Ransomware: Prevention & Mitigation of an Evolving Menace

Syed Muhammad Kumail Raza and Derek Sedlack[1]
Information Security, WS-2018-19
Technical University of Kaiserslautern, Germany
sraza@rhrk.uni-kl.de, derek@sedlack.com

Abstract— **Ransomware is a type of malware that encrypts the files of infected hosts and demands payment, often in cryptocurrency such as Bitcoin. Ransomware targets have become more educated, aware and cautious, motivating cybercriminals to respond with innovative attacks. Therefore, this malware is a rapidly evolving threat to individuals and businesses dealing in Data. In this paper, we present a review of Ransomware evolution with respect to current technology and it's future direction. We also analyze what makes an individual or an organization susceptible to the succumbing demands of Ransomware. The paper further presents approaches to prevent the attack in terms of simple recommended practices targeted towards businesses and individuals, along with other more advance solutions involving intelligent intrusion detection systems. Finally it presents mitigation techniques involving approaches to recover from an infection, should one happen and some predictions on upcoming challenges based on the current trends of Ransomware and technology.**

I. INTRODUCTION

Over the last two decades, a class of malware known as scareware has become popular among cybercriminals. This malware takes advantage of peoples fear of revealing their private information, losing their critical data, or facing irreversible hardware damage. In particular, this paper focuses on Ransomware, a particular class of scareware that locks the victims computers until they make a payment to re-gain access to their data. Since its inception as AIDS Trojan in 1989, Ransomware remained aloof until 2005 when in Russia, the first cases of the attack led to substantial monetary loss, Kaspersky lab reported [1]. This pernicious malware gained stronger roots of severity when CryptoLocker evolved in 2013 causing fatal destruction to educational institutions, business organisations, law enforcement agencies, hospitals and local and state government who ended up paying exorbitant amounts of money through virtual currencies. It is now the big business adopted by the cybercriminals to stealthily steal, encrypt and destroy sensitive information. Advances in computer and network security has, in parallel, given rise to stronger encryption algorithms, improvement in attack installation and deployment methods, virtual currencies and anonymous networks. These advances make Ransomware more powerful and challenging to control and conquer. Cybercriminals have adapted reactively to this fast-changing cybercrime environment to maintain their extremely profitable operations. They have become more business savvy in their stealthy endeavours transforming Ransomware into a lucrative venture for them. From 2016 onwards we witnessed an increased percentage of attacks caused by some entirely new set of Ransomware family variants. Cyber criminals tend to feed off the booming 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[2]. Given the significant growth of Ransomware attacks [3], it is very important to develop a protection technique against this type of malware. However, design- ing effective defense mechanisms is not practically possible without having an insightful understanding of these attacks. Currently, many of the recent security reports about Ransomware [4] rely on ad-hoc procedures rather than a scientific assessment. Moreover, these reports mainly focus on the advancements in Ransomware attacks and their levels of sophistication [5], rather than providing some insights about effective defense techniques that should be adopted against this threat.

II. RANSOMWARE: OVERVIEW OF LITERATURE

Ransomware is big business. The computer security firm Symantec conservatively estimates that Ransomware extorts hundreds of millions from victims each year. Symantec also notes that paying the ransom is no guarantee that the decryption key will be provided and, in many cases, it is not [6], [7]. Ransomware can be divided into two basic types. The most common is crypto Ransomware, which encrypts files and data. The second type is locker Ransomware. This version locks the computer or other device, preventing the victims from using it [8]. Locker Ransomware only locks the device; the data stored on the device is typically untouched. As a result, if the malware is removed, the data is untouched. Even if the malware cannot be easily removed, the data can often be recovered by moving the storage device, typically a hard drive, to another functioning computer. This makes locker Ransomware much less effective in extorting ransom

[1] Department of Informatik, Technical University of Kaiserslautern www.uni-kl.de

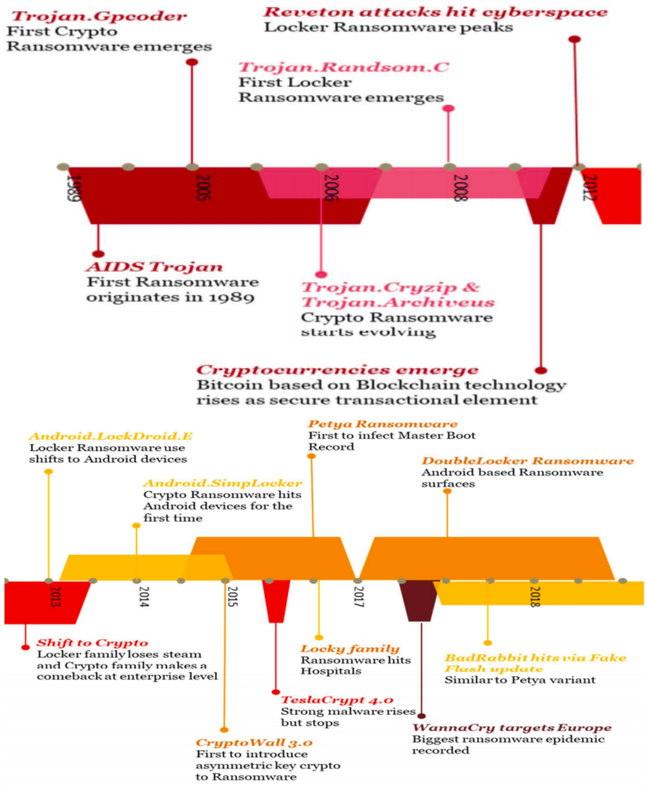

Fig. 1. The figures show the time-line of Ransomware attacks as they were surfaced from the first one in 1999 to the most recent one in 2018.

payments [8]. Crypto Ransomware, on the other hand, encrypts the data, so even if the malware is removed from the device or the storage media is moved to another device, the data is not accessible. Typically, crypto Ransomware does not target critical system files, enabling the device to continue to function in spite of being infected after all, the device could be needed to pay the ransom [8]. Figure 1 show the Ransomware evolution timeline with different attack vectors and targeting various systems. It is clear from the timeline that as the organizations started to adopt more up to date security measures and computer security algorithms became sophisticated, the attacker became more and more innovative and the malware evolved.

By 2013 it started to target large enterprises finding vulnerabilities in their operating systems, firewalls etc [4]. In the same year, scareware arrived in the form of Reveton, which locked and prevented access to the infected device (known as a Locker). After locking the computer, the Ransomware falsely alleged that the computer (and user) had engaged in unlawful activities and needed to pay a fine to unlock the computer. Reveton demanded payment via an anonymous prepaid voucher service [9]. To encourage payment, Reveton displayed police enforcement warnings and in some strains, displayed webcam footage to enforce the illusion that the victim is the criminal. Reveton was followed by a spate of copycat Ransomware Urausy and Tohfy claiming to be police enforcement and that a fine had to be paid to prevent further legal action [10]. Then CryptoLocker (encryption based) arrived in 2013 and spread using multiple infection methods such as email attachments, compromised websites and in 2014 used the GameOver Zeus botnet infrastructure for distribution. CryptoLocker used Advanced Encryption Standard (AES)-256 file encryption and used 2048-bit RSA for their C&C on the TOR networks [11], [12].

2014 heralded a new revolution in Ransomware with the adoption of ransom payment via a TOR-based Bitcoin to ensure improved anonymity [13]. In February, CryptoDefense used Windows' built-in encryption libraries to perform RSA-2048 file encryption. However, using this method has a weakness; the Windows API creates the private key that needs to be transmitted back to the attacker's C&C server [14]. CryptoDefense creators went on to develop an enhanced Ransomware known as CryptoWall. Then till 2016 and even after that, most ransomwares adopted what is called *the default configuration*. AES Encryption, command-control and communication through the TOR Servers and payment via Bitcoin [10]. Also in 2016 a Ransomware named KeRanger [15] heralded revolution; it targeted the Apple OS X, which had been considered to have a high immunity to malware [16]. The criminals had created a legitimate signed Trojan using a stolen update certificate. This valid certificate made the Trojan appear as an authorized update which installed without any warning [10].

WannaCry Ransomware Attack 2017 was the worst malware attack of all times. WannaCry [6, 7] was one of the largest Ransomware attacks in history, halting hospital facilities and infecting large corporations and consumers in over 150 countries. From initial exploit to completing encryption of a hosts data, Ransomware must perform a series of actions; e.g., identifying files for encryption/deletion and exchanging encryption keys with a command and control (CC) server. WannaCry used the Windows API encryption routines to generate the encryption keys and conceal the private key[10]. WannaCry uses two sets of keys, one for a small selection of files demo decrypt files and a second for the main ransom files, thereby ensuring that releasing the demo decrypt key will not enable the victim to decrypt the main encrypted files[17]. However, the most effective aspect of the WannaCry campaign is probably the Exploit Kit that targeted the Windows vulnerability. It is widely believed that this exploit was derived from a toolset leaked from the National Security Agency named EternalBlue [18]. EternalBlue targeted a known vulnerability that had been patched. Unfortunately, many users failed to pick up this patch and were left at the mercy of WannaCry.

With Ransomware families like WannaCry on the move, the computer security companies started adopting much more innovative solutions and algorithms for malware detection. The interest of the industry and academia shifted towards automated analysis of Ransomware activities. Chen et al. introduced this technique for the first time by presenting algorithms that use system logs as inputs to automatically identify patterns for different kinds of Ransomware signature activities [17]. Then Kharraz et al. developed UNVEIL. UNVEIL automatically generates an artificial user environment, and detects when Ransomware interacts with user data. In parallel, the approach tracks changes to the systems desktop that indicate Ransomware-like behavior [19]. Then the Ransomware started to target Android smartphones, so Yang et. al presented their work on detection of Ransomware analyzing the OS logs and behaviors and provided effective countermeasures against malicious applications. In 2018, as the datasets containing different attacks families and victim devices became public, deep learning based solutions emerged. Tseng et. al in [20] present their deep learning model which can work in high speed network in real-time for detecting various Ransomwares and preventing them from encrypting victims data.

The rest of the paper accounts for the Infection Vectors and detecting Ransomware, mitigation once the attack happens, prevention techniques and some eye-opening current & future trends and aspects of Ransomware.

III. Infection Vectors and Detection

Ransomware requires much more than just a functioning computer system to execute itself properly. It must communicate with a server to get an encryption key and report its results. This requires a server hosted by a company that will ignore the illegal activity and guarantee the attackers anonymity. These hosting companies are called Bulletproof Hosting. Most are located in China or Russia. Attackers also use a proxy or VPN services to further disguise their own IP addresses [21]. This means two things: The obvious one is that the attack is now much more difficult to probe, detect, prevent and investigate. The other proposition is that due to the use of multiple technologies for the attack to function, we have now more probe points which can serve as potential detection points of the attack. An analogy can be the difference between a home pc and an enterprise network of a business. A typical home pc has only one public interface through the ISP. The business enterprise network can have hundreds of computers (possibly data centers, servers etc.), many of which would have multiple public interfaces thus providing the attackers with more attack points. This in turn also provides the computer security analysts with a lot of data in terms of all those attack points which were exploited. These potential attack points and possible ways of infecting a computer or a network with Ransomware are discussed in the following subsections.

A. Potential Targets

Initially unsophisticated home users were the cash cows for Ransomware because they lacked computer security knowledge and have least amount of access to technical assistance, thus exposing their systems to vulnerable attacks. Several researchers have conducted surveys against home users testing the level of knowledge and engagement in computer security-related activities [22], [23], [24]. It was found that users failed to make security decisions independently, rather outsourced the security and maintenance tasks to resident expert or paid technicians. Symantec survey reported in 2009 that only 25% of home users back up their computer files, and out of those, most do not regularly or thoroughly back up their data. Attackers exploited this attitude of home users by capturing personal electronic assets such as pictures, sensitive financial documents, home videos, academic documents and resumes. It is also a glaring fact that businesses have more money to shell out when compared to an average user. The compelling reason behind paying exorbitant ransom is the valuable data such as databases full of business transactions, personnel files, proprietary documents such as blueprints, source code or development specs, which will not only reveal critical information but will disrupt mere existence of business organisations. Take for example a medical billing corporation. Due to the HIPAA (Health Insurance Portability and Accountability Act of the US)[25] law a Personal Health Record (PHR) is now treated as a confidential document. Medical billing companies deal with millions of these documents everyday, therefore they need data-centers, which makes them all the more lucrative option to attackers. This is because loosing access to even a single PHR (which if happens, must be reported) is considered a massive breach under the HIPAA laws and the company is forced to pay huge fines to compensate for the loss [25]. It is believed that larger the businesses, affordability for secure infrastructure might increase but not all security teams are well trained to protect against such zero-day threats.

Other public agencies like hospitals, municipal departments, town officials and police departments have surprisingly been frequent targets of Ransomware targets [26], [27]. Although Ransomware indiscriminately chooses victims, it does aimfully target operating systems. Windows dominates computer operating systems for servers and even more so for desktops. It has been noted that Windows because of it's recurring vulnerabilities is an easy target to Ransomware attacks [14]. However as the attackers improve, we can expect them to attack Linux platforms in no time.

B. Attack Vectors

An attack vector is a path or means by which a hacker can gain access to a computer or network server in order to deliver a payload (Ransomware) or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element. There are various attack vectors which are common. One such method is spear phishing in which malicious emails are sent to recipients, who are specific well-known targets to the attacker. This method has gained significant importance among the social engineering techniques, which exploits the morals of trust and belief of the receiver. The more information a hacker is able to obtain about a target the more customized and seemingly legitimate emails are crafted to captivate the target

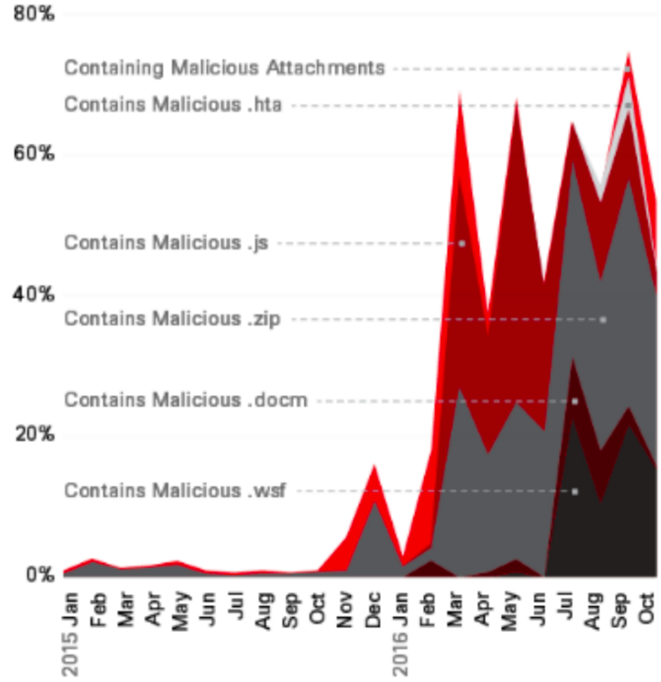

Fig. 2. Cisco Security Research showing the most common attack vector formats for malicious files [28]. Most of these formats are disguised as regular everyday work files like .doc .zip .hta and others, to sneek past an average computer user.

[27]. The payload is delivered as an attachment from emails sent through spam using botnets and other compromised hosts. The victim is social engineered into interacting with the attachment by directly opening an attachment which executes the Ransomware payload, opening a malicious file which in turn initiates payload delivery via a macro or by clicking on a URL in the email which redirects to an exploit kit which in turn runs to find vulnerabilities on the target system and executes the Ransomware payload thereafter. Cisco Security Research [28], [29] shows spam attachments, usually carry files of different formats which could be used to deliver the Ransomware payload. These are shown in Figure 2.

Another attack vector in this domain finding growing usage is brute-forcing user credentials to different systems. Attackers employ automated scripts to achieve this task. Bucbi Ransomware [30] utilized this attack vector to obtain access to the system via RDP. Zimba et al. contend in the paper [31] that Ransomware threat actors can alternatively leverage malware-free intrusion backdoors to obtain access through RDP as some system implement a lockdown mechanism upon failed multiple authentication attempts.

Exploit Kits (EK) are another popular attack vector for Ransomware payload delivery. EKs are software packages which scan for vulnerabilities with the purpose of malware installation upon successful discovery. These scans are run on third party servers and inject code into different portions of the server depending on the context which in turn redirect server visitors to the malware. The Angler EK [32] for example accounted for close to 20 million attacks thwarted by Symantec. Other attack vectors include injection of redirect links in JavaScript, Malvertising, Driveby-Downloads [31], [33], [34] etc.

C. Detection

Ransomware attacks get more refined by the day, as cybercriminals 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 [35]. 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 for further analysis, such as AI-based Intrusion Detection Systems (IDS). We'll discuss that in a while. Current areas of Detection can be summarized in the techniques discussed in the following sections.

1) Behavioural Analysis: Once a device has been infected it performs a series of tasks in steps. These tasks and the corresponding system's behaviour can serve as a signature for Ransomware detection. For example the Ransomware 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. Since all these activities and tasks are being monitored and logged in the so called 'Activity Manager' of an operating system, this serves as a central repository for analysis of system behavior. As proposed by Kharaz et al. [4], this kind of a detection is system is not only dynamic but also provides real time analysis and response. For example changes in Master File Table, the types of I/O Request Packets to the file system and massive renames of the files due to encryption, all at the same time are sufficient pointers to a Ransomware attack. Another similar detection system is proposed by Scaife, N. et al. [36] 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. Another system that makes use of the virtual environment is UNVEIL[19]. UNVEIL automatically generates an artificial user environment, and detects when Ransomware interacts with user data. In parallel, the approach tracks changes to the systems desktop that indicate Ransomware-like behavior.

2) Detection of Exploit Kit Activity: EKs 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 EKs to target a specific group, called a watering hole attack. The agility of EKs 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 EK of choice for cyber-criminals prior to July 2016 has been the Angler exploit kit [37]. To detect Ransomware attacks from exploit kits Taylor et al. [38] 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, they 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 of 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 [38].

3) Detection Using AI: Artificial Intelligence is a type of technique which comes into play when the the number of parameters in traditional algorithms becomes too large to handle or when the problem becomes too complex to find a concise algorithm to solve it. If we model the problem of early detection of Ransomware in a system as a time-series problem i.e in terms of live system logs and behavior, Deep Learning approach has proved to be a good fit [39]. Usually the biggest challenge in training Deep Learning models is the availability of sufficient data-sets. Thankfully with the public releases of thousands of Ransomware libraries along with the logs of infected systems, sufficient data is available. Tseng et. al [20] provided the first approach to detecting Ransomware with Deep Learning. In the paper [20] they present a complete detection pipeline i.e from labelling the data and behaviours to a Recurrent Neural Network model and the training parameters. The results of the experiments performed on the datasets display state of the art performance, and even surpassing that as these models can be deployed on high speed networks to detect even the latest Ransomwares timely [20]. Research is underway in developing the best possible deep learning architectures for Ransomware detection [40]. The idea is that these architectures can then be deployed to intelligent intrusion detection systems enhancing their capabilities to detect various Ransomware families in real-time.

IV. Mitigation

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 [41].

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 [42].

NIST Incident Response Life Cycle [43] is a good and effective framework if followed and executed properly for Ransomware mitigation. 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 dont 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 [43].

A. Paying the Ransom

Over the years, based on their awareness on computer security and preparedness against secutiy incidents, the public has reacted to a Ransomware infection in much the same way. Due to widespread panic, urgency of required data and no other alternatives to handle the situation, most of these have resulted in a payment of the ransom. Of course the best case would be not to pay the ransom and retreive the data lost by some alternative means. But in most of the business and enterprise level cases this is not possible. Any decision to pay a ransom should be based on a Risk-Benefit analysis. What is important to consider here is that while many of the victims have successfully recovered their data after paying the ransom, the way Ransowmare malware works provides no guarrantee that an organization will receive the necessary keys to decrypt the affected files. IBM Incident Response Services [42] 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. The IBM Incident Response Services Report [41], [42] also outlines some major questions which need to be answered in the Rist-Benefit Analysis, answers to which in turn produce a recommendation whether or not to pay the ransom.

Paying a ransom to get needed files back can make economic sense. Nevertheless, experts give four reasons not the pay the ransom. First, you become a bigger target. Criminals talk and tell each other who paid and who did not. Second, as discussed above, you cannot trust criminals to decrypt your data. CryptoWall has a reputation for excellent customer service. Other malware families do not. Third, your next ransom will be higher. Perhaps the criminals demand a second ransom before decrypting your data or perhaps you are infected a second time. Either way, you will pay more. Fourth, your payment encourages the criminals to continue doing what they are doing [44], [10].

As the malware is growing, there are now a number of tools available which can detect the family of Ransomware and try to decrypt the files. Some of these reported tools are Apocalypse, BadBlcok, Crypt888, Legion, SZFLocker, and TeslaCrypt [10], [21], [45]. Whether a tool is used to recover files, the files are recovered from a backup, or the ransom is paid, the Ransomware software must be removed from the computer. Experts recommend that the data files be copied off the computer and then the hard drive should be reformatted and the operating system and files be reinstalled fresh [21].

V. Prevention

Ransomware is a scary predicament both for individuals as well as businesses. However, preventing the malware from infecting the systems is somewhat guaranteed, at least in terms of careless behaviour, if some simple steps are taken. These are recommendations from the industry and literature combined based on the studies conducted on various Ransomware infections.

1) **Back Up**: If the data is backed up, there is no need to pay a ransom to get the data back. Instead, it can be recovered from the backups [46]. Of course, the backups need to be current. It is also important to keep multiple backups. Cloud backups are also essential as the Ransomware announces itself after it has blocked user access to the backup systems [46].
2) **Avoid Email Links and Attachments**: As discussed in the paper before, phishing attacks are the most common way to spread Ransomware, so avoiding clicking on links or opening attachments in spam email will go a long way to avoiding Ransomware. However, criminals have also started using compromised advertising (malvertising) to spread Ransomware. These can target trusted websites. Ad blockers can protect against malvertising [6]. Turning off Java and JavaScript can also help. Business should train employees to avoid suspicious email, and corporate IT should consider standardizing ad blocking software [21]. In addition to standard phishing, there is an increase in targeted phishing emails [27]. For example, the phishing email might contain what it claims to be a resum. Most recipients would either ignore it or forward it to HR, while an HR recipient might open it without thinking about it. Other categories are billing, shipping, and invoice related phishing emails [47].
3) **Patch and Block**: The operating system, browsers, and security software should always be kept patched and up-to-date [48]. Likewise, third-party plug-ins, like Java and Flash, need to be kept patched if they are allowed at all. Business systems can also rely on whitelisting and limiting user rights to reduce the chance of a Ransomware infection [7], [6]. Of course, these steps will help reduce other types of malware infections as well.
4) **Drop-and-Roll**: At the first sign of an infection, the infected machine should be immediately turned off (or unplugged) to minimize the damage to files. If it is connected to a network, administrators should immediately shut down the network to minimize the propagation of the Ransomware [6], [7]. The above applies to both individuals and organizations.

Some other more general but equally important recommendations include:

- *Understand the Risks.* Ransomware is a very real danger to both data and the ability of the organization to continue operations and that danger is growing at an accelerating rate [10], [8], [2]. Organizations cannot make good decisions regarding prevention and training expenditures without understanding the full extent of the threat that Ransomware makes to the organization.
- *Develop Adequate Policies.* Organizations almost always have policies defining the situations but often lack the description of actions to take when that situation actually occurs [49]. Also most of the policies are open to interpretation. Some seemingly non-important aspects also play a vital role in data security. Such aspects should be identified and clear policies should be drafted and implemented. One such example of such an aspect are devices not owned by the organization. They are often connected to the organizations network. These would include, for example, cell phones and tablets owned by employees. This is sometimes called shadow IT [50]. Ransomware policies, protection, and response procedures need to include the entire network, including shadow IT [51].
- *Institute Best Practices for Users.* These would include appropriate password management, ongoing security

awareness training, back-channels for key employees dealing with finances or sensitive so requests for funds transfers can be double-checked, periodic testing of employees to make sure the training is effective, an appropriate social media policy, and making sure employees keep the software on their personal devices up-to-date [51].

Federal Bureau of Investigation also has its own recommendations to prevent Ransomware for business enterprises: Make sure employees understand their role in protecting against Ransomware, manage the use of privileged accounts so that work gets accomplished at the lowest privilege level possible, configure access controls, including file, directory and network share permissions appropriately, disable macro scripts, and implement software restriction policies or other controls to prevent Ransomware from executing from commonly used locations [52].

NIST Incident Response Life Cycle [43] as discussed in the previous section is also an effective framework which provides some recommendations on Cyber Security Incident responses. In case of Ransomware, 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 [43]. Some more technical aspects of the recommendations are presented below.

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)[53]. 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[51]. 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 [43]. Other recommendations include disabling unnecessary processes and plugins, cyber insurance policies, software defined networking [54], system hardening [55], Intelligent Intrusion Detection and Prevention Systems [19], [11] and more.

VI. Predictions and future challenges

Analysing various behaviours of Ransomware attacks and their evolution, one is compelled to conclude that the malware is extremely hard to control. Ransomware now becomming a big dark business itself is seen targetting more and more business organizations and firms dealing with sensitive user data. With the introduction of new technology and trends such as Internet of Things (IoT) and ubiqutous computing, more and more devices are now becoming on-line. This could open up a whole new interest group for Ransomware business, potentially holding these devices 'hostage', blocking user access until a ransom has been paid. These can be softer targets like Android smart televisions, smart watches and hard targets like Industrial Control systems and devices running Mac and Linux operating systems, in an effort to maximise ransom opportunities. In general, as long as there are markets to reach and revenues to gain this trend will always continue to grow. One particularly scary trend seen recently is Ransomware as a Service (RaaS) [56]. This shows that the cyber criminals have been able to evolve the malware to such an extent that they can offer this attack as a service to the world. It also reflects on the failure of apparent great deal of work done by the cyber-security experts and firms to stop these attacks. One instance of this alarming evolution rate is that in early Ransomware period, locker Ransomware falsely claimed to be a law enforcement agency, using social engineering and psychology principles to elicit the victims respect for authority and instilling intimidation. Lately, Ransomware cybercriminals have brazenly and deliberately attacked law enforcement agencies itself and health organisations who had no choice other than to pay the ransom to redeem their data.

With objects becoming smart and increasingly reliant on data-driven algorithms, the systems we interact with for our daily tasks becoming interconnected using smart grids and self-aware using artificial intelligence and machine learning algorithms, the attacks like Ransomware can evolve massively and accordingly. Combining the state of the art currently unbreakable encryption algorithms with generative adversarial networks to attack the machine learning models and then encrypting their current and original model weights can be 'Ransomware 2.0' for the new world. The attackers can demand ransom to restore the previous state and in the mean time the device will continue to produce false data, disrupting the whole network pipeline. Not paying the ransom would result in a waste of long training times and years of work spent in perfecting model architecture. This could be crucial for example for medical imaging domain where machine learning algorithms are quite extensively used [57] and emerging implications as well like insurance fraud. Moreover with such hidden layers in the pipelines of machine learning frameworks, detecting which models are failing (or have been attacked) would be another daunting challenge.

On the other hand, end users today have developed increased security orientation and they are self-protected particularly when it comes to their online presence. Interestingly, psychological studies show that increased security orientation does not warrant users security behaviour [58], [59]. The fact that home users show more affinity towards trusted websites is capitalised by attackers to seek out sites of high reputation, to host malicious software or mimic for phishing and pharming purposes.

VII. Conclusion

Over the years the cyber-security community has evolved towards building better security systems. This evolution was influenced by security incidents, data breaches and other attacks all of which led them to see beyond their illusion of doing an excellent job of protecting the digital resources. New technology aided the process allowing the solutions to be smart, efficient and stronger. Unfortunately, the cyber-criminals on the other side were undergoing a similar evolution, being influenced by the very same factors. They have become more and more innovative in their attacks, knowing with increasing accuracy what vulnerabilities to exploit and where to attack. Ransomware reflects on this evolution. More to their advantage, the products of new and emerging technology opens up a world of new vulnerabilities for them to exploit, making it even more challenging for the cyber-security community to understand and implement the right measures. Moreover, Ransomware now a complete business, thanks to cryptocurrency has more markets to discover extorting millions and bankrupting businesses and individuals. Fortunately, there has been promising advancements in the AI domain towards recognizing and preventing Ransomware where technology giants like Google and the academia finally join hands to cut the chord. In the current age where every company wants to move towards becoming a 'data company', it's about time they realize this growing menace is an urgent threat. The future directions would involve studying about the various influences of home and organisational user's behaviour affected by Ransomware, analyzing how the malware itself behave in it's eco-system and applying pattern recognition to be able to design stronger security solutions to defend against it.

References

[1] Alexander Gostev et al. Malware evolution: January-march, 2005. *Kaspersky Lab Report*, 4, 2005.

[2] Pranav Narain. *Ransomware-Rising Menace to an Unsuspecting Cyber Audience*. PhD thesis, University of Houston, 2018.

[3] Alex Zarifis and Xusen Cheng. The impact of extended global ransomware attacks on trust: How the attackerâ s competence and institutional trust influence the decision to pay. 2018.

[4] Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda. Cutting the gordian knot: A look under the hood of ransomware attacks. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 3–24. Springer, 2015.

[5] Danny Yuxing Huang, Maxwell Matthaios Aliapoulios, Vector Guo Li, Luca Invernizzi, Elie Bursztein, Kylie McRoberts, Jonathan Levin, Kirill Levchenko, Alex C Snoeren, and Damon McCoy. Tracking ransomware end-to-end. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 618–631. IEEE, 2018.

[6] K Zetter. Hacker lexicon: A guide to ransomware, the scary hack that's on the rise. retrieved from security. *Wired Magazine*, 2015.

[7] Kim Zetter. A cyberattack has caused confirmed physical damage for the second time ever. *Wired Magazine*, 2015.

[8] Kevin Savage, Peter Coogan, and Hon Lau. The evolution of ransomware. *Symantec, Mountain View*, 2015.

[9] Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof, and Syed Zainudeen Mohd Shaid. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, 74:144–166, 2018.

[10] Philip O'Kane, Sakir Sezer, and Domhnall Carlin. Evolution of ransomware. *IET Networks*, 7(5):321–327, 2018.

[11] Keith Jarvis. Cryptolocker ransomware. *Viitattu*, 20:2014, 2013.

[12] Leo Kelion. Cryptolocker ransomware has' infected about 250,000 pcs'. *BBC News techology*, 2013.

[13] PB Pathak and Yeshwant Mahavidyalaya Nanded. A dangerous trend of cybercrime: ransomware growing challenge. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume*, 5, 2016.

[14] Nikolai Hampton, Zubair Baig, and Sherali Zeadally. Ransomware behavioural analysis on windows platforms. *Journal of information security and applications*, 40:44–51, 2018.

[15] Alexander Adamov and Anders Carlsson. The state of ransomware. trends and mitigation techniques. In *East-West Design & Test Symposium (EWDTS), 2017 IEEE*, pages 1–8. IEEE, 2017.

[16] Flavio Lombardi and Roberto Di Pietro. Heterogeneous architectures: Malware and countermeasures. In *Secure System Design and Trustable Computing*, pages 421–438. Springer, 2016.

[17] Qian Chen and Robert A Bridges. Automated behavioral analysis of malware a case study of wannacry ransomware. *arXiv preprint arXiv:1709.08753*, 2017.

[18] Matt Burgess. Everything you need to know about eternalbluethe nsa exploit linked to petya. http://www.wired.co.uk/article/what-is-eternal, 2007. Wired (June 28, 2017).

[19] Amin Kharraz, Sajjad Arshad, Collin Mulliner, William K Robertson, and Engin Kirda. Unveil: A large-scale, automated approach to detecting ransomware. In *USENIX Security Symposium*, pages 757–772, 2016.

[20] Aragorn Tseng, Y Chen, Y Kao, and TsungNan Lin. Deep learning for ransomware detection. *IEICE Tech. Rep.*, 116(282):87–92, 2016.

[21] Ronny Richardson and Max North. Ransomware: Evolution, mitigation and prevention. *International Management Review*, 13(1):10–21, 2017.

[22] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. Do or do not, there is no try: user engagement may not improve security outcomes. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 97–111, 2016.

[23] Elizabeth Stobert and Robert Biddle. The password life cycle: user behaviour in managing passwords. In *Proc. SOUPS*, 2014.

[24] Steven M Furnell, Adila Jusoh, and Dimitris Katsabas. The challenges of understanding and using security: A survey of end-users. *Computers & Security*, 25(1):27–35, 2006.

[25] Centers for Disease Control, Prevention, et al. Hipaa privacy rule and public health. guidance from cdc and the us department of health and human services. *MMWR: Morbidity and mortality weekly report*, 52(Suppl. 1):1–17, 2003.

[26] Kyung-shick Choi, TM Scott, and Daniel P LeClair. Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory. *International Journal of Forensic Science & Pathology*, 2016.

[27] Dean F Sittig and Hardeep Singh. A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Applied clinical informatics*, 7(2):624, 2016.

[28] Catalin Cimpanu. Spam accounts for two-thirds of all email volume, and it's still going up. https://www.bleepingcomputer.com/news/security/spam-accounts-for-two-thirds-of-all-email-volume-and-its-still-going-up/, February1 2017. Last Accessed: 13 Jan, 2019.

[29] Salvatore J Stolfo, Eleazar Eskin, Shlomo Herskop, and Manasi Bhattacharyya. System and methods for detecting malicious email transmission, February 2 2010. US Patent 7,657,935.

[30] Symantec. Ransom bucbi [online]. https://www.symantec.com/security-center/writeup/2016-050921-2018-99 , May7 2016. Last Accessed: 13 Jan, 2019.

[31] Aaron Zimba. Malware-free intrusion: a novel approach to ransomware infection vectors. *International Journal of Computer Science and Information Security*, 15(2):317, 2017.

[32] Ankit Singh. What symantecs intrusion prevention system did for you in 2015. *Symantec Security Response*, 2016.

[33] Aditya K Sood and Richard J Enbody. Malvertising–exploiting web advertising. *Computer Fraud & Security*, 2011(4):11–16, 2011.

[34] Karen McDowell. Now that we are all so well-educated about spyware, can we put the bad guys out of business? In *Proceedings of the 34th annual ACM SIGUCCS fall conference: expanding the boundaries*, pages 235–239. ACM, 2006.

[35] Savita Mohurle and Manisha Patil. A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5), 2017.

[36] Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin RB Butler. Cryptolock (and drop it): stopping ransomware attacks on user data. In *Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on*, pages 303–312. IEEE, 2016.

[37] M. Burgess and J. Ieraci. Telstra security report. https://www.telstraglobal.com/TelstraCyberSecurityReport2017Whitepaper.pdf, May7 2017. Last Accessed: 13 Jan, 2019.

[38] Teryl Taylor, Xin Hu, Ting Wang, Jiyong Jang, Marc Ph Stoecklin, Fabian Monrose, and Reiner Sailer. Detecting malicious exploit kits using tree-based similarity searches. In *proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*, pages 255–266. ACM, 2016.

[39] Martin Längkvist, Lars Karlsson, and Amy Loutfi. A review of unsupervised feature learning and deep learning for time-series modeling. *Pattern Recognition Letters*, 42:11–24, 2014.

[40] R Vinayakumar, KP Soman, KK Senthil Velan, and Shaunak Ganorkar. Evaluating shallow and deep networks for ransomware detection and classification. In *Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on*, pages 259–265. IEEE, 2017.

[41] Molra J West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, and Robin Ruefle. Handbook for computer security incident response teams (csirts). Technical report, Carnegie-mellon univ pittsburgh pa software engineering inst, 2003.

[42] Anca Sailer, Hidayatullah Habeebullah Shaikh, and Yang Song. System and method for incident management enhanced with problem classification for technical support services, January 29 2013. US Patent 8,365,019.

[43] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. Computer security incident handling guide. *NIST Special Publication*, 800(61):1–147, 2012.

[44] Cath Everett. Ransomware: to pay or not to pay? *Computer Fraud & Security*, 2016(4):8–12, 2016.

[45] A. Buckingham. Avg announces 6 new tools to free your data from ransomware. http://betanews.com/2016/07/01/avg-announces-6-new-tools-to-free-your-datafrom-ransomware/, July1 2016. Last Accessed: 13 Jan, 2019.

[46] Hua Ye, WeiChao Dai, and Xiaodong Huang. File backup to combat ransomware, April 19 2016. US Patent 9,317,686.

[47] M Korolov. 93% of phishing emails are now ransomware. https://www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-now-ransomware.html, 2016. Accessed October 12,2016.

[48] Mohammad Ali Hadavi, Hossein Shirazi, Hasan Mokhtari Sangchi, and Vahid Saber Hamishagi. Software security; a vulnerability activity revisit. In *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, pages 866–872. IEEE, 2008.

[49] Kenneth J Knapp, Thomas E Marshall, R Kelly Rainer, and F Nelson Ford. Information security: management's effect on culture and policy. *Information Management & Computer Security*, 14(1):24–36, 2006.

[50] Mario Silic and Andrea Back. Shadow it–a view from behind the curtain. *Computers & Security*, 45:274–283, 2014.

[51] CM Alstin Van. Ransomware: It's as scary as it sounds. but with security best practices, you can fight back. *Health management technology*, 37(4):26–27, 2016.

[52] Federal Bureau of Investigation. Incidents of ransomware on the rise: protect yourself and your organization. https://www.fbi.gov/news/stories/ransomware-on-the-rise, April 29 2016. Accessed October 12,2016.

[53] Manos Antonakakis, Roberto Perdisci, Yacin Nadji, Nikolaos Vasiloglou, Saeed Abu-Nimeh, Wenke Lee, and David Dagon. From throw-away traffic to bots: Detecting the rise of dga-based malware. In *USENIX security symposium*, volume 12, 2012.

[54] Krzysztof Cabaj and Wojciech Mazurczyk. Using software-defined networking for ransomware mitigation: the case of cryptowall. *IEEE Network*, 30(6):14–20, 2016.

[55] Raoul Strackx and Frank Piessens. Fides: Selectively hardening software application components against kernel-level or process-level malware. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 2–13. ACM, 2012.

[56] V Kremez. Ransomware as a service: Inside an organized russian ransomware campaign (flashpoint)(p. 9). *Flashpoint. Recuperado a partir de https://www. flashpointintel. com/library*, 2016.

[57] Samuel G Finlayson, Isaac S Kohane, and Andrew L Beam. Adversarial attacks against medical deep learning systems. *arXiv preprint arXiv:1804.05296*, 2018.

[58] Doohwang Lee, Robert Larose, and Nora Rifon. Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, 27(5):445–454, 2008.

[59] Noriaki Yoshikai, Shun-ichi Kurino, Ayako Komatsu, Daisuke Takagi, Masashi Ueda, Atsuo Inomata, and Hideo Numata. Experimental research on personal awareness and behavior for information security protection. In *Network-Based Information Systems (NBiS), 2011 14th International Conference on*, pages 213–220. IEEE, 2011.