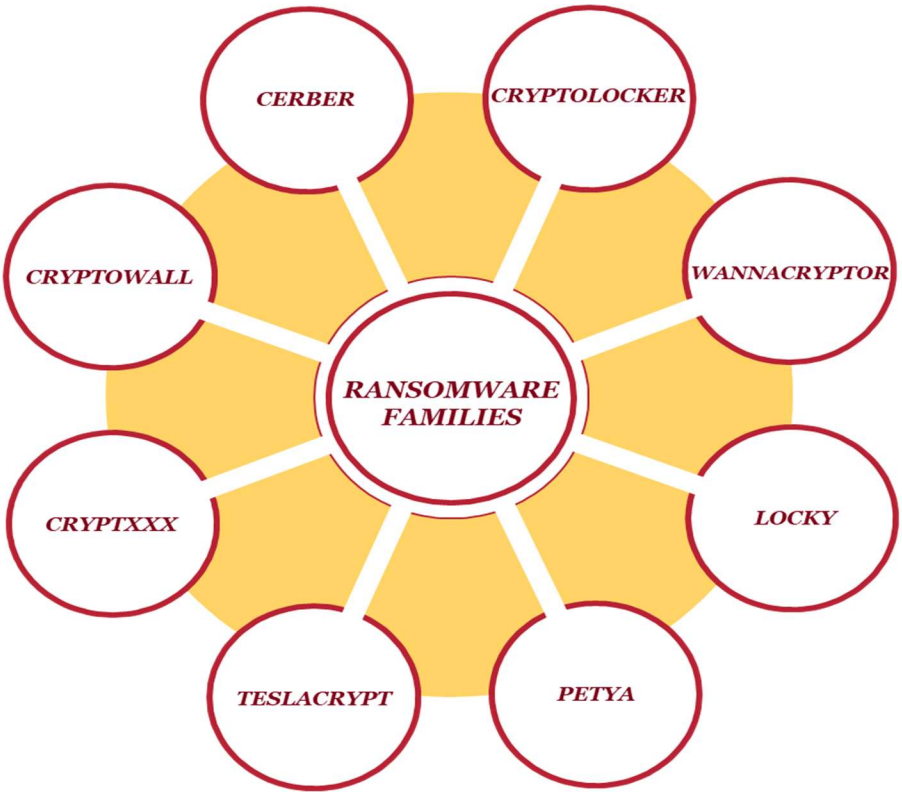

Figure 4 Prominent Ransomware Families

WHAT MAKES THE MODERN RANSOMWARE TICK?

Much debate has gone into whether the modern ransomware will survive in the long run and how will it evolve based on the prevention techniques that develop over time. Even though detection has become more advanced and most ransomware families have been identified with their distinctive characteristics, the form of attack still, at its core, uses typically the same components to get at the people, processes and property. To conduct a ransomware successfully on a large scale there are typically three pre-requisites that need to be met. The current state of technology allows the attacker to meet these requisites. Orman, H. (2016)

a) The payload containing the hostile binary code must not possess the deciphering keys. This is where Command and Control comes into play. The idea is to not make it easily retrievable. In hindsight, white box cryptography can be applied to ransomware

b) The cyber-criminal is the only one that should be able to decrypt the infected device and know the location of the decryption components present in the crypto files of the system.

c) The modern ransomware now mimics the properties of a worm and can self-propagate to multiple devices on the network or Work group and thus it is essential that one device cannot provide any decrypting information for other devices that get infected, which basically means that the key must not be shared among them.

From a malicious attacker's perspective, meeting these pre-requisites before pushing the payload into the system is essential. Therefore, the attack itself requires preparation and will differ based on the environment it is trying to infiltrate which makes it harder to react to quickly and respond. The core components of a ransomware and the processes involved have been largely consistent as the system works well and therefore over the past few years, the pattern has remained unchanged. The components of a ransomware attack that help execute the attack efficiently have been highlighted below for a better understanding of what it takes to execute it. Orman, H. (2016)

Encryption Scheme

Symmetric and asymmetric encryption both have been used over the past decade by ransomware families. Based on current enterprise systems, asymmetric (or also known as public key cryptography) encryption has taken precedence as the preferred form of encryption scheme. Using a key pair allows the attacker to implement a C&C center and store the private pair necessary for decryption at a secured server hence meeting the pre-requisite (b). Implementation of standard algorithms (DES, Triple DES, RSA, PGP) in the 90s were not publicly available due to government legislation. Murray, W. H. (2008)

The OpenSSL project began in 1998 which paved the way for attackers to use the methodology first proposed by Young, A., Yung, M. (1996) in their paper. Now multiple free third-party cryptographic libraries exist which are used by criminals for malicious encryption purposes (OpenSSL, mbed TLS, libsodium). The most effective of the current encryption suites are the cryptographic designs involving Elliptic Curve Cryptography (ECC) for shared secret and per-victim key-pair generation. File encryption is performed almost exclusively by Advanced Encryption Standard (AES) with recent ransomware, difference can be pointed only on the chaining mode used. Ransomware authors might use the default setting of the system (MS CAPI). National Institute of Standards and Technology (NIST). (2001)

The scientific paper by Young, A., Yung, M. (1996), demonstrated the concept on a Windows target using Triple DES and RSA implementation with a 1024-bits public-key. This proof of concept is based on public cryptographic services given to userland applications through the Microsoft's Cryptographic API (MS CAPI) framework.

Distribution methodologies

The most common infection vectors used by ransomware attacks have been highlighted below:

- Spam email campaigns that contain malicious links or attachments
- Security exploits in vulnerable software

- Internet traffic redirects to malicious websites
- Legitimate websites that have malicious code injected into their web pages
- Drive-by downloads;
- Malvertisements
- SMS messages (when specific to mobile device);
- Botnets
- Self-propagation (spreading from one infected computer to another);
- Affiliate schemes in ransomware-as-a-service. (author of the ransomware also benefits)
- Social Engineering is employed by Crypto-ransomware attacks via a subtle mix of technology and psychological manipulation.

Source: Mateiu, Monica. (2018)

Out of the list above, the most effective infection vectors to data have been through malicious email attachments, compromised software and drive-by downloads exploit kits. Do-It-Yourself (DiY) malware kits and additional armoring techniques to generate new executable files based on the same code. An infinite number of variants based on an original sample can be generated. Adding an automation component into the mix and it makes it even more deadly. Some ransomware utilize malware factories techniques for automation and morphing code to defeat hash-based signature IDS tools. Cerber is one of the families whose variants are generated every 15 seconds via on the fly server-side malware factories. That's why each new variant is a bit different from its original. Malware creators incorporate new evasion tactics and pack their "product" with piercing exploit kits, pre-coded software vulnerabilities to target and exploit. Zaharia, Andra. (2017).

Payment transaction methodology

Due to traceable methods used by law enforcement during analysis of attack, it was not viable to use ransomware, but the block chain technology resolved that issue. In rare cases, SMS or call to an overtaxed premium mobile number were encountered but carried a huge amount of risk for the attacker and a lot of planning to maintain anonymity. Large-scale attacks or campaigns were limited so as to not attract attention. The new generation of ransomware relies on Bitcoin (BTC),

an application of the Blockchain (i.e. secure virtual ledger-based) technology almost exclusively. Fergal, R., and Martin, H. (2012)
The introduction of Bitcoin has undeniably stimulated ransomware threats for massive attacks due to the following features that were otherwise previously missing leading to chances of traceability:

- confidentiality
- rapid rate of transfer
- absence of central banking group

The Bitcoin protocol was extended in 2014 and can now be used to store 80 bytes not related to the transaction. It is interesting to note that it is not just applicable for payment transfers but also for sending the decryption keys to the victim. The new variant of CTB-Locker uses this field as a side channel to send back the decryption keys once the ransom is paid. Fergal, R., and Martin, H. (2012)

Anonymizing network communication

Communication with Command & Control servers is encrypted and difficult to detect in network traffic; It features built-in traffic anonymizers, like TOR to avoid tracking by law enforcement agencies and to receive ransom payments. Once a user's computer has been infected by TOR based ransomware, the tipoff that the hacker is hiding out on TOR is that part of the ransom message will include a link that ends with ".onion." Often, the hacker will direct the user to a TOR site where they'll be required to pay for the decryption of their files. Beelen, Aubrey. (2016)

The Onion Router uses onion routing to keep a user's activity concealed. This is accomplished through encryption that takes place in the application layer of the TCP/IP stack, not once, but several times. The result is that the user's information is safely encrypted within onion-like layers of insulation. This insulation makes it virtually impossible to track a user's identity or where that user goes on the Internet when using the TOR browsers. Dingledine, R., Mathewson, N. and Syverson, P. (2004).

Malware that needs to access a website in the Tor network utilizes a Tor2web service. These free services enable one to connect to an onion site with a regular browser. They provide a gateway to the Tor network over HTTP or HTTPS and connect to Tor themselves. This way, the malware doesn't need to come with a full-blown Tor client. One of the most popular Tor2web domains is onion.to. A user can basically append the *.to* extension to almost any onion link to access it from the Clearnet. Dingledine, R., Mathewson, N. and Syverson, P. (2004).
As an example, a mirror of The Hidden Wiki can be accessed by using this format in the URL: https://zqktlwi4fecvo6ri.onion.to/wiki/index.php/Main_Page

While Tor2web is straightforward, there are also cases where ransomware prompts victims to download the Tor browser manually themselves and some malware use actual Tor components to obscure their C&C communication. Some of the types of ransomware that utilize TOR are: CryptoWall, CryptoLocker, TeslaCrypt, TorrentLocker, CTB-Locker, Onion Ransomware. They utilize domain shadowing to conceal exploits and hide the communication between the downloader (payload) and the servers controlled by cyber criminals. Beelen, Aubrey. (2016)

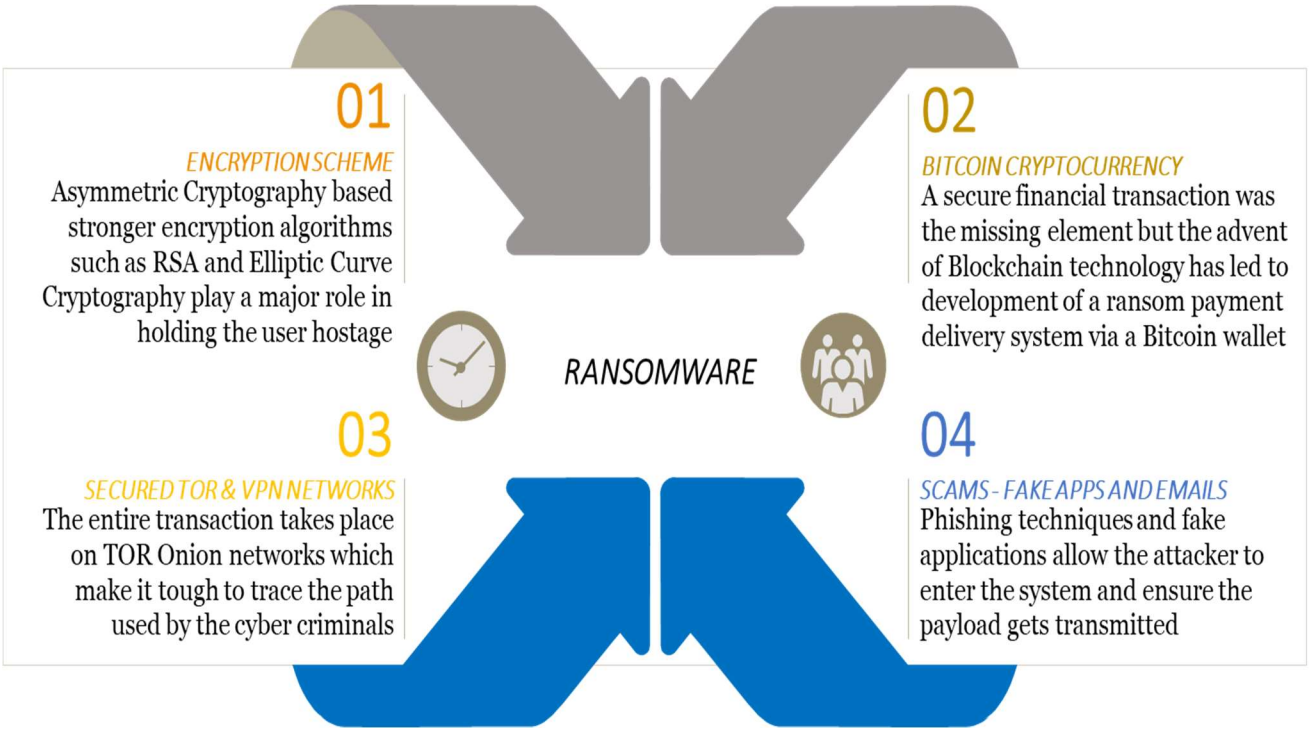

Figure 5 Components of a Ransomware attack

WHAT IS BITCOIN?

Bitcoin provides some unique technical and privacy advantages for the cyber-criminals behind ransomware attacks. Bitcoin itself is a payment system based on a decentralized architecture that provides a mechanism to obtain multiple anonymous credentials, Bitcoin addresses, that can be used to perform and receive payments. Fergal, R., and Martin, H. (2012)

Herrera-Joancomart, J. (2015) has perfectly explained how Bitcoin and Blockchain function in his article, "Research and Challenges on Bitcoin Anonymity." The same has been highlighted below to explain how Bitcoin is a pivotal link in the chain for a Ransomware attack to be executed. A Bitcoin account is defined by an Elliptic Curve Cryptography key pair. The Bitcoin account is publicly identified by its Bitcoin address, obtained from its public key using a unidirectional function. Using this public information, users can send Bitcoins to that address. Then, the corresponding private key is needed to spend the Bitcoins of the account. Regarding this definition, it is easy to understand that any user can create any number of Bitcoin addresses (generating the key pair) either using any standard crypto-software or self-purpose created programs, like Bitcoin wallets. He does call into question the full anonymity of the transaction as it can be traced back. The research performed so far has proven that the way the system uses such addresses may unveil some information from their owners. Since all transactions performed by the system are freely available in the blockchain for analysis, it allows to cluster different addresses of the same user and characterizes some uses. Furthermore, if one of the addresses of the cluster can be mapped to a real identity, then the payment history of the entire cluster may disclose relevant information of that user. Herrera-Joancomart, J. (2015),

Bitcoin transactions are cryptographically signed messages that embody a fund transfer from one public key to another and only the corresponding private key can be used to authorize the fund transfer. A Bitcoin transaction details the exact number of Bitcoins to be transferred from each input address. The same applies to the output addresses, indicating the total amount of Bitcoins that would be transferred to each account. For consistency, the total amount of the input addresses (source of the money) must be greater or equal than the total amount of the output addresses (destination of the money). The Bitcoin protocol forces that input addresses must spend the exact

amount of a previously received transaction and for that reason, in a transaction, each input address can unambiguously indicate the index of the transaction in which the Bitcoins were received. Fergal, R., and Martin, H. (2012)

Before accepting a payment from a standard transaction, the receiver should validate that the Bitcoins of the input addresses are not previously spent and also validate that the digital signature is correct. These validations are kept in check through an unmodifiable, append-only ledger called Blockchain which we will understand more in depth in the next section. Fergal, R., and Martin, H. (2012)

BLOCKCHAIN TECHNOLOGY – ORIGIN OF BITCOIN

The blockchain is a general append-only ledger containing all Bitcoin transactions performed since the system first started to operate in 2009. Such approach implies that the size of the blockchain is constantly increasing (21GB by September 2014) and, for that reason, scalability is probably the biggest challenge that the system faces. The blockchain is freely replicated and stored in different nodes of the Bitcoin network, making the Bitcoin a completely distributed system. Blockchain uses sequential hashing – the data content of transactions in a block has a mathematical function performed on it, to generate a unique 'fingerprint' (hash). The blocks of transactions are linked by the hashes to create a unique history that tests and secures the integrity of the chain every 10 minutes. Fergal, R., and Martin, H. (2012)

According to Constantin, Lucian. (2016), transactions are included in the blockchain at time intervals, rather than in a flow fashion, and such addition is performed by collecting all new transactions of the system, compiling them together in a data structure, called blocks, and including the block at the top of the blockchain. Every time that a block containing a specific transaction is included in the blockchain such transaction is said to be a confirmed transaction since it has been already included in the blockchain and can be checked for double-spending prevention.

Blocks are data structures that mainly contain a set of transactions that have been performed in the system. To achieve the append-only property, an addition of a block in the blockchain is a hard

problem, so adding blocks to the blockchain is time and work consuming. Furthermore, every block is indexed using its hash value and every new block contains the hash value of the previous one. Such mechanism ensures that the modification of a block from the middle of the chain would imply to modify all remaining blocks of the chain from that point to the top to match all hash values. Adding a block to the blockchain is known as the mining process, a process that is also distributed and that can be performed by any user of the Bitcoin network using specific-purpose software (and hardware). The mining process uses a hash-cash proof-of-work system, first proposed by Adam Back as an anti-spam mechanism. The proof-of-work consists in finding a hash of the new block with a value lower than a predefined target. This process is performed by a brute force varying the nonce value of the block and hashing the block until the desired value is obtained. Once the value has been found, the new block becomes the top block of the blockchain and all miners discard their work on that block and move to the next one, by collecting new transactions and taking the hash of the top block as the previous block hash. The Bitcoin system needs to disseminate different kinds of information, essentially, transactions and blocks. Since both data are generated in a distributed way, the system transmits such information over the Internet through a distributed peer to peer (P2P) network. Such distributed network is created by Bitcoin users in a dynamic way, and nodes of the Bitcoin P2P network are computers running the software on the Bitcoin network node. This software is included by default into Bitcoin's full-client wallets, but it is not usually incorporated in light wallet versions, such as those running on mobile devices. Fergal, R., and Martin, H. (2012)

It is important to stress such distinction in a case to perform network analysis because when discovering nodes in the P2P Bitcoin network, depending on the scanning techniques, not all Bitcoin users are identified, but only those running a full-client and those running a special purpose Bitcoin P2P node. We can seal the data within the blockchain transaction fabric with very trusted sources of input. In addition to the above, due to its distributed nature, the system is highly resilient against downtime. All these properties combined make an appealing infrastructure for a wide variety of applications, and indeed explains much of the interest in blockchain technologies. We might end up with a system that is harder to hack, and more reliable to trust than many that we've seen historically. Constantin, Lucian. (2016)

DETECTION OF RANSOMWARE ELEMENTS

Now that the essential elements of a ransomware have been discussed we can now look at what has been done about identifying them on both a reactive and pro-active basis. Ransomware attacks get more refined by the day, as cyber-criminals learn from their mistakes and tweak their malicious code to be stronger, more intrusive and better suited to avoid cyber-security solutions. The WannaCry attack is a perfect example of this since it used a wide-spread Windows vulnerability to infect a computer with basically no user interaction. Mills, Chris (2017)

Every time a new ransomware variant is detected, it gets analyzed thoroughly via cyber forensic tools and added to the signature list of an antivirus software, which helps create a bigger data set to help the new AI-based Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) to identify anomalies at a higher rate of precision. AI seems like an obvious answer for detection and prevention of ransomware and thus we have already seen sophisticated algorithms being added to antivirus and security systems. This will keep getting relevant to the increase in the learning set and a test set of the algorithm making it much more efficient at identifying the elements that constitute a payload for a ransomware. Chen, Y. C. et al. (2018)

To this day, that aspect has only been theoretically discussed and its implementation has lacked the backing of companies active in the industry for commercial reasons. Determining a suitable ransomware detection method and deploying it to add an additional layer of security and to protect the network; actions must be taken based on the knowledge of an attack, Additionally, shutting down a server when a user legitimately updates a collection of files would be a severe response. All the while keeping in mind that not reacting quickly to a ransomware attack would result in more files becoming encrypted. Having said that, the focus to prevent has been largely on software-based solutions and much less on the hardware level. Liska, Allan and Gallo, Timothy (2016)

SOFTWARE LEVEL DETECTION

Behavioral Analysis Based Remediation

Once a device or system is infected, it typically first looks for local files and removable devices such as USB sticks and then looks network shares. A typical solution to slow down the ransomware is to utilize a sacrificial network share; therefore, it will delay the ransomware to reach to the critical data.

According to Kharraz, A. et al. (2015), a more real-time solution for detecting suspicious activity is to utilize file activity monitoring (i.e., the changes in Master File Table and the types of I/O Request Packets to the file system), hence in this way, it is possible to get a historical record of all files and folder activities to detect abnormal file system activity. As an example, some ransomware variants on execution will result in a massive increase in file renames due to the encryption of the data. Therefore, it is possible to trigger an alert in the case of this unexpected behavior.

Kharaz, A. et al. (2016) proposes a dynamic analysis system, called Unveil, which executes applications in an artificial environment and monitors files system activities and desktop interactions to detect anomalies which could indicate the presence of ransomware. Unveil is the first defense system for ransomware which achieved a high detection rate of 96.3%. However, Unveil can also falsely identify high file system acts as a presence of ransomware.

CryptoDrop

Scaife, N. et al. (2016) designed a detection system, called CryptoDrop, which monitors common indicators of ransomware and terminates if a process performs a suspicious activity. In the experiments, the authors show that CryptoDrop could detect all the ransomware families, though, the detection happened after a number of files are encrypted, the median loss is about 10 files out of about 5100 files. It was expected in this study that most ransomware samples perform a depth-first search using ordered lists of directories and upon reaching the deepest files, sequentially encrypt them but that was not always the case.

TeslaCrypt uses a depth-first search. It starts accessing files once it has reached the deepest directory. CTB-Locker, on the other hand, attacks files with certain extensions (.txt and .md) in ascending order by file size. The set of files the samples encrypted before detection was composed of files throughout the file corpus we provided the malware; the sample encrypted the next file in size ascending order regardless of whether it existed in a different directory. This behavior is different from the general strategy employed by ransomware because one might assume that a victim's largest files are the ones that contain the most information and therefore have a higher likelihood of being valuable. There is a high latency from write and rename operations often manifests during measurement. To optimize this factor, it is essential to perform these measurements without additional disk access, heavily reducing these latencies. This tool requires multiple updates to reduce false positives and to allow legitimate files to run like PGP as well as manage detection of variants before a high loss of data. Scaife, N. et al. (2016)

PayBreak - Key Vault mechanism

Kolodenker, E. et al. (2017) 's mechanism, called PayBreak, is the first and only ransomware defense mechanism which monitors calls to crypto APIs and collects the parameters such as encryption keys and type of algorithm.

The Hooking Technique which is one of the relevant principles that enable a ransomware to infiltrate the system by temporarily providing control over APIs that handle crypto functions in a system i.e. the symmetric key (session key) generation. Hooking is a scheme that is used to modify application behavior by augmenting original functions with arbitrary new functionality. In Windows, functions can be hooked by various means, ranging from modifying a processes' Import Ad- dress Table, to injecting DLLs. Kolodenker, E. et al. (2017)
Their prototype utilizes Microsoft Research's Detours library for hooking. Detours hooks a function by first saving a minimum of 5 bytes (the size of an unconditional JMP instruction in x86 assembly) from the beginning of the original function's memory ad- dress into a new hook function. Kolodenker, E. et al. (2017)

Detours creates an unconditional jump instruction that transfers control to the original function skipping over the bytes already saved into the hook function. To activate the hook and redirect control from the original function to the hook function, an unconditional jump instruction to the hook function overwrites the first five bytes in the original function. This completes the hook, and any calls made to the original function will now be redirected to the hook function. CryptoAPI hides sensitive information such as keys and their locations in memory by only allowing operation through a set of subroutines that have special access to it. The security, platform consistency, and API completeness of the CryptoAPI makes it a common choice for local file encryption by ransomware authors. Microsoft's CNG library is the long-term replacement for the classic CryptoAPI. All encryption through the CryptoAPI must be performed via the CryptEncrypt function, or be exported (i.e., for external use) via the CryptExport function. CryptoAPI based ransomware uses the CryptEncrypt function of the CryptoAPI to perform local encryption of files. Because the CryptoAPI is dynamically linked, adding a hook is completely independent of the calling process, and malware obfuscation does not impact this capability. In Windows' case, the supported API to generate a random number is CryptGenRandom, and many crypto- graphic libraries (OpenSSL, NaCl, LibTomCrypt, and more) leverage this API for their cryptographically secure pseudorandom number generator (CSPRNG). Kolodenker, E. et al. (2017)

Working of Key Vault

Kolodenker, E. et al. (2017) further proposes that the system's key vault asserts that symmetric keys used by Microsoft's CryptoAPI and Crypto++are securely stored only to be accessed by the ransom victim when necessary. The details about the symmetric encryption schemes are stored as well.

The key vault system, in this case, is designed similar to the hybrid cryptosystems that ransomware deploys. Session keys are encrypted and exported using the user's public key (PKU) generated during installation of the system. Our implementation uses 2048-bit RSA keys for this step. The large key size of 2048 bits guarantees secure encryption of data in size less than or equal to the key size. A call to CryptEncrypt is augmented with the behavior of the CryptExport function. The auxiliary CryptExport call takes as arguments the handle to a session key that is passed to the

CryptEncrypt function, as well as our system's exchange key (i.e., the user's PKU) to securely export the session key. Keys being used by CryptEncrypt also contain algorithm (i.e., AES, 3DES, RC4, etc.) information, and as such this information is exported as well. Kolodenker, E. et al. (2017)

As a safety precaution to prevent the vault itself from being encrypted by ransomware, the vault is configured to be append-only, and all other access is only allowed to the Windows Administrator group. In the unfortunate event that the key vault requires access, the private key (ski) set up during installation of PayBreak is used to decrypt the key material stored. Kolodenker, E. et al. (2017) claim that their proposal is essentially different from government-mandated key escrow systems by arguing that there is exactly one entity who can access PayBreak's key vault.

Observations on the PayBreak mechanism:

- One of the major drawbacks of PayBreak is that it logs session keys of all running applications in a key vault acting as a key escrow (key recovery) agent. It would be reasonable to expect that key vault would be a valuable target for adversaries and may lead to fatal security or privacy issues once it is disclosed

- A single point of failure would constitute a big risk for enterprises. For instance, TLS, SSH and VPN protocols (which run in Application Level of OSI Model) promise forward secrecy which is contributed by ephemeral keys. Such a key escrow system would diminish that feature.

- A weakness arises when a ransomware downloads a public key from its C&C center and encrypts files directly under that public key instead of a hybrid encryption scheme. Cybercriminals can create such a malware.

- PayBreak also needs to know the signature of the third party crypto libraries to detect and log the parameters, otherwise, PayBreak cannot recover any encrypted file. Signature-based mitigation can be bypassed by using advanced packers and obfuscation methods.

- Zero-day attacks can also be used by ransomware authors to destroy the key vault thus making recovery a lost cause.

Detection of Exploit Kit activity to stop Ransomware infection

Exploit kits are used primarily for drive-by downloads, when a user is unknowingly redirected to a malicious website from a legitimate vulnerable website, or infecting a legitimate website using exploit kits to target a specific group, called a watering hole attack. The agility of exploit kits that are continually evolving to evade detection and taking advantage of new vulnerabilities, mobile devices, and Internet of Things (IoT) to widen their infection campaigns. The exploit kit of choice for cyber-criminals prior to July 2016 has been the 'Angler' exploit kit. However, cyber-criminal group 'Lurk', who had developed and were selling the Angler exploit kit as a service to other cyber-criminals, was arrested in Russia around early June 2016. Burgess, M. and Ieraci, J. (2017)

According to Burgess, M. and Ieraci, J. (2017), Locky ransomware was the most prevalent malware family downloaded in 2016. It is typically delivered in a Microsoft Word document within a phishing email but has also been delivered using exploit kits on infected websites and most recently as JavaScript's inside zip files. Palo Alto found 'Usnif' was also pervasive in 2016. 'Usnif' is a banking Trojan which has been targeting Australian banks with recent variants utilizing the Tor network and typically delivered using phishing emails or via the Neutrino exploit kit (with 21 percent of downloads). Palo Alto experts observed the number of Neutrino sessions increase in late June 2016. This was the result of cyber criminals moving to adopt the Neutrino exploit kit for their criminal campaigns.

The Nemucod exploit kit is a popular delivery method for ransomware and has also been used to deliver a new payload to its victims called Win 32/Kovter that delivers a backdoor to a Command and Control (C&C) server with the ad-clicking capability. Locky ransomware can be delivered using the JavaScript Nemucod downloader malware and is primarily used as an infection vector to plant various families of ransomware onto a victim's computer to encrypt files and demand Bitcoin ransom payments. Burgess, M. and Ieraci, J. (2017)

To detect ransomware attacks from exploit kits¸ Taylor, T. et al. (2016) identified that the utility of using redirects as the main feature to detect exploit kits in traffic by exploring the full packet payload HTTP traces associated with 110 exploit kit instances. Redirection chains were built from each trace by extracting server and HTML (meta tag) redirects. Additionally, we manually analyzed a subset of 50 traces using an instrumented HTML parser, javascript engine(Rhino) and DOM (envjs) to build chains that included javascript redirections. It was found that the traces had relatively short redirection chains, and the length the chain was dictated by the type of exploit kit. Exploit kits such as Blackhole, Nuclear, Fiesta, Goon DotkaChef, Fake, and Sweet Orange consistently had a single indirection to the exploit kit server. Taylor, T. et al. (2016)

It is important to note that server and meta redirections are rare with the main form of redirection being an iframe injection into the compromised site, or a javascript injection that built an iframe. Magnitude, Angler, Flashpack, Zuponic, and Neutrino saw anywhere from 1 to 3 redirects with a combination of server, meta and javascript redirects. In fact, Styx, another exploit kit variant was the only instance that had more than 4 redirects. Taylor, T. et al. (2016)

HARDWARE LEVEL DETECTION

Detecting large arithmetic for Crypto Ransomware

The technique proposed by Kiraz, M. S., Genç, Z. A. and Öztürk, E. (2017) is one of the few researches that provide a hardware level approach to tackle ransomware before it hits the system. Kiraz et all propose a new detection mechanism called EXPMonitor that deals with detection and analyzing rather than prevention. The idea is to observe the public key encryption running on the CPU. Monitoring integer multiplication instructions can detect large integer arithmetic operations, which allows one to detect suspicious activity. Since it is a hardware level fix, it allows a generic solution and thus is OS independent which is unique feature of this idea.

Kiraz, M. S., Genç, Z. A. and Öztürk, E. (2017) critically analyze software detection mechanisms and lay into the PayBreak solution suggested by Kolodenker at length by highlighting that if the public key is taken from a C&C server and encrypts directly instead of encrypting the session keys, then the key escrow system falls apart. Although they acknowledge this hasn't been used yet and would require high amount of computation. A simple overview chart for the EXPMonitor explains the access to the machine code to identify MUX instruction and detect the loops around that instruction and trace them to compute the number of times the large integer was detected and hence save the address to identify the public key. The properties that are brought to light under this mechanism are that

1. Public key cryptography utilizes large integers
2. The code for Public key crypto contains loops which happens because the ratio of operand size to core multiplier is too high, public key cryptographic operations need to perform excessive integer multiplication operations
3. The input and output operands share a relation that is easy to identify

Since, symmetric encryption requires high percentage of bitwise arithmetic instructions, asymmetric encryption requires high percentage of large integer arithmetic instructions, they look at the machine code instructions that need to be monitored and explains mathematical computations that take place while public key encryption is in progress. Kiraz, M. S., Genç, Z. A. and Öztürk, E. (2017)

In elliptic curve cryptography (ECC), the most compute-intensive part of ECC operations is common for all these protocols, i.e., scalar point multiplication. Intel implemented a Carry-Less Multiplication Instruction into their Westmere architecture. This instruction is called PCLMULDQ and it multiplies two 63-degree polynomials (which are represented as 64-bit binary numbers) and results in a 127-degree polynomial (which is represented as a 128-bit binary number). This instruction could be utilized to realize ECC operations and characteristics of this instruction could be utilized to detect ECC operations. Kiraz, M. S., Genç, Z. A. and Öztürk, E. (2017)

In RSA, the most compute–intensive operation for RSA is modular exponentiation and analysis of modular exponentiation algorithm shows that the most time–consuming operation is multi–precision multiplication. Therefore, if one is able to detect code for multiplication of large integers is included in some piece of software that will be run on the CPU, one will be able to detect if the CPU will be running RSA operations and take necessary measures.
Another factor that can be examined to provide better accuracy of whether it is a ransomware, is to look at public key operations, where the integers to be multiplied will be random integers and will have a large Hamming distance. Multi-core systems could be traced via monitoring high- level common cache structures. For example, modern Intel processors utilize L1 and L2 cache structures for each core and a common L3 cache that is shared by all the cores. Thus, any run-time monitoring could be realized via monitoring the L3 cache structure. Since, security focus has largely been on software until major revelations through zero-day attacks cause an uproar, hardware vulnerabilities are suddenly taking forefront and there isn't much research into other mechanisms to tighten security at the hardware level. Kiraz, M. S., Genç, Z. A. and Öztürk, E. (2017),

The Key Reinstallation Attacks (KRACK) in November 2017, showed how one can get into networks by replicating keys and post intrusion one could deploy a ransomware for monetary gain if they so choose to in case the system is about to chuck the malicious user out. Hence, exploiting the hardware through system32 files or Linux kernel-based payloads has become a rising trend and will continue to rise till a major event provides enough reason to change the way hardware is built. Inbuilt security into the hardware will go a long way with prevention of attacks and provide more secure options in the cyber world. Vanhoef, M. and Piessens, F. (2017),

ANDROID BASED RANSOMWARE

A recent change in focus on Android as a vulnerable platform and the growing interest of malicious hackers on portable devices has caused multiple android based ransomware variants to turn up. Double Locker has been in the news as one of the latest Android ransomware attacks to have been recorded by security companies. Most of these attacks utilize the entry points on the embedded software of the operating system used in mobile devices although they have been fairly simple to identify and bad coding behind them make it weak ransomware that can be reasonably dealt with. Whenever an Android device is infected with ransomware, it initially targets administrative privilege by simply asking for it or by tricking the user by showing installing patch updates pop-up. At root level access, it asks for permissions, which are required by an app to perform necessary tasks. The permissions have been granted to the app, it starts gathering information from victim's device and then, it contacts command and control server. It sends this information to the attacker and these messages are usually encrypted with Transport Layer Security. It obtains a private key from command and control server in case of crypto ransomware. Using this key, it encrypts the selected files present on the Android device. Although the locker ransomware performs an extra step, it will reset the PIN of the Android device and then asks for the ransom to restore access to the device. Locker ransomware has been more prevalent in the mobile device domain, making fake claims by portraying themselves as these agencies and then, warn the device users to pay some amount of money as a fine for violation of the law. The ransomware analysis of the infected Android applications in this paper mainly focuses on *AndroidManifest.xml* and the source code of an application. Yang, T. et al. (2015)

During its information-gathering process, ransomware applications collect information like IMEI number, call logs, contacts, profile, history bookmarks, SMS, the list of accounts in account service, phone state, GPS location of the phone, and IP address. Some of the ransomware even check the tasks running on the device. Simplocker family contacts Command and control server and sends the information found on the mobile device to the attacker. Yang, T. et al. (2015)

During installation as a rogue application, on opening the app, it asks for administration rights. Once the user clicks on activate button, the application takes the privileges of device administrator,

and this makes difficult to remove the malicious application from the device. In the recent versions of ransomware attacks, the activation window is overlaid with a malicious window pretending to be an Update patch installation. The application then tries to obtain the administrator privileges to lock the victim's device or to set a new PIN for lock screen of the device. An application that tries to make a secure HTTP request to a suspicious target is a clear hint of malevolent purposes. The upcoming new variants use XMPP communication to communicate with the C&C server. These communications look like normal instant message communications, which makes the ransomware even harder to get detected with anti-malware software. Yang, T. et al. (2015)

According to Monika, Zavarsky, P. and Lindskog, D. (2016), XMPP communications channel is used by the new Simplocker variants. Its variant uses an external Android library to communicate with the command and control network through a legitimate messaging relay server. And these messages can be encrypted using Transport Layer Security (TLS). The messages are received from the command and control network by the operators of the scheme via Tor. We observed that all communications to C&C server are done through port numbers 443, 80 and 123.
Crypto ransomware like Simplocker and Pletor use AES encryption scheme to encrypt the data present in SD card. It usually searches for specific types of files and then encrypts them
All the permission requests which don't seem to be in accordance with app services
can be taken seriously and may not be granted. Savage, K., Coogan, P. and Lau, H. (2015)

Common permissions that android based ransomware asks for include the following:

- *READ_PHONE_STATE* - Allows read-only access to phone state
- *INTERNET* - Allows applications to open network sockets
- *ACCESS_NETWORK_STATE* - Allows the app to access information about networks
- *WRITE_EXTERNAL_STORAGE* - Allows an application to write to external storage
- *READ_EXTERNAL_STORAGE* - Allows an application to read from an external storage
- *RECEIVE_BOOT_COMPLETED* - Allows an application to receive the below command
- *ACTION_BOOT_COMPLETED* - Broadcast after the system finishes booting
- *ACCESS_COARSE_LOCATION* - Allows an app to access approximate location
- *ACCESS_WIFI_STATE* – Allows the app to access information about Wi-Fi networks

- *ACCESS_FINE_LOCATION* - Allows an app to access precise location
- *WAKE_LOCK* - Accesses Power Manager Wake Locks to keep processor from sleeping
- *INSTALL_SHORTCUT* - Allows an application to install a shortcut in Launcher
- *GET_TASKS* - Allows an application to get information about the currently running tasks
- *CALL_PHONE* - Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call

There are very distinct permissions that are also sometimes identified during analysis of the ransomware used in scenarios where the malware containing application permanently wishes to embed itself into the device. An app utilizes permissions like *KILL_ BACKGROUND_PROCESSES* to stop the antivirus processes running in order to prevent ransomware from detection. *FACTORY_TEST* is used to run an app as manufacturer test application using root user privileges. *BIND_DEVICE_ADMIN* ensures that only the system can interact with an application. These kind of permissions makes ransomware much more malicious and removal of these ransomware apps from Android devices becomes much more difficult. Yang, T. et al. (2015)

Historical review of Android Ransomware

In the case of Android, the first locker ransomware appeared in 2012, which was detected by antivirus engines as Genric.17.1762. In 2013, LockDroid, Kovter, Sypeng, and Pletor arrived. In 2014 Simplocker, Koler, ScarePackage, ScareMeNot, ColdBrother, Jisut, Locker, LockerMaster and many variants of LockDroid came into existence. In 2015, Lockerpin, FakeInst, SMSSend, Agent, HiddenApp, Slocker families started surfacing all over the Android devices. Monika, Zavarsky, P. and Lindskog, D. (2016)

The first crypto android ransomware, as explained by Savage, K., Coogan, P. and Lau, H. (2015), Simplocker, came in 2013. It uses AES Encryption to encrypt files. Crypto ransomware like Simplocker and Pletor encrypts files present on Android device's memory card. Simplocker family malware scans the SD card and searches for files with jpeg, jpg, png, bmp, gif, pdf, doc, docx, txt,

mp4, mkv, avi and then uses AES algorithm to encrypt these file's data. First spotted in May 2017, DoubleLocker Android ransomware started spreading as a fake Adobe Flash update via compromised websites. DoubleLocker is the first-ever ransomware to misuse Android accessibility—a feature that provides users alternative ways to interact with their smartphone devices, and mainly misused by Android banking Trojans to steal banking credentials Once executed, DoubleLocker first changes the device PIN to a random value that neither attacker knows nor stored anywhere and meanwhile the malware encrypts all the files using AES encryption algorithm. DoubleLocker ransomware demands 0.0130 BTC (approximately USD 74.38 at time of writing) and threatens victims to pay the ransom within 24 hours. If the ransom is paid, the attacker provides the decryption key to unlock the files and remotely resets the PIN to unlock the victim's device. Monika, Zavarsky, P. and Lindskog, D. (2016)

In July 2017, a new variant of Android ransomware called LeakerLocker entered the fray, with a completely distinct threat to unsuspecting mobile users who downloaded certain applications from the Google Play Store. It threatens to send the victim's private information and web history to all their contacts has been discovered in the official Google Play app store. LeakerLocker doesn't encrypt the victims' files but instead claims to have made a backup of data stored on the device and threatens to share it with all of the user's phone and email contacts. The ones behind the malware demand $50 in exchange for not leaking personal data including photos, Facebook messages, web history, emails, location history and more, playing on fears of potential embarrassment rather than any form of cryptography. Two applications in the Google Play Store contained the malware, Wallpapers Blur HD, which has been downloaded between 5,000 and 10,000 times, and Booster & Cleaner Pro, which has been downloaded between 1,000 and 5,000 times. The combined number of downloads means that up to 15,000 people have fallen victim to this ransomware, which has been in the Google Play Store since at least April. Both apps have good review scores, suggesting that those behind the scheme have been giving them fake reviews. The reverse malware analysis of the code shows it's capable of at least accessing an email address, some contact information, Chrome browser history, text messages and calls, and photos from the camera. Snippets of this data are chosen at random to convince the victim that all their data has been copied -- although at this point the information hasn't actually been copied, there is a chance it could happen if the control server issues relevant instructions. This basic form of ransomware

demands the ransom via credit card, although researchers advise infected victims not to pay because there's is no guarantee that the information will be released or not used to blackmail victims again. Monika, Zavarsky, P. and Lindskog, D. (2016)

How do Android apps work? – In a nutshell

Android apps are generally written in the Java programming language and have four types of components:
(1) Activities represents a single screen with a user interface.
(2) Services is a component that runs in the background to perform long-running operations or to perform work for remote processes.
(3) Content providers manages a shared set of app data.
(4) Broadcast receivers are a component that responds to system-wide broadcast announcements
Source:
Android Developers (2018) explain that three of the four component types except content providers are activated by an asynchronous message called **intent**. Android intent binds individual components and associates them with others whether the component belongs to the app or not another. The other component type, content provider, is not activated by intents. Rather, it is activated when targeted by a request from a *ContentResolver.*

Yang, T. et al. (2015) identify that Android apps have a manifest file to declare all its components. This manifest file also contains user permissions, the app requires and minimum API level. Therefore, manifest file can be thought as a catalog of android application, and it plays a decisive role in android detection. *DeviceAdminReceiver* and *DevicePolicyManager* are two major classes one needs to pay attention to. *DeviceAdminReceiver* is an *onReceive()* method return operations based on different actions. *DevicePolicyManager* is a public interface for managing policies enforced on a device, especially for the locker. Most clients of this class must have published a *DeviceAdminReceiver* that the user has currently enabled.

Detection of Android Ransomware

Analysis or detection in this section can be conducted in two ways as there is a way to handle different components in the process flow of installing applications on a mobile device. Static Analysis can be conducted at the very first step, i.e. thorough scanning of APK file to detect changes made in terms of malicious code. An APK file contains important information. META-INF directory stores signature data and is used to ensure the integrality of APK package. Res directory is used to store resource files such as images and UI layout. Manifest file describes the name, version, permissions, library files, and other information. *Classes.dex* is a java byte file and can be decompiled on Java or another programming language. A Resource is a binary resource file after compilation. Thus, we can obtain useful information from APK file to detect malicious apps. Malicious apps have different types. Some of them use similar hacking techniques and are called a malicious family. Android Developers (2018)

These malicious families can be identified by feature matching. The four primary features to look at include:

- Permissions: Malicious application also needs permissions to execute malicious functions. For examples, some malware utilizes SMS to send out sensitive data and this malware contains SEND_SMS permission in manifest file.
- Sequence of API invoking: One can decompile Classes.dex to Smali emulation and recall the sensitive API to extract the sequence of method invoking.
- Resources: Some Android applications have executable files that are encrypted to disguise into becoming resources files and the encryption executable file will be executed when the malware is running.
- APK structure: Because of the specificity of APK structure, APKs would be easily repackaged and released. One can use package name and signature and compare with the official application to verify repackaging.

Having mentioned the initial steps for static analysis, it cannot deal with the situations involving code obfuscation and encryption, hence, dynamic analysis is essential. Dynamic analysis is needed to monitor the behaviors of the running application and detect whether the behaviors match the

malicious activity or not. Tools like LogCat can help in log monitoring and recent accesses to permissions can help identify if an application is utilizing access for malicious purposes at which point it is clear that it is infected. Bypassing permissions and untrusted domain names are key features of dynamic analysis. Stolen data by malware would send user's information to a specific domain. Zombie and Trojans malwares would send to C&C server to get commands. Also, while conducting dynamic analysis, we can track the destination of SMS and Call. If there is an unknown destination, the software would be considered as a malware. There has been some research done on offline detection. Mercaldo, F., Nardone, V., Santone, A., Visaggio, C.A. (2016) utilize a model checking approach to identify the malicious payload in Android ransomware. They analyze Java Byte Code to construct Formal Models and formulate logic rules to detect real-world dataset ransomware samples.

HelDroid is a detection tool that utilizes a text classifier that applies linguistic features to detect threatening text. It uses a fast Smali emulation to detect locking capabilities and identifies the presence of encryption by using taint analysis which is computationally demanding. Their solution to detect encryption is limited to the android well-defined API and a malware author could easily evade the system by using native code. Another tool, R-PackDroid demonstrates the possibility of detecting ransomware by only extracting information from system API packages. Andronio, Nicoló & Zanero, Stefano & Maggi, Federico. (2015)

In terms of online detection, Song, S., Kim, B., Lee, S. (2016) propose dynamically monitors read and write accesses to the file systems. This technique can detect and stop ransomware having abnormal CPU and I/O usage. The proposed method can detect modified patterns of ransomware without obtaining information about specific ransomware families. The main weakness of this approach is that it cannot detect ransomware with threatening text and when locking takes place.

One of the best works done so far in terms of detection is the approach based on Deep learning techniques which involve hidden layers for better correlation-based analysis. DNNs are one of the more recent and promising section of AI utilized to fuel more sophisticated and intelligent learning by the system. Chen, Y. C. et al. (2018)

B, A. Gharib. and Ghorbani, A. (2017) in their paper stress on how the few approaches that have come up in the mobile sector, are focused on static analysis and adding a dynamic analyzer on top of the static analyzer can solidify the framework even more. They introduced a bi-layered framework called DNA -Droid, a real-time hybrid detection framework to manage issues like low accuracy and high false positives in presence of obfuscation or benign cryptographic API usage that is faced by most current solutions. It utilizes a dynamic analysis layer as a complementary layer on top of a static analysis layer. They identify DNA-Droid to have three components, where, to specifically note in the static module, they talk about APM (API calls and Permission Module). The end product is an Android sandbox with all the features added and is available to researchers publicly as a web service. Its static module consists of a Text Classification Module wherein performing linguistic analysis on strings can reveal extortion behavior of ransomware. Ransomware shows itself in payday by notifying users that the device is infected and requesting a specific amount of ransom. This notification is usually done through text messages. For each category of notification messages, a bag of words is constructed and term frequency-inverse document frequency (tf-idf) is used to remove insignificant words from each bag. B, A. Gharib and Ghorbani, A. (2017)

DNA-Droid extracts strings by parsing the disassembled APK. To clean the strings, the TCM removes meaningless words/stop words (e.g., to, the, or) and then lemmatizes the remaining words (e.g., locking and locked are replaced with lock). There is an Image Classification Module in this framework that compares application images with this collection using the Structural Similarity Index Measure algorithm (SSIM) and reports the number of detected images as a feature. The API calls and permissions Module identify the permissions granted by the user upon app installation. The APM extracts the list of permissions from the AndroidManifest.xml file and by decompiling an APK, we obtain a list of API methods. Due to a large number of Android APIs and permissions, the APM considers only APIs and permissions with the highest information gain between malware and benign apps. B, A. Gharib and Ghorbani, A. (2017)

Shallow machine learning algorithms such as Support Vector Machine (SVM), Random Forest (RF), and Decision Tree (DT) have been extensively applied in malware detection. Deep learning

has shown better performance in classification by learning new features using hidden layers. Chen, Y. C. et al. (2018)

To use deep learning, we first push features into the Deep Auto Encoder. It can be a challenge at times to decide on the number of hidden layers and nodes. Choosing the number of hidden neurons is the main concern. Using too few neurons will result in under-fitting and using too many neurons can result in over-fitting and increased time overhead. For a test set, this is a critical problem as one doesn't want false negatives to increase lack of a balanced test set. Several supervised machine learning approaches have been used to compare the efficiency of the proposed designs. Chen, Y. C. et al. (2018)

The proposed system consists of a dynamic module that defines the dynamic behavior as an API call sequence to differentiate benign and malicious samples. In the training phase, dynamic module profiles malware families based on the API call sequences and produces a DNA for each family. In the detection phase, run-time behavior of a suspicious sample is continuously compared with families' DNA and will be terminated if the sample is matched with a DNA. The DNA-Droid real-time detection module shows a high capability to detecting ransomware activity in early stages before the infection happens. In addition, we provide a publicly available dynamic sandbox, which allows users to submit a sample and receive a report on its dynamic behavior.
B, A. Gharib and Ghorbani, A. (2017)
Static analysis implementation of the DNA-Droid mostly used shell and Python scripts. It uses Apktool to decompress and decode APKs and Natural Language Toolkit (NLTK) to extract linguistic features. Machine learning tasks including preprocessing, dimensionality reduction, training and testing phases are carried out through Scikit-learn and Tensorflow libraries. Dynamic analysis implementation consists of a modified emulator, an Android application to hook API calls (written in Java), and python scripts to control the emulator and apply MSA and BSA techniques
It is important to note that malware authors usually inject malicious code into popular benign apps and distribute them through the markets. Therefore, malware samples within a family might show different behavior in general but all of them contain the same malicious behavior containing the same set of malicious API calls invoked from the malicious part. B, A. Gharib and Ghorbani, A. (2017)

RANSOMWARE MITIGATION AND RESPONSE

Over the years, based on the level of security awareness and preparedness, the public has reacted to a ransomware infection in much the same way. Most of these have resulted in a payment of the ransom due to widespread panic and no other alternatives to handle the situation.

Ideally, one should never pay the ransom and any decision to pay a ransom should be based on a Risk vs. Benefit analysis and with the understanding that while many users have reported success in getting their files back after paying a ransom, there are no guarantees that if a ransom is paid, an organization will receive the necessary keys to decrypt the affected files. I. B. M. and Incident Response Services (2016) highly recommended that an organization first consider their internal backup infrastructure as a way to recover important files before considering paying a ransom. If backups are not available, then the relevant stakeholders within the organization should be involved in any decision to pay a ransom. In case of infections, there are going to be costs associated with recovery, such as hiring external incident response capability to help determine root cause and/or bolster internal incident response, capital and operational expenditures required for both security and IT staff to work around the clock to bring systems back to operational status, etc., There are numerous quantitative/qualitative damages attached when becoming a victim of such an attack. I. B. M. and Incident Response Services (2016)

While conducting a Risk vs Benefit Analysis, the following questions need to be answered first –

- What is the organization's threshold for an acceptable loss of data?
- Are the local backups viable, or has everything in the tape library or SAN been erased or otherwise been made unviable?
- If the data in the tape library or SAN has been erased or is no longer viable, are the off-site backups available?
- How often are backups sent off-site? Once a week, Bi-Weekly, Monthly?
- How critical is the data?
- What is the total revenue loss the organization would incur from the loss of data during that time frame in which backups are not available?

- Is there a way to manually restore that data?
- How much would a manual restoration cost?

Source: I. B. M. and Incident Response Services (2016)

NIST Incident Response Life Cycle

Cichonski, P. (2012) identifies in the NIST publication that the NIST Incident Response Life Cycle is a good and effective framework if followed and executed properly. The first step is essentially the most important step. Preparation in terms of recovery and contingency plans go a long way in responding effectively to an incident especially in the case of Ransomware infections. It is important to utilize a defense-in-depth strategy; several preparatory prongs are essential in confronting ransomware and ensuring it never has the opportunity to infect the environment. The risk is even more with the evolution of ransomware variants where they don't require administrative privileges to encrypt and also self-propagate onto the other devices on the network which makes it harder to completely eradicate and a complete overhaul becomes necessary. Cichonski, P. (2012)

On an enterprise level, it is recommended to have periodic training for end-users on the types of threats they are likely going to encounter and what actions they should or should not take on an information system while performing their jobs. Organizations should adopt an aggressive patch management policy, especially with browser vulnerabilities such as Adobe Flash and Java that are used by a large population of employees. Patches should be applied on a timely basis. The recent Adobe patches for ransomware are to be applied "as soon as possible" and Adobe defines this time period as within 72 hours due to its products being utilized primarily as attack vectors by malicious authors. Cichonski, P. (2012)

In the case of ransomware, increasing DNS visibility, sinkhole and web filtering capabilities is feasible in the long run. Initial DNS resolution by the malware relies on the domain generation algorithm (DGA). This makes blocking known bad domains much more difficult since it has the ability to generate and use thousands of different domain names to reach the command & control server. Keeping track of blacklisted IPs, domains and sites, in general, is a never-ending job. Next-

generation firewalls and proxies rely on real-time reputation feeds that crowdsource intelligence information and help protect organizations by implementing known bad destinations quickly, providing rapid blocking capabilities when sites have been discovered as having malicious content. The principle of least privilege is extremely valid due to the use of permissions available to the user by the ransomware. Only grant the permissions necessary into folders each user may require in order to perform their daily job. Since an infected computer operates with the permissions of the user currently logged on, it can only traverse and encrypt files it has read & write access to. If a user does not require read/write access to various network shares, consider removing, at a minimum, write permissions from the locations that are not required to be accessed by users for a routine business need. Cichonski, P. (2012)

Disabling unnecessary processes and plugins

The use of JavaScript or VBScript by ransomware (and other malware) has been increasing over the last few years. This has been used by the malware authors because Windows Scripting Host (WSH) is enabled on all Windows systems by default. However, many organizations do not use it or use it sparingly. This allows a large attack vector for the ransomware authors to use and abuse, leading to a high chance of the malware-dropper script being successful and starting the ransomware ball rolling to its file-encrypted conclusion. This can be centrally prevented via Group Policy. Liska, Allan and Gallo, Timothy (2016). Create the following registry key and value:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings\ Enabled and set the 'Value data' field Enabled to '0' (That is a zero without the quotes)
Service providers can also provide customer awareness programs to make sure they aren't susceptible to a ransomware infection via phishing techniques. The same can be done for Adobe Flash plugins as it is a major spoofing attack and infection vector. Should a business case exist for select users to use Flash, said uses may benefit from additional safeguards (e.g. dedicated high-risk network segmented from the organization). Liska, Allan and Gallo, Timothy (2016)

Containment and Isolation Strategy

Once a system has been identified as potentially having ransomware, the potentially infected computer should be immediately removed from the networks (including Wi-Fi), and either shut down or ideally hibernated (to assist in forensic and sample analysis) to minimize the risk of the ransomware continuing the encryption process. Failure to quickly isolate the system from the network may contribute to the incident by allowing the malware to continue to encrypt files on the local system and/or network shares, thus increasing the recovery efforts the organization will need to take. I. B. M. and Services Incident Response (2016)

For enterprises, if the organization cannot quickly determine the source of the ransomware and encryption process, as a last resort the organization should consider taking the file share(s) offline to help minimize the risk and impact to the business. The file server(s) do not need to be shut down, but all access to the file shares should be terminated (remove the share, restrict by network or host-based firewall ACL, etc.). It is not recommended to change permissions on the files within a share in an attempt to restrict access since depending on the number of files, permission propagation could take hours and would allow the encryption process to continue during this time. A comprehensive Root Cause Analysis can help in identifying whether the ransomware arrived via a web browser exploit, in that case, those sites should be blocked and monitored. The organization should then assess the need to update/remove any vulnerable browser components. Passwords for affected users should be changed as a precaution. I. B. M. and Services Incident Response (2016)

Cyber Insurance Policy – Ransomware Claim

It is an upcoming trend and more companies are starting to see the need for having an insurance policy in place to make sure they are able to handle the damage to cost and minimize financial losses. As a part of the recovery process, the company may file a cyber insurance claim, if they

have a cyber insurance policy. Cyber insurance is relatively new and requires multiple iterations before it is stable enough to avoid loop holes. Wagner, William C. (2015)

There are a number questions that have to be considered here while handling a ransomware incident:

- Will the cyber insurance provider validate the claim?
- Will they find that the victim has been negligent?
- Is there a rider on the policy to cover ransomware or "cyber extortion"?
- Does cyber insurance cover the cost of paying criminals the ransom demanded to regain access to locked data?
- If reliable backups are available, should companies try to recover data from backups first, even if would be less expensive to pay a ransom?
- Will the policy be sufficient cover the damages?

Losses that can be expected following a ransomware attack fall into several categories, including business interruption, as well as the costs associated with removing infections from machines (which can be substantial) and recovering data that the ransomware makes inaccessible. The answers to some of the questions mentioned above can at times be straightforward or complicated based on the incident and the situation as a whole.
Wagner, William C. (2015) mentions that in the event of a ransomware attack, victims talk over the possible course of action with their insurers. Most policies would cover paying a ransom, but they would pay the money to the client – insurers wouldn't want to get involved with criminals directly. The insurance company would ideally first want a company to do everything they can from an IT perspective to get data back first. Paying a ransom would be the last resort because of the concern that the criminal would then come back with another attack.

In most cases, the cyber insurance policy is either insufficient to provide full coverage or didn't attach an appropriate policy rider to cover specific damages and more often than not the customers of the company are the ones worst affected. Many standard cyber policies that insure cyber extortion do not expressly contemplate covering a ransom demanded in Bitcoin or other

cryptocurrencies. In those cases, insurers may deny coverage, using the policy's silence to their advantage, thus setting the stage for a coverage battle. But a proactive policyholder can avoid that. Many insurers will amend their standard policy forms to explicitly cover ransom demanded and paid in a digital currency. But companies need to ask for it.

According to Ismail, Nick. (2017), cyber policies provide a limit of liability, but certain types of coverage, like cyber extortion, are often subject to much lower sub-limits. A sub-limit of $50,000 for cyber extortion may suffice for some companies, but be wholly inadequate for others. Rather than being surprised by the amount of any sub-limit after the ransom demand is made, companies should purchase insurance eyes wide open and confirm that any sub-limits are consistent with their risk tolerance. In the same vein, cyber extortion coverage often extends to credible threats by a hacker to enter a company's network, shut down its website, or infect its computer systems unless a ransom payment is made. Cyber insurance coverage for ransomware provides the same critical components offered by kidnap and ransom polices. If and when a cyber extortion threat is made, companies are expected to respond immediately. But in the chaos of the moment, insurance cannot be forgotten. Most insurance policies require immediate notice of cyber extortion threats or ransom demands. And many policies will require the insurer's consent to any ransom payment – whether in Bitcoin or otherwise – for it to be covered.

A typical step by step procedure for invoking the policy during ransomware incidents would include:

- Providing the background knowledge into ransomware attacks that allows the victim organization to make an informed business decision whether to pay. For example, an understanding of the attacker - are they likely to be cooperative; the time it will take to decrypt crucial data even if a ransom is paid; and the amount of corruption that has been caused by the attack that will remain even if a ransom is paid
- Carrying out due diligence on the attacker to confirm that the ransom payment is not in breach of anti-money laundering or anti-terrorist laws
- Professionally negotiating with the attacker in their native language, shielding the victim's identity, and avoiding the discussion from becoming personal. Once the business

decision is made to pay a ransom (and sufficient due diligence has been carried out), the sole aim of the process is to get the victim's system restored as quickly and efficiently as possible

- Being able to make immediate payment of the ransom in the relevant crypto currency (usually Bitcoin or Ethereum)
- Providing a road map for the process to avoid the same outcome again. Paying the ransom and restoring the data does not mean that the system is secure or that the vulnerability that caused the incident has been identified or remediated. Even if the specific attacker has moved onto other victims, literally thousands of attackers are waiting to test the same vulnerability.

Source: Wagner, William C. (2015)

Therefore, companies' response plans must incorporate cyber insurance, starting with an understanding of the policy's notice requirements.

Mitigation via Software Defined Networking

Cabaj, K. and Mazurczyk, W. (2016) in their paper propose the utilization of the SDN paradigm to provide network security in a more efficient and flexible manner. OpenFlow which is used parallelly with SDN has become the de facto standard that implements the SDN paradigm. It is a protocol that allows networking devices, such as switches and routers, which rely on internal flow tables, to be managed by an external controller.

The SDN paradigm is able to identify crypto ransomware and disrupt access by monitoring flow tables and DNS identification. The experimentation by Cabaj, K. and Mazurczyk, W. (2016) was majorly done on CryptoWall and Locky ransomware which helped define two applications called SDN1 and SDN2. Both rely on an up-to-date database of malicious ransomware proxy servers.

The main functionality of the first application (SDN1) was associated with a simple layer 2 learning switch. The SDN application forces the switch to forward all DNS traffic to the controller by adding custom crafted flows to the switch during the initialization of the application. As a result, each DNS message is inspected, and all responses are sequentially evaluated with the remote database (containing the list of known proxy servers used for ransomware purposes). If the domain

name extracted from the DNS message exists in the database, the response is discarded and never reaches the infected host, and thus the encryption process will not be performed. In the other case (i.e., when the domain is not listed in the data- base), no additional actions are performed. When even a single blacklisted proxy server is detected, further communication from this host is not possible, that is, it is completely blocked, and an alert is sent to the system administrator. Cabaj, K. and Mazurczyk, W. (2016)

The second application (SDN2) was developed by Cabaj, K. and Mazurczyk, W. (2016) to further enhance the performance of the first application. The potential drawback of SDN1 is that DNS traffic from legitimate and infected hosts is delayed, as for each DNS query the response message is checked with the blacklisted domains database. In the majority of cases there will be no match, and the additionally delayed DNS request will be forwarded to the recipient. The SDN2 application solves this problem by introducing custom flows, which forward the DNS query to the intended recipient and only its copy to the controller. This way no additional delay is introduced. While the DNS query is processed, the SDN controller evaluates the extracted domains against the database. If a hostile domain is detected, the associated IP address is extracted and used to prepare the flow responsible for blocking the traffic between the victim and the C&C server. This flow is then installed in the switch using the OpenFlow protocol. With the extensive utilization of Software Defined Networking in multiple organizations, this seems to be a viable measure to disrupt the connection between the C&C server and the machine to stop encryption, which makes it more a mitigation strategy than a full prevention scheme but additional research in this domain is possible to add that utility in the future. Cabaj, K. and Mazurczyk, W. (2016)

Recovery and Removal Strategies

The first step during an infection is to first isolate all infected systems and the network that might have been compromised. The victim computer should be shut off immediately since the likelihood is that the malicious process is currently active and still going through the various folders on the local (and possibly network) drives and rendering them inaccessible. The system should be turned off immediately and IT security staff should be notified. The system should not be turned back on otherwise the encryption process will continue and may complete, rendering all user files

inaccessible. Network segmentation helps in preventing compromise in different zones. Once the isolation is complete and thorough analysis of all other parts of the network as well as connected devices is finished, the green signal to move forward with recovery is given. It is essential to make sure that the recovered files are not infected or there is any lingering threat, therefore, a complete forensic analysis is of critical importance. I. B. M. and Services Incident Response (2016)

Backups

The primary way that organizations recover after being hit by ransomware is by restoring systems from backups. However, restoring all systems can take days, and changes since the last backup before the attack will be lost. But investigate thoroughly so one knows when the data was tampered with, so one can make sure they restore from an unaffected backup instance. Offline backup servers stored in different isolated locations is an essential measure that is carried out to make sure that if the on-site backup is also affected and compromised, there is an alternative restoration point available. Decryption tools don't always work so it is always wise to make additional backups. Whether or not backups are compromised depends on how well backup systems and/or network and/or recovery sites are sufficiently segmented from the main network. Even in the event where the organization does not utilize on-site backups at all, instead opting for cloud backup solutions (e.g. Amazon Glacier), if those cloud backup credentials are left in easily accessible locations, or if passwords are reused, our hypothetical adversary could easily delete all backup instances, resulting in 100% data loss if there is no other backup solution in place. The secure, off-site, enterprise backup solution could easily be defeated through password reuse and/or poor password management. Preston, Curtis W. (2018)

Version Restores

In some cases, it may be possible to restore files on individual systems using a built-in file versioning service like Windows Volume Shadow Copy. This keeps the version history of all files on a drive and makes it possible to "go back in time" to restore them to their unencrypted state. However, newer ransomware variants are able disable this capability, so it cannot be relied upon. I. B. M. and Services Incident Response (2016)

Decryption Tools

The **'No More Ransom'** initiative -- launched in July 2016 by Europol and the Dutch National Police in collaboration with a number of cybersecurity companies including Kaspersky Lab and McAfee -- offers free decryption tools for ransomware variants to help victims retrieve their encrypted data without succumbing to the will of cyber extortionists. Initially launched as a portal, it offered decryption tools four for families of ransomware -- Shade, Rannoh, Rakhn, and CoinVault -- the scheme is regularly adding more decryption tools for even more versions of ransomware including Crypt XXX, MarsJoke, TeslaCrypt, Wildfire and Nemucod. The portal -- which also contains information and advice on avoiding falling victim to ransomware in the first place -- is updated as often as possible in an effort to ensure tools are available to fight the latest forms of ransomware. No More Ransom Project. (2016)

The No More Ransom Project. (2016) has grown from offering a set of four tools to carrying 52 decryption tools covering hundreds of families of ransomware. So far, these tools have decrypted tens of thousands of devices, depriving criminals of millions in ransoms. The platform is now available in over 29 languages with more than 100 partners across the public and private sectors supporting the scheme.

In some ransomware variants, the encryption process has not been competently implemented, providing an opportunity for data to be recovered. As an example, the Linux.Encoder1 ransomware has a flaw in the way the encryption key is generated, allowing the key to be derived from a file's timestamp. Security firm Bitdefender has released a decryption tool that automatically generates the keys and decrypts files. Individual security companies also regularly release decryption tools to counter the ongoing evolution of ransomware -- many of these will post updates about these tools on their company blogs as soon as they've cracked the code. For example, another decryption tool was recently released which may be able to help if the PC has been hit by one of the original versions of the Petya malware -- the Red Petya, Green Petya, and GoldenEye -- and may enable users to recover the lost files (although it can't help with PetrWrap or those hit by the Petya/NotPetya global attack).
No More Ransom Project. (2016)

More recently, Kaspersky Labs has discovered a flaw in the Xpan ransomware and will provide help decrypting files. The company has not released a decryption tool, perhaps to avoid alerting the ransomware authors to the flaw in their encryption implementation. Kaspersky Lab (2016)

Android based Recovery

For rooted Android devices with debugging mode enabled, victims can use Android Debug Bridge (ADB) tool to reset PIN without formatting their phones. The best solution is to have a good backup process — one that utilizes industry best practices, such as ensuring that not only local backups are done, but that backups are also archived to removable media (tapes, optical disks or removable hard disks). All passwords should be updated periodically, and two-factor authentication should be activated to prevent access. Remote access should not be enabled.
Song, S., Kim, B., Lee, S. (2016)

RANSOMWARE PREVENTION

Employee Awareness programs

With email being by far the most popular attack vector for ransomware, one should provide employees with training on how to spot an incoming malware attack. Even picking up on little indicators like poor formatting or that an email purporting to be from 'Microsoft Security' is sent from an obscure address which doesn't even contain the word Microsoft within it might save the network from infection. The same security policies that protect the user from malware attacks in general will go some way towards protecting the company from ransom demands too. Raising awareness about ransomware by educating staff about the dangers of clicking on attachments or links in emails is clearly important as a baseline security measure. But it only takes one employee to lower their guard on one occasion for an organization to be compromised, and for that reason staff training should not be relied on. There is plenty of evidence to suggest that the effects of a training session wear off over time, but companies such as PhishMe provide technology to help

keep employees on their toes by sending them simulated malicious emails on an ongoing basis; if an employee clicks on a simulated malicious link, they get feedback to help ensure that they don't fall victim to a similar email again. I. B. M. and Services Incident Response (2016)

System Hardening

It's a basic security precaution to ensure that all software is patched and updated with the latest security patches, but it's worth reiterating because a security risk report from HP in 2016 found that 44% of successful ransomware attacks were caused by software that had not been patched for between two and four years. Privilege escalation is often possible by exploiting known but unpatched vulnerabilities. The 2017 WannaCry strain took advantage of an unpatched Microsoft Windows vulnerability. Mills, Chris (2017)

Security solutions

PhishMe and Wombat Security are two vendors offering anti-ransomware solutions. The security providers should have their software inbuilt with services that can combat ransomware. This includes next-generation firewalls, email gateway security software, data loss prevention systems and endpoint antivirus software, which should be capable of the following:

- Preventing users from visiting malicious web pages: Security software should be able to unmask URLs, so users know what page they are visiting and retrieve a risk/reputation rating and preview of the target page. Known malicious sites can then be blocked.
- Blocking ransomware files: Security software linked to a cloud-based threat intelligence network can block known malicious files. Unknown files can be intercepted and uploaded to the cloud to be sandboxed and analyzed, and then given a threat rating or blocked.
- Preventing suspicious activity: Anti-virus endpoint software should block known malicious files, but products that offer heuristic analysis can also spot and prevent ransomware-like behavior in unrecognized files. In particular, most ransomware uses Windows' own encryption DLLs, so effective security software will block calls to these

DLLs by untrusted applications, or request confirmation from the user that an encryption operation has been requested.

- Monitoring for mass modifications: File integrity monitoring capabilities can detect changes to system files and the registry. This can be used to block applications that attempt to create or modify large numbers of files or change their names.
- Detecting anomalous behavior Data Loss Prevention systems can create dummy files that should never be accessed or backed up. If these files are accessed, they can trigger an alarm that a possible ransomware attack is taking place.

Source: Fulbright, Norton Rose (2016)

F-secure Labs (2016) provide an updated framework for measures against Ransomware infections that consists of four phases:

PREDICT

- Identify software with vulnerabilities that may serve as entry points to devices, data or local network
- Identify program settings that can be configured for optimal security
- Evaluate user behavior patterns and security awareness

PREVENT

- Take regular backups and ensure they are clean
- Regularly patch any installed software y Use robust, multilayered security software
- Educate users in best security practices and threat awareness

DETECT

- Use security software with behavioral analysis capabilities to identify suspicious behavior on a device in the local network

- Identify the resources (devices, network shares) connected to an affected device to estimate potential exposure
- Identify changes done on the affected device by the threat

RESPOND

- Immediately disconnect the affected machine from the local network and the Internet
- Scan all connected devices, network shares and cloud storage for evidence of the threat
- Examine the affected device for information on how the threat was able to install and run

Source: F-secure Labs (2016)

Prevention for Windows based systems

- Restrict user's write access rights to network shares and connect to partitions only when necessary. Disconnect from partitions after use.
- Enable "Show hidden Files, Folders and Drives" and disable "Hide extension of known file types".
- Implement rules in Group Policy Objects to restrict execution of executable files (.exe) in %APPDATA%, %LOCAL_APPDATA%, and their sub-directories, and apply exclusions for known good files
- Limit users to accounts without administrator rights to prevent silent system installations and modifications.
- Enable the Applocker feature available in Windows 7 and 2008 R2
- On Windows Vista and later operating systems, enable application restriction strategies.
- Activate User Account Control (UAC) to prevent 'elevation of privilege' vulnerability attacks on the user accounts.
- Configure the anti-spam solution to filter email messages with file attachments of the type ZIP, DOC, DOCX, XSL, XSLX, and XML, in addition to all file attachments of executable programs.

- Prevent malicious JavaScript files from running. To prevent users inadvertently running a malicious JavaScript file, disable the Windows Script Host (which is responsible for running JavaScript files outside a browser).

Source: Zaharia, Andra. (2017)

Network Segmentation

Network segmentation is very useful to reduce ransomware affects due splitting device network into subnetworks This technique is very useful because it makes the network traffic work separately without sharing the entire network in possible ransomware attack. In this case attackers, cannot have access to another segment or machine from the network. Moreover, security companies provide latest prevention techniques to stop the ransomware attacking the entire networks. As an example, Cisco company designed some specific security programs to detect and prevent ransomware attacks such as Advanced Malware Protection (AMP). AMP takes full advantage of the vast cloud security intelligence networks provided by Cisco Collective Security Intelligence, Talos Security Intelligence and Research Group, and AMP Threat Grid to deliver advanced protection. According to the Cisco company AMP based on the three categories such as file reputation which is dealing with files inline, File Sandboxing to understanding the behaviors of the file, and file retrospection to know the severity level of the threat. Cisco Talos. (2016)

Web browser plugins

Ransomware frequently uses advertising and web ads from the popular websites to infects end users. Ransomware is often distributed through malicious ads served when visiting certain sites. Blocking ads or preventing users from accessing certain sites can reduce that risk. In addition, ads, can be removed and disabled from the browsers both manually and by certain programs. In addition, each browser needs a different approach to perform such task. Finally, educating and training end users and company employees are highly recommended to avoid ransomware attacks. I. B. M. and Services Incident Response (2016)

Cloud based Ransomware Prevention Systems

The cloud is the only platform with the agility to respond to evolutions in ransomware. The purpose of these attacks won't change, but the delivery methods certainly will. Because cloud environments offer scalable and flexible resources, they allow enterprises to reliably keep up with changes in the threat landscape. Particularly sensitive industries like healthcare, retail, and finance can leverage the cloud by partnering with security providers who offer cutting-edge portfolios of security services. It is one of the popular anti ransomware strategies being utilized currently by enterprises. Lee, J. K., Moon, S. Y. and Park, J. H. (2017) propose CloudRPS which collects information from the cloud system and analyzes it to prevent ransomware attacks. The proposed system consists of six components: classifier, analyzer, ransomware, inspector, network monitor, file monitor, and server monitor. The research can detect and respond to various ransomware attacks based on server, network, and file using monitoring of filesystem operation as a countermeasure. In an operating system, if a large amount of data is converted, the CloudRPS starts to conduct an analysis in advance. At this point, the existing data is backed up through the cloud system is the data backup DB. To verify whether there is a malicious code the pre-processing step and threat components are extracted. The information is received from the data base that has the existing ransomware's information, threat information and classification information, and it is then categorized into the risk level, alert level, or normal level. For accurate detection, other application programs are terminated. Based on the level identified, the data is classified to defend against ransomware. The detected ransomware is stored in the database after analysis. When an email arrives, monitoring of the network and the file takes place as well as mirroring onto the CloudRPS. The mirrored data is analyzed by the CloudRPS. Before the user reads the email, it is sent to the File monitor. If an attached file is downloaded or a linked web page is visited for downloading a file, the user will end up downloading a malicious code. Whenever an email moves, the log is sent to the CloudRPS and analysis is constantly conducted. Lee, J. K., Moon, S. Y. and Park, J. H. (2017)

In Lee, J. K., Moon, S. Y. and Park, J. H. (2017) 's work, the tool conducts file analysis through dynamic and static analysis and monitoring through collecting domain information through blacklist method, but it is only possible to detect when there are analyzed samples. The file to be executed is tested prior and if the file monitor detects malicious software then the CloudRPS

informs the user of infection and shows the trace of malicious codes through the log information. For accurate detection, other application programs are terminated. The CloudRPS, by tracing the infection path, deletes the malicious activity or abnormal activity from all terminals that are along the infection path, thus removing the threat of additional infection. When malicious or abnormal behaviors are not removed, restoration is connected. If restoration is not completed, through data backup DB of CloudDB, data is restored and when the restoration is done successfully, continuous monitoring is conducted. The first step generally in the case of ransomware infections is to make sure that backups are not visible to the computer that gets infected, either as a drive letter or even as a network share. One of the best features of cloud backup systems is that the backups are not on the office network or inside the system. This makes it virtually impossible for ransomware to encrypt backups unless they get access to the cloud through APT attacks. The backup client application on the system sends backups to a cloud application. The cloud application then stores the backup data outside of the network. The cloud application should only accept new backups. Once backups are stored, they should never change. Occasionally, they will be restored. It is essential to make sure that there isn't a drive letter on systems that makes backups available from the system in case of it being compromised. Lee, J. K., Moon, S. Y. and Park, J. H. (2017)

Cloud-based storage provides a second layer of protection. While cloud-based security features thwart threats by keeping them outside the borders of your wide area network, if hackers do breach the network's defenses, using cloud storage neutralizes the negative effects of a ransomware attack. Because the whole system gets backed up, the ploy won't affect the organization, and one won't need to worry about paying ransom to criminals. Raju, Kent (2017)

CONCLUSION

Extensive research has been done to understand the various components that constitute a ransomware attack including public key encryption schemes, Bitcoin transactions, and C&C servers hosted on TOR. It helps us, to a certain extent, confirm that taking even one of them out of the equation may help with minimizing the threat and and allow security researchers to disrupt the business model of the ransomware scheme. Currently, most research performed by security researchers along the years has been inclined towards software-based detection although it is clear that there are key arithmetic components that can be measured on the hardware level as shown by Kiraz, M. S., Genç, Z. A. and Öztürk, E. (2017) via EXPMonitor to detect ransomware at a much faster and precise rate. This allows us to reach an understanding that hybrid detection mechanisms mixed with AI based prevention systems can lead us to a definitive answer and a robust solution against the struggle with Ransomware. Chen, Y. C. et al. (2018)

Companies making updates to firmware and hardening at the hardware level is essential and providing in-built security to detect high multiplication arithmetic, Kiraz, M. S., Genç, Z. A. and Öztürk, E. (2017), as well as feature matching on software level along with better protection of keys stored in the system should help prevent encryption before it occurs. At the same time, the trend seems to be shifting towards destruction of data after holding people to ransom as seen in the case of Not Petya which means that paying the ransom is never a feasible option.

Backups are the most essential aspect to mitigating ransomware as they minimize data loss and allow faster recovery in order to reduce downtime and get all business services back up. Consistent updates and patching of the systems along with monitoring of the two primary attack vectors, that is, phishing emails and web browser vulnerabilities will minimize chances of a ransomware infection drastically. It is important to note that that hardening of systems and patching is crucial to avoid any existing vulnerabilities to be used as entry point. Preston, Curtis W. (2018)

Human error or lack of due care and due diligence is often the reason for the window of opportunity to be present for the malicious authors to take advantage of. A socio- technological approach that focuses on not just the systems but the personnel running them, is essential to protect and prevent

against ransomware. At its core, the attacks follow similar patterns which involve duping the unsuspecting audience, cyber criminals that send malware in documents are relying on the chance taken when the user shouldn't open a document until they are sure if it's one they want, but in haste that is forsaken leading to an opening that can be exploited. Sittig, D. F. and Singh, H. (2016)

The need for smarter AI based security solutions inbuilt into systems that can monitor hardware and software levels dynamically is clear and can be experimentally researched as future work based on the information provided in this work. Fu, Josh (2018)

A defense in depth strategy is preferable in the long run as there can never be enough contingency plans with the rate at which technology changes. As an example, using cloud storage for backups along with off-site physically isolated backups will add to recovery options. The cloud will always have more reliability and resiliency built in than the average data center. Thanks to expansive storage capabilities and streamlined failover processes, the cloud is becoming the preferred platform for backup recovery. They combine sophisticated access controls and advanced encryption technology with expansive capabilities for testing security and vulnerability. Many of these security features also provide necessary levels of protection against distributed denial of service attacks, amplifying their overall utility. Raju, Kent (2017)

REFERENCES

Murray, W. H. (2008) 'What the Graduate Needs to Know about Cryptography', pp. 153–157.

Lanet, J., Guernic, C. Le and Legay, A. (2017) 'Risks and Security of Internet and Systems', 10158, pp. 11–28. doi: 10.1007/978-3-319-54876-0.

Young, A., Yung, M. (1996) Cryptovirology: extortion-based security threats and countermeasures. In: Proceedings of the IEEE Symposium on Security and Privacy, pp. 129–140. IEEE

Orman, H. (2016) 'Evil Offspring - Ransomware and Crypto Technology', IEEE Internet Computing, 20(5). doi: 10.1109/MIC.2016.90.

Savage, K., Coogan, P. and Lau, H. (2015) 'The Evolution of Ransomware', Security Response, p. 57. doi: 10.5437/08953608X5403011.

Kotov, V. and Rajpal, M. S. (2012) 'Understanding Crypto Ransomware', Bromium, pp. 1–35. Available at: https://www.bromium.com/sites/.../bromium-report-ransomware.pdf

Gazet, A. (2010) 'Comparative analysis of various ransomware virii', Journal in Computer Virology, 6(1), pp. 77–90. doi: 10.1007/s11416-008-0092-2.

Herrera-Joancomart, J. (2015) Data privacy management, autonomous spontaneous security, and security assurance, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). doi: 10.1007/978-3-319-17016-9.

Kolodenker, E. et al. (2017) 'PayBreak: Defense Against Cryptographic Ransomware.', AsiaCCS, pp. 599–611. doi: 10.1145/3052973.3053035.

Taylor, T. et al. (2016) ‘Detecting Malicious Exploit Kits using Tree-based Similarity Searches’, Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY), pp. 255–266. doi: 10.1145/2857705.2857718.

Moore, C. (2016) ‘Detecting ransomware with honeypot techniques’, in Proceedings - 2016 Cybersecurity and Cyberforensics Conference, CCC 2016. doi: 10.1109/CCC.2016.14.

B, A. Gharib and Ghorbani, A. (2017) ‘Network and System Security’, 10394, pp. 184–198. doi: 10.1007/978-3-319-64701-2.

Hutchison, D. (2013) Detection of Intrusions and Malware, and Vulnerability Assessment. doi: 10.1007/978-3-642-37300-8.

Kiraz, M. S., Genç, Z. A. and Öztürk, E. (2017) ‘Detecting Large Integer Arithmetic for Defense Against Crypto Ransomware’.

Monika, Zavarsky, P. and Lindskog, D. (2016) ‘Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization’, Procedia Computer Science, 94, pp. 465–472. doi: 10.1016/j.procs.2016.08.072.

Yang, T. et al. (2015) ‘Automated detection and analysis for android ransomware’, Proceedings - 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security and 2015 IEEE 12th International Conference on Embedded Software and Systems, H, (1), pp. 1338–1343. doi: 10.1109/HPCC-CSS-ICESS.2015.39.

Bos, H., Monrose, F. and Blanc, G. (2015) ‘Research in attacks, intrusions, and defenses: 18th international symposium, RAID 2015 Kyoto, Japan, november 2-4, 2015 proceedings’, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9404, pp. 382–404. doi: 10.1007/978-3-319-26362-5.

Mbol, F., B, J. R. and Sadighian, A. (2016) ‘Cryptology and Network Security’, 10052, pp. 532–541. doi: 10.1007/978-3-319-48965-0.

Lee, J. K. et al. (2017) ‘CloudRPS: a cloud analysis based enhanced ransomware prevention system’, Journal of Supercomputing, 73(7). doi: 10.1007/s11227-016-1825-5.

Cabaj, K. and Mazurczyk, W. (2016) ‘Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall’, IEEE Network, 30(6), pp. 14–20. doi: 10.1109/MNET.2016.1600110NM.

Scaife, N. et al. (2016) ‘CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data’, in Proceedings - International Conference on Distributed Computing Systems. doi: 10.1109/ICDCS.2016.46.

Kharaz, A. et al. (2016) ‘UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware’ This paper is included in the Proceedings of the 25th USENIX Security Symposium.

I. B. M. and Services Incident Response (2016) ‘Ransomware Response Guide’, (May).

Lanet, J., Guernic, C. Le and Legay, A. (2017) ‘Risks and Security of Internet and Systems’, 10158, pp. 11–28. doi: 10.1007/978-3-319-54876-0.

F-secure Labs (2016) ‘Ransomware: How to prevent, predict, detect & respond’, (November).

Gorman, G. O. and McDonald, G. (2012) ‘Ransomware : A Growing Menace’, Symantec, 1, p. 16.

Burgess, M. and Ieraci, J. (2017) ‘Telstra Cyber Security Report 2017’. Available at: https://www.telstraglobal.com/images/assets/insights/resources/Telstra_Cyber_Security_Report_2017_-_Whitepaper.pdf.

Mansfield-Devine, Steve. (2016) “Ransomware: Taking Businesses Hostage.” Network Security 2016 (10). https://doi.org/10.1016/S1353-4858(16)30096-4.

Zaharia, Andra. (2017). what-is-ransomware-protection [Web blog post]. Retrieved May 15, 2017, from https://heimdalsecurity.com/blog/what-is-ransomware-protection/#ransomwaredefinition

Kharraz, A. et al. (2015) ‘Cutting the gordian knot: A look under the hood of ransomware attacks’, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9148, pp. 3–24. doi: 10.1007/978-3-319-20550-2_1.

Android Developers (2018) Application Fundamentals [doc post]. Retrieved April 30, 2018, from https://developer.android.com/guide/components/fundamentals

Bisson, David. (2016) The top 10 ransomware strains of 2016 [Web blog post]. Retrieved December 18, 2016, from https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/top-10-ransomware-strains-2016/

Constantin, Lucian. (2016) Ransomware authors use the bitcoin blockchain to deliver encryption keys [Web blog post]. Retrieved April 14, 2016, from https://www.csoonline.com/article/3056685/security/ransomware-authors-use-the-bitcoin-blockchain-to-deliver-encryption-keys.html

Roccia, Thomas. (2018) Free Ransomware Available on Dark Web [Web blog post]. Retrieved February 16, 2018, from https://securingtomorrow.mcafee.com/mcafee-labs/free-ransomware-available-dark-web/

Beelen, Aubrey. (2016) The relationship between TOR and ransomware [Web blog post]. Retrieved June 21, 2018, from http://blog.dataunit.be/the-relationship-between-tor-and-ransomware

Cisco Talos. (2016) Ransomware: Past, Present, and Future [Web blog post]. Retrieved April 11, 2016, from https://blog.talosintelligence.com/2016/04/ransomware.html#ch6

Krebs, Brian. (2012) Inside a 'Reveton' Ransomware Operation [Web blog post]. Retrieved August 13, 2012, from https://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

Krebs, Brian. (2015) Ransomware Now Gunning for Your Web Sites [Web blog post]. Retrieved November 15, 2015, from https://krebsonsecurity.com/2015/11/ransomware-now-gunning-for-your-web-sites/

No More Ransom Project. (2016) Available at: https://www.nomoreransom.org/.

Wagner, William C. (2015) Cyber Insurance: Do I Really Need It? [Web blog post]. Retrieved March 23, 2015, from https://www.privacyanddatasecurityinsight.com/2015/03/cyber-insurance-do-i-really-need-it/

Goodin, Dan. (2013) You're infected—if you want to see your data again, pay us $300 in Bitcoins [Web blog post]. Retrieved October 17, 2013, from https://arstechnica.com/information-technology/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/

Fulbright, Norton Rose (2016) Ransomware Incident Response – Prevention, Readiness and Strategy [Web blog post]. Retrieved February 28, 2016, from https://www.dataprotectionreport.com/2016/02/ransomware-incident-response-prevention-readiness-and-strategy/

Liska, Allan and Gallo, Timothy (2016) 'Ransomware: Defending Against Digital Extortion', 1st Ed. by O'Reilly Media, Inc. ©2016. ISBN:1491967889 9781491967881

Bookshire, Nathan (2016) Locky Virus File Encryption Removal. How To Remove Guide (2016). Available at: https://howtoremove.guide/locky-virus-file-encryption-removal/

Cisco Inc. (2015) Ransomware on Steroids: Cryptowall 2.0. Retrieved from https://blogs.cisco.com/ security/talos/cryptowall-2, 2015.

National Institute of Standards and Technology (NIST). (2001) Specification for the Advanced Encryption Standard, FIPS PUB 197, November 2001

Abrams, L. (2017) CTB-Locker for Websites: Reinventing an old Ransomware. http://www.bleepingcomputer.com/news/security/ctb-locker-for-websites-reinventing-an-old-ransomware/

Mills, Chris (2017) Global cyber attack could cost $53 billion, report warns. Retrieved from: https://bgr.com/2017/07/18/wannacry-worst-cyber-attack-cost/

Moffitt, Tyler (2017) Locky ransomware rises from the crypt with new Lukitus and Diablo variants. Retrieved from: https://www.webroot.com/blog/2017/08/17/locky-ransomware-resurges-diablo-lukitus/

Spagnuolo, M., Maggi, F., and Zanero, S. (2014) BitIodine: Extracting intelligence from the bitcoin network. In Financial Cryptography and Data Security (March 2014), Lecture Notes in Computer Science (LNCS), Springer-Verlag.

M. L´eveill´e, M.-E. (2014) Torrentlocker ransomware in a country near you. Retrieved from: http://www.welivesecurity.com/2014/12/16/torrentlocker-ransomware-in-a- country-near-you/

Fergal, R., and Martin, H. (2012) An analysis of anonymity in the bitcoin system. This paper is included in Security and Privacy in Social Networks.

Ismail, Nick. (2017) Ransomware, cyber insurance and cryptocurrency: are you covered? [Web blog post]. Retrieved September 29 2017, from http://www.information-age.com/ransomware-cyber-insurance-cryptocurrency-covered-123468796/

Song, S., Kim, B., Lee, S. (2016) The effective ransomware prevention technique using process monitoring on android platform. Mob. Inf. Syst., 1–8

Mercaldo, F., Nardone, V., Santone, A., Visaggio, C.A. (2016). Ransomware steals your phone. Formal methods rescue it. In: Albert, E., Lanese, I. (eds.) FORTE 2016. LNCS, vol. 9688, pp. 212–221. Springer, Heidelberg. doi:10.1007/ 978-3-319-39570-8 14

Andronio, Nicoló, Zanero, Stefano & Maggi, Federico. (2015). HELDROID: dissecting and detecting mobile ransomware. 382-404. 10.1007/978-3-319-26362-5_18.

Vanhoef, M. and Piessens, F. (2017) 'Key Reinstallation Attacks', Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS '17, pp. 1313–1328. doi: 10.1145/3133956.3134027.

Cichonski, P. (2012) 'Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology', NIST Special Publication, 800–61, p. 79. doi: 10.6028/NIST.SP.800-61r2.

Dingledine, R., Mathewson, N. and Syverson, P. (2004) 'Tor: The Second-Generation Onion Router'. doi: 10.21236/ADA465464.]

Mateiu, Monica. (2018) The ultimate guide to ransomware [Web blog post]. Retrieved February 14, 2018, from https://www.avg.com/en/signal/what-is-ransomware

Vanderburg, Eric. (2017) Part 2: The Psychology Behind Infamous Ransomware [Web blog post]. Retrieved December 13, 2017, from https://www.tcdi.com/the-psychology-behind-infamous-ransomware/

Vanderburg, Eric. (2017) Part 4: A Timeline of Ransomware Advances [Web blog post]. Retrieved December 27, 2017, from https://www.tcdi.com/ransomware-timeline/

TCDI. (2017) The Five W's (and How) of Ransomware [Web blog post]. Retrieved December 06, 2017, from https://www.tcdi.com/the-five-ws-and-how-of-ransomware/

Chen, Y. C. et al. (2018) 'Deep learning for malicious flow detection', IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC, 2017–October, pp. 1–7. doi: 10.1109/PIMRC.2017.8292316.

Trend Micro. (2017) Machine learning and the fight against ransomware [Web blog post]. Retrieved April 26, 2017, from https://blog.trendmicro.com/machine-learning-and-the-fight-against-ransomware/

Kaspersky Lab (2016) The Rise of Ransomware – Most Glaring Examples from 2015-2016 [Web blog post]. Retrieved December 06, 2016, from https://usa.kaspersky.com/resource-center/threats/ransomware-threats-an-in-depth-guide

Raju, Kent (2017) Can Cloud Storage save you from Ransomware Attacks? [Web blog post]. Retrieved July 17, 2017, from https://www.infosecurity-magazine.com/opinions/cloud-storage-save-ransomware/

Preston, Curtis W. (2018) Can Patching and Backup Protect from Ransomware? [Web blog post]. Retrieved February 16, 2018, from https://www.infosecuritymagazine.com/opinions/patching-backup-protect-ransomware/

Fu, Josh (2018) How AI Can Stop Ransomware, Detect Malware and Reduce Risk [Web blog post]. Retrieved March 16, 2018, from https://www.infosecurity-magazine.com/next-gen-infosec/ai-ransomware-detect-malware-risk/

Infosec Institute. (2017) A Brief Summary of Encryption Method Used in Widespread Ransomware [Web blog post]. Retrieved January 13, 2017, from https://resources.infosecinstitute.com/a-brief-summary-of-encryption-method-used-in-widespread-ransomware/#gref

Sittig, D. F. and Singh, H. (2016) ‘A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks’, Applied Clinical Informatics, 7(2). doi: 10.4338/ACI-2016-04-SOA-0064.

Wu, C., Lou, D. and Chang, T. (2014) ‘Computational Complexity Analyses of Modular Arithmetic for RSA Cryptosystem’, pp. 215–224. doi: 10.1109/IS3C.2014.216

Charette, N. Robert (2018) ‘Healthcare IT Systems: Tempting Targets for Ransomware’ Retrieved on February18, 2018 from https://spectrum.ieee.org/riskfactor/computing/it/healthcare-it-systems-tempting-targets-for-ransomware