Contemporary Cybercrime: A Taxonomy of Ransomware Threats & Mitigation Techniques

Ibrahim Nadir, Taimur Bakhshi
Department of Computer Science
National University of Computer & Emerging Sciences
Lahore, Pakistan
ibrahim.nadir@nu.edu.pk

***Abstract*— An ever-increasing number of Internet-enabled devices over the past decade have highlighted the requirement for robust cybersecurity primitives to effectively deal with contemporary forms of cybercrime. Among the recent cybercrime threat canvass, ransomware has come to limelight as a prominent form of crypto-virus, aiming to hamper everyday user device operation through unsolicited encryption of device data. The perpetrators on successfully encrypting user data, require a payment or ransom, often in the form of digital currencies to furnish a decryption key. Depending on the urgency and criticality of data restoration, both novice users as well as corporate organizations have been observed to pay significant compensations for reinstating normal operation, often without any post-payment assurances. The present paper seeks to review the history and recent evolution of ransomware attacks, providing a detailed taxonomic classification of the inherent attack vectors and currently available mitigation techniques. Furthermore, preventive recommendations are discussed to aid users and organizations in securing devices against ransomware threats. Finally, financial and long-term implications of making ransom payments, along with online resources made available by security and law-enforcement concerns are overviewed to increase end user awareness and equip them against this increasingly successful form of recent cybercrime.**

Keywords*— *Ransomware, malware, cybercrime, bitcoin

I. INTRODUCTION

The term ransomware is derived from a combination of two words ransom and malware. Essentially, any malware that steals some user device functionality and requires the user to pay a ransom for service restoration falls within the domain of ransomware. Since the inception of crypto-virology, several different forms of ransomware have been developed. Starting from nascent scareware tactics, coercing users to buy a much-needed antivirus software resulting in system lockdown, ransomware has progressed to several sophisticated variants. A recent example is Reveton, imitating as a message from a law enforcement agency and advising users to pay a penalty for prior unlawful usage or face system lockdown [1]. Another prominent example includes the infamous CyrptoLocker encrypting user data using a strong encryption algorithm such as RSA and AES [2]. Using exceptionally long RSA keys (e.g., 2048 bits), decryption becomes close to impossible [3]. While a number of commercial tools offer file decryption, mostly prove ineffective leaving the user without options except paying ransom to the attackers [4]. In addition to user computers, ransomware can also target smartphones. LockerPin [5] for example, is ransomware targeting android devices. The malware changes the device PIN demanding a ransom money to be paid to the perpetrators for unlocking the device. A variant of LockerPIN is the LeakerLocker [6] that takes a backup of user data and demands ransom otherwise threatening to release personal information of the user [7] .

Ransomware attackers may demand payment in different ways, however, the prevalent method is to make and receive payments in the form of digital or cryptocurrency such as Bitcoin [8]. The payments are difficult to trace and form an ideal choice for attackers wanting anonymity [9]. Other forms of payment may include forcing the user to buy a product on a website, clicking on links, etc. so the attacker can generate revenue from such interactions. With increase in ransomware attacks, the average ransom demand has increased to almost $1077 by the end of 2016 from a mere $294 in 2015, a substantial increase of almost 266% in just one year [10]. Along the same timeline the number of ransomware attacks increased from 18% in January 2016 to around 66% in November 2016 [11]. The emergence of technologies such as Internet of Things (IoT) means that the number of such attacks will continue to increase as attackers find more vulnerable devices online yielding additional schemes of forcing users into paying ransom for service normalization [12]. The present paper reviews the state-of-the-art in ransomware technologies discussing in detail the existing attack vectors and available mitigation techniques. Additionally, recommendations are made for preventing users from online victimization by including best practices and the paper also overviews the online resources available to victims of ransomware.

The remaining of this paper is organized as follows. Section 2 highlights the history of ransomware and crypto-virology. Section 3 discusses and classifies the prevalent ransomware attacks according to threat propagation and means of ransom payment. Section 4 explores the available ransomware mitigation techniques detailing best practices. Section 5 reviews the financial implications and long-term consequences of ransomware payments, as well as detailing the online resources made available to increase ransomware awareness and help victims. Final conclusions are drawn in section 6.

978-1-5386-1370-2/18/$31.00 ©2018 IEEE

II. History

As recent as it sounds, the history of ransomware goes back to 1989 when Joseph L. Popp, a revolutionary biologist from Harvard, first created a malware called PC Cyborg [13] [14]. Popp created and sent 20,000 copies of diskettes to World Health Organization's attendees. The malware encrypted files on the computer after 90th reboot and demanded a ransom of $189 to a postal address in Panama. A brief history of ransomware development timeline through the previous years is depicted in Fig. 1. The first modern ransomware subsequently, came in the form of fake spyware or performance enhancement tools which not only infected Microsoft Windows OS but also MAC OS X. The fake tools promised to solve certain issues with the operating system by either deleting some malware or fixing some registry issues for which it demanded a relatively small amount of money (between $30 and $90). After the amount was paid, nothing really happened, as in reality there were no issues to be fixed. Later on the GPCode Trojan appeared that encrypted files using symmetric and asymmetric keys in different variants. Although the initial variants were flawed and decryption tools worked well against the Trojan, the developers of GPCode further refined and improved the malware learning from mistakes in previous versions [1].

By the year 2006, Archiveus Trojan appeared that copied files of "My Documents" folder to a password protected zipped file and deleted the original documents [5]. The victims were ransomware attacks continued, with the third quarter of 2011 reporting an increase of 50,000 ransomware samples when compared to the first quarter. Most of the ransomware code was however, updates and copies of previous versions. A new variation of crypto-virus surfaced in 2012, named Reveton [1]. The idea was to use scareware tactics, displaying a fake message to end users from local law enforcement agencies giving alarming notices of unlawful computer usage such as watching child pornography or copyright infringement. The victims were advised to pay a penalty as a result of this purported illegal activity. Another milestone in 2012, was the formal introduction of the word "ransomware" in Oxford English Language dictionary [15]. The first major case of ransomware affecting number of global users surfaced in the form of CyrptoLocker malware in 2013 [16][17]. CryptoLocker used military grade encryption of RSA-2048 bits to encrypt files. While previous ransomware attacks generally used to leave the decryption key on victim's computer making it feasible to quickly provide the key on payment as well as provide system administrators a means to retrieve the local key, the authors of CryptoLocker improved on this scheme and stored the decryption key on a server. Remote storage of the key made it quite impossible for users to decrypt the data unless the key was captured at the time of encryption. Moving on 2014, saw the release of a number of ransomware particularly CryptoWall [18] and CryptoDefence [19][16]. Both forms of malware used a strong symmetric encryption employing AES. To fully exploit the user and coerce them into making payments, a portion of the victim's data was allowed to be decrypted to prove that the user data could be fully recovered if a payment was made. An estimated 500,000 computers were globally infected by either malware. Furthermore, the attackers also started using anonymous networks like TOR [20] for communication and new technologies like Bitcoins [8] to further improve and streamline the ransom business model. The evolution of new ransomware threats continued, TelsaCrypt [18] was released in 2015, again using AES encryption, along with revival of Reveton and CryptoWall variants. TelsaCrypt is capable of encrypting more than 170 file extensions and uses Bitcoins as the currency of choice for ransom payments. Quite recently, in 2016, it has been reported that almost 65% to 70% of all malware used comprises of ransomware [10]. Some new names to the existing list of crypto-viruses include Locky [21][10], Cerber [21][10], CryptXXX [21][10] with a substantial increase in ransom demenda ranging between $500 all the way up to $1200. On a separate strand, the detection rate of ransomware by antivirus tools increased by almost 36% during 2016 in comparison with 2015. Additionally, approximately 101 new families of ransomware were detected in 2016 compared to 2015 where 30 new families were discovered [10]. The most recent and notorious attack in 2017 was of the ransomware WannaCry [13] which infected over 200,000 computers and demanded a ransom of $300. The Philadelphia [22] malware another recent example mainly targeted health industry. Some other worthy names were Kirk [23] that mainly encrypted files and Doxware [24] which was much like LeakerLocker, threatening to publish private user data online with malicious intent. Overall, the ransomware trend has been on the rise gaining momentum in recent years. Up until now, the United States has been the most affected country by ransomware with a total of 28% out of all global attacks being carried out in USA, Canada being the runner-up with a 16% global share of ransomware attacks in 2016. Most of the attacks were targeted

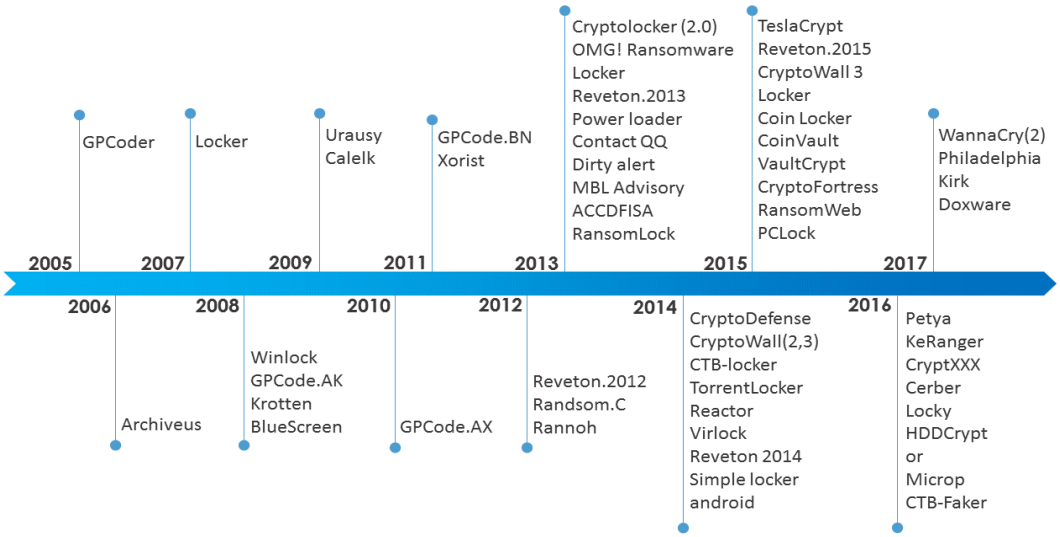

Fig. 1. Timeline depicting Ransomware evolution

at individuals (57%) rather than enterprises (43%) [21]. As mentioned earlier, the incorporation of IoT in the end user domain would increase further chances of users falling prey to ransomware attacks. The requirement for end user awareness in recognizing ransomware attacks, availability of online tools to aid users in dealing with such cybersecurity threats and robust security software is therefore, very much required. The next section classifies the prominent ransomware attack vectors.

III. RANSOMWARE CLASSIFICATION

Ransomware attacks can be classified with regards to the type of attack vectors employed for propagation as well as the mode of payment employed. A brief description and properties of each category is listed in Table 1. Divergent vectors exist in each category having its own relative merits. While sending spam Emails containing malicious attachments might be dynamic and cheap means of propagation it remains technically novice compared to the sophisticated affiliate programs offering ransomware-as-a-service. Affiliate programs rely on existing botnet networks and brokers to propagate malware. Each attack vector comes with its own set of social engineering tactics to lure the user into submitting to the delivery mechanism. Similarly, ransomware attackers may utilize the services of a third-party website to solicit money from the victim or use a more direct approach of depositing/transferring cryptocurrency such as Bitcoins in the attacker's wallet. Further classification in the two broadly defined categories is discussed in the following sub-sections.

A. Ransomware Propagation

Primarily, ransomware attacks can be generally classified in three different categories in terms of the crypto-virus propagation mechanism: as a combination of pre-packaged tools named exploitation kits (EK), affiliate programs providing ransomware service and malware campaigns.

- **Exploitation Kits:** An exploitation kit (EK) is a pre-packaged bundle of tools that can be purchased or leased for the purpose of distributing general malware including ransomware [25] [26]. The code is engineered to serve as an open communication channel that can be used by attackers to communicate with the compromised system and administer remote instructions. Authors of new ransomware therefore, do not need to go hunting or developing new delivery system but use an EK to distribute the malware to victims. EK usually builds on browser vulnerabilities and security holes to inject malicious JavaScript code which carries out a series of sequential attacks until one is successful. One of the most popular EK has been the Angler exploit kit used by attackers who lack deep technical knowledge and need automated web-based attack capability. According to a vulnerability analysis report by Proofpoint security [27], as many as 10 million Android devices are thought to have been compromised by EKs letting attackers take control of user devices. Exploitation kits greatly ease the ransomware work of finding known bugs in web browser plug-ins and the working procedure to turn such bugs in to further exploits and to entice victims.

- **Affiliate Programs:** At present ransomware attackers do not need to write complete malware code, run hosting servers and keep track of payments from victims, retrieve and harvest user information such as passwords as it can all be outsourced [28]. The entire syndicate which has come to be known as Crimeware-as-a-Service allows individuals to specialize in one area of cybercrime business. Affiliate programs allow attackers to utilize existing malware and support infrastructure to deliver the infectious vectors with a great deal of effectiveness and with simplicity [29].

TABLE I. RANSOMWARE THREAT CLASSIFICATION

Parameter	Properties	
	Primary Approaches	***Description***
Propagation	Exploitation Kits	Pre-packaged bundle of tools.
	Affiliate Programs	Outsourced code development, propagation.
	Malvertising Campaigns	Email based spam campaigns targeting users.
Payment	Direct Payment	Wire transfers, cryptocurrency payments.
	Indirect Payment	Pre-paid vouchers, online buying and premium rate calls/SMS.

- **Malvertising and Spam Campaigns:** Despite the availability of sophisticated EK and affiliate programs, the use of basic malware advertising (malvertising) and spam Email campaigns offering cheap and convenient method for attackers to generate attack vectors cannot be ruled out. Highly localized Email messages and advertisement campaigns using social engineering tactics may lure victims into downloading and opening an Email attachment [30] or visiting a relatively nascent local supplier resulting in system compromise. One recent ransomware referred to as CryptoLocker.f Trojan (or Locky), dominates Email campaigns. Among the attacks launched using emails containing malicious attachments, 69% reported containing the Locky virus in second quarter of 2016 compared to 24% in the first quarter [31][21]. Carefully planned campaigns employing local information and high degree of grammatical correctness of the respective languages used may compromise users not having enough awareness to distinguish between tell-tale social engineering indicators [32] [30].

B. Ransomware Payment

Ransomware classification according to the mode of payment can be generally identified along the method of payment collection, direct or indirect. Details regarding each classification category are described in the following sub-sections.

- **Direct Payments:** Further to the de-facto method of attackers receiving payments using cash transfers, the use of cyber currency such as Bitcoins is recently on the rise. Bitcoin refers to a digital payment and asset tracking system which was released as an open source project in 2009 [8]. The bitcoin exchange system uses peer-to-peer networking and transactions take place directly between individuals without an intermediary or broker. Verification of transactions is via network nodes and all exchanges are recorded in a public accounting (distributed) ledger referred to as blockchain [33]. Financial regulatory bodies consider bitcoin to be a virtual currency (cryptocurrency) which is decentralized and supposed to be the largest among virtual currencies in terms of its market share. Bitcoin is often cited as the payment method of choice in ransomware owing a significantly difficult to investigate and trace trail the transactions may leave behind without direct affiliation with the attackers. According to a report by Citrix [12], a number of companies based in the United Kingdom are stockpiling on bitcoins to pay attackers in the event of a successful ransomware compromise. Of the 250 IT specialists surveyed by Citrix, almost 33% advised having a stockpile of bitcoins to serve ransomware [31][34].

- **Indirect Payments:** Indirect forms of payment can also be employed in ransomware attacks, where the attacker is concerned about a high level of anonymity. Some of the prominent methods include the use of pre-paid voucher cards,

online product purchases as well as calls to premium rate numbers. While using pre-paid vouchers as a payment mode, attackers advise the victims to make payments using voucher cards bought from different retail outlies. Since the cards have to be purchased by the victims the transaction again leaves minimal (if any) trail to the attackers. Prepaid voucher cards have been quite noticeable in some high-profile ransomware investigations. Other forms of payment include coercing users in to buying online products from a particular website to redeem their computing equipment. The tactic has mostly been employed in scareware and in addition to requiring users to buy products may also allow the attacker to capture user payment card details for subsequent exploitation [35][36]. Finally, premium rate calls and texts have also been reported as the payment method of choice in ransomware. Attackers advise victims to call premium rate numbers in geographically dispersed and expensive call locations to get validation code for locked services e.g. Windows expiration, etc. Calls and text messages in turn yield profits for the attackers with most end points being in the same region as them while calls and texts are routed through foreign countries [37]. The next section overviews the presently available mitigation techniques against the classified ransomware attack vectors.

IV. Mitigation Techniques

Over the years, a number of solutions have been suggested to avoid or recover from ransomware threats. With each solution though, the authors of ransomware came with new techniques of attacks introducing new variations and improved attacking methodologies. The number of ransomware detections increased from 933 in 2015 to 1271 in 2016 per day [10]. Due to this increase, it is almost impossible for any antimalware software to catch every ransomware variant. Even if the signature for a particular ransomware is present, it maybe encrypted and fly under the radar of security tool. Providing adequate security to the system using a number of techniques may prove helpful if not completely secure. No matter what security tool or technique is used, an updated version of it must always be ensured. Be it operating system or security software, the cybersecurity industry recommends updates and patches at all times. Below we present some techniques which mitigates against ransomware and can also help in recovery if a ransomware attack does execute.

A. Backup of data

Backing up of data against any security attack is pleasant[38][39][40][41][42]. Ransomware business relies on the idea of forcing users to pay ransom to retrieve their sensitive data. If regular (recoverable) backups are maintained by user ideally on external resources (like cloud, USB, hard drives), the ransomware attack is almost useless. A number of cloud solutions are available which lets you synchronize your computer's data with a redundant copy on the cloud. In this case, even if the data is encrypted by ransomware, an online copy of it can still be retrieved. Some cloud solutions like Dropbox can retrieve even older versions of the data. In case the data gets encrypted or deleted and the desktop tool synchronizes the ransomware attacked data, the Dropbox can retrieve the original data [43].

B. Antivirus & security tools

Antivirus and related security software is an essential security measure against the ransomware. Although these tools may only be resistant against existing threat signatures, some advanced tools have machine learning capabilities which can do comprehensive analysis against the ransomware. Updating the security tools is indispensable no matter which security software is used against all kind of threats [21][44][45]. ShieldFS, a security tool, which detects ransomware-like behaviour and automatically backs up files making modern operating systems more resilient [46].

C. Updating all software & operating system

All operating systems updates and patches are not for security purposes but a lot are. Therefore, regular automatic updating and patching is compulsory to avoid new vulnerabilities that can be exploited [47]. Ransomware attackers look for weaknesses in operating systems or application software in order to successfully execute their attacks. During its infection, one of the goal of a well-known ransomware called CryptoWall 3 is to disable Windows Update Service and Windows defender [19][48][42].

D. Email security

Email has been one of the most extensive infection vector for the distribution of ransomware [9]. With the reduction in the Exploit Kits usage and increased capturing capability of antimalware software, email remains an attractive infection vector [47]. A decent email filter can minimize the percentage of attacks by a decent number [21][48]. Of course, the user's personal vigilance is important alongside security tools and filters. The mailing server also has an important role to play in this regard. Some basic spam filters are always installed on a reliable mailing server [49]. The user, however, has to be careful at all times not to download or click any suspicious files from both unknown and known contacts.

E. Access Control/Authorization and Permissions

Different levels of permissions and access should be implemented in enterprises. Depending upon the user, the level of privilege must be assigned. Even privileged users should be working with an account that has lower level of authorization because everyone makes mistakes. Access control and permissions can be implemented via an intrusion prevention system such that roles and policies are assigned in the lowest possible privileges for accomplishing tasks [4]. Files and access permissions need to be carefully worked out allowing only necessary accounts access to make changes such as encryption because a lot of recent ransomware families depend on encryption. Since ransomware is also attacking smartphones, it is important to note the permissions requested by a ransomware when installing an application from app store [21] [13]. At the same time, smartphone applications must be updated regularly. In businesses and offices, personal smartphones, tablets, and laptops of staff and employees should be maintained under a security policy. All devices, as such, should be managed by the network since they are a part of the network [16].

F. Application Whitelisting

Effective system administration requires only a certain set of trusted applications to be whitelisted in the system registry for automated updating and making changes to system parameters and other files [50][51]. This greatly limits the extent to which downloaded malware. For example, via web browser plug-ins would propagate and make further changes to user data. In addition to applications, users also need to be wary of the add-ons to popular web browsers allowing limited control by customizing plug-in features.

G. Volume Shadow Copies

In Windows systems, if the file system used is NTFS, one of windows service takes manual or automatic backup of files called Volume Shadow Copies. Also referred to as Volume Snapshot Service (VSS) can be used to recover some portion of the data if not all. If an implementation of ransomware is not sophisticated, it will ignore deleting volume shadow copies of a drive and a portion of the data can be recovered even after encryption [45]. Detailed oriented ransomware, for example TeslaCrypt deleted windows shadow volume copies [52].

H. Decryption tools

A number of free tools are available online for free to decrypt ransomware encrypted data. Companies like AVG, AVAST [2], Kaspersky, and Windows Defender etc. provide decryption tools. Although, they would work only if the encryption techniques, algorithm or key used by the authors of ransomware are not strong enough, the user might still have a chance of getting the data back without paying any ransom.

I. Data recovery tools

Once data is deleted from a file system, it may not be completely lost until it is replaced by new data on the same drive. Victims of ransomware whose data is encrypted or lost can try to recover their deleted data using a data recovery tool [19].

The following section details the financial implications for victims who go ahead and making ransom payments to restore data, negotiation trends as well as online resources to aid and educate users about ransomware.

V. Attack Implications & User Options

During the past few years, ransomware victims have paid huge amounts as ransom to the attackers. Ransomware has further evolved with the advent of "Ransomware-as-a-service (RaaS)", enabling even a script kiddie to successfully execute a ransomware attack using automated tools. The author of the ransomware tool gets a percentage of the ransom paid by the victim and the rest of the money is paid to the script kiddie. In sophisticated scenarios, even a customer support is offered to victims for ransom payment and negotiation [53]. In view of increasing number of ransomware attacks, key questions arise for the victim, whether to pay ransom in the hope of quick recovery of data, can the ransom money be negotiated, and finally how to report the cybercrime. The following sub-section briefly discuss each of these concerns.

A. Implications of Paying Ransom – To Pay or Not to Pay!

If individuals or businesses do not have any backup policy, a successful ransomware attack boils down to this question: whether to pay the ransom or not? Also, after payment, will the data be recoverable? What kind of guarantees exist that the cybercriminals will provide a key that can successfully decrypt the data after the ransom is paid. The recent ransomware WannaCry [13] is an example of such problems where the ransomware had no way of associating an ID with the ransom payer. So even after the payment was made, a victim's data was never recovered. According to a security report by Symantec, globally around 34% of the victims end up paying ransom. The average is quite high in the US, where 64% of victims pay ransom. Paying ransom emboldens the attacks and inevitably the US has reported the highest number of recent ransomware attacks [10]. It is therefore, advisable not to pay ransom. Some of the compelling reasons for not paying are listed as follows.

- The basic business model behind ransomware relies on and develops because the victims pay ransom. If there are no payments made, the business model would collapse.
- Despite making payments there are no guarantees whatsoever, that the victim might not get the data back.
- Once a payment has been made, the attackers are well aware of the victim's vulnerability as well as capacity to make a payment. Hence the possibility of future attacks on the same victim cannot be ruled out.

B. Negotiation with Attackers – Any guarantees!

Getting less ransom is better than no ransom at all, that is generally the basic psyche behind ransomware attacks. Typically, negotiations with attackers have resulted in payments in a number of occasions where victims were either able to buy more time for making payment arrangements or successfully reduce the amount of ransom to be paid. F-Secure cybersecurity report states that on average, 3 out of 4 ransomware criminals negotiate providing an average of 29 percent discount [47]. A basic depiction of some popular ransomware families and payment and negotiation trends as per security firm F-Secure [47] is provided in Table 2. Relatively recently a high-profile ransom payment case surfaced, that of the Hollywood Presbyterian Medical Center where attackers demanded a ransom of $3.7 million owing the sensitivity of medical data that was compromised. The victims were reduced to the usage of pen and paper to maintain daily reports and negotiated their way to $17,000 as ransom for normalizing operations [13]. Although being able to successfully obtain discounts might seem a feasible idea for victims at first, at the same time this would lure more victims into paying ransom. A victim able to pay a ransom of $100 to get things restored might not be able to pay $300. Hence the attacker can benefit from providing discounted ransoms and coercing more victims to pay in the long term. Negotiation, in any case, is a sign of a victim ready to pay some amount and that is reason some attackers have also started hosting websites to provide "customer support" to victims for negotiation [54]. Nonetheless payment of ransom does not guarantee that the data could be restored, and essentially the victim could end up in a situation where payment has been made but data remains in encrypted or locked state. To make matter worse, on receiving the payment, attackers might ask for additional money hoping to get something extra from the victim. The following sub-section highlights some online resources specifically for the education and support of end users about this emerging cybercrime.

C. Support Resources

Since the recent re-emergence of ransomware, several initiatives have been taken both by information security organizations as well as law enforcement agencies to help raise awareness about this peculiar cybercrime. A brief list of presently available resources to aid the general user population as well as ransomware victims is detailed as follows.

- **No More Ransom Project:** The "No More Ransom" website has been an initiative by two law enforcement agencies, the National High-Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre along with two cyber security companies – Kaspersky Lab and McAfee [55]. The primary objective of the project is to help victims of ransomware retrieve their encrypted data without having to pay the criminals [55]. The project provides general

TABLE II. SAMPLE PAYMENT NEGOTIATION TRENDS (F-SECURE 2017)

Ransomware Family	Starting Demand	Lowest Demand	% Discount
CERBER	$30	$30	0%
CRYPTOMIX	$1900	$635	67%
JIGSAW	$150	$125	17%
SHADE	$400	$280	30%
Average Value	$620	$267.5	29%

information about ransomware, prevention advice, decryption tools as well as an easy to use form to record the traits of ransomware type being experienced by the user (including the option to upload the encrypted file) and advise on the available data restoration options.

- **FBI Ransomware Prevention & Response:** The US department of Justice, the Federal Bureau of Investigation, have set up dedicated webpages under the cybersecurity section to educate and provide users with information regarding ransomware threats [56]. Among the range of helpful information provided include documents that provide aggregate information about already existing federal government and private industry best practices and mitigation strategies. The documents are targeted both at general audience as well as corporate concerns to limit and prevent ransomware incidents.

- **Internet Crime Complaint Center (IC3):** The IC3 accepts online Internet crime complaints from the actual ransomware victim and also from a third party [57]. The center falls within the auspices of FBI and encourages users to share their ransomware experience. Some of the data required includes the date and specifics of the incident. The general instructions also provide additional information primarily educating the user against making ransomware payments which might embolden the adversary and as discussed earlier are still not guarantee for obtaining a decryption key.

- **National Cybercrime Security Center (NCSC, UK):** The national cybercrime security center in the United Kingdom, has dedicated webpages offering support and raising awareness about ransomware [58]. The pages included general information about ransomware, types and mitigation techniques or best practices. As a matter of policy, NCSC states that the matter of making a payment is entirely up to the victim, however, encourages against it due the same reasons of encouraging further propagation and increasing attacker confidence cited earlier. The website also contains a link for victims to report ransomware attacks and provide the relevant details of the cybercrime.

Overall, an increasing number of security firms and commercial organizations are also actively participating and creating online resources, wiki pages and helpful FAQs to aid users in understanding and dealing with ransomware.

VI. CONCLUSION

The seriousness of ransomware threats to individuals and businesses cannot be negated especially in light of the recent hype this peculiar form of cybercrime has created quite recently. While the basic technique and schemes employed for ransomware have existed for over a decade, an ever-increasing number of Internet enabled user devices have created new attack vectors for the perpetrators. The present paper provided a classification of ransomware attack vectors along the means of attack propagation as well as the mode of payment. Furthermore, mitigation strategies were considered in detail to help users against ransomware threats and the available recovery techniques in case of a successful attack were also discussed. It was noted that the key to mitigating or reducing the number of successful ransomware attacks directly relates to a high level of user awareness and an appropriate response. Key online resources provided by law enforcement agencies were also detailed with the aim to aid users in furthering their knowledge about ransomware. It is anticipated that future evolution of Internet connected devices, especially the inclusion of Internet of Things (IoT), adequate level of user knowledge, effective security tools and timely availability of online resources is required to minimize the threat posed by ransomware attacks.

REFERENCES

[1] N. Hampton and Z. A. Baig, "Ransomware: Emergence of the cyber-extortion menace," 2015.

[2] "AVAST, 'Free Ransomware Decryption tools'.," *https://www.avast.com/ransomware-decryption-tools*. .

[3] K. Zetter, *Hacker lexicon: A guide to Ransomware, the scary hack that's on the rise*. Retrieved from Security, https://www. wired. com/2015/09/hacker-lexicon-guideransomware-scary-hack-thats-rise, 2015.

[4] F. Mercaldo, V. Nardone, A. Santone, and C. A. Visaggio, "Ransomware steals your phone. formal methods rescue it," in *International Conference on Formal Techniques for Distributed Objects, Components, and Systems*, 2016, pp. 212–221.

[5] M. H. U. Salvi and M. R. V. Kerkar, "Ransomware: A cyber extortion," *ASIAN J. Converg. Technol. AJCT-UGC List.*, vol. 2, 2016.

[6] "McAfee, 'LeakerLocker: Mobile Ransomware Acts Without Encryption.'" .

[7] "Philip B., 'Beware LeakerLocker: Ransomware That Locks Your Mobile.'" .

[8] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*. 2008.

[9] J. Hernandez-Castro, E. Cartwright, and A. Stepanova, "Economic Analysis of Ransomware," 2017.

[10] Symantec, "ISTR: Internet Security Threat Report," 22, Apr. 2017.

[11] MalwareBytes Lab, "'State of Malware Report,'" 2017.

[12] S. Cobb, *RoT: Ransomware of Things*. Trends, 2017.

[13] T. A. Mattei, "Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack," *World Neurosurg.*, vol. 104, pp. 972–974, 2017.

[14] "Virus Bulletin: The Authoritative International Publication on Computer Virus Prevention, Recognition, and Removal. Abingdon, England: Virus Bulletin, 1900. Print.," 2005.

[15] J. Jouhal, "The rise of ransomware and how to avoid being held hostage. New Statesman, Spotlight on cybersecurity," Feb. 2017.

[16] R. Richardson and M. North, "Ransomware: Evolution, Mitigation and Prevention," *Int. Manag. Rev.*, vol. 13, no. 1, p. 10, 2017.

[17] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. 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*, 2015, pp. 3–24.

[18] J. Wyke and A. Ajjan, "The Current State of Ransomware," *SophosLabs Tech. Pap.*, 2015.

[19] K. Savage, P. Coogan, and H. Lau, "The evolution of ransomware," *Symantec Mt. View*, 2015.

[20] D. McCoy, K. Bauer, D. Grunwald, T. Kohno, and D. Sicker, "Shining light in dark places: Understanding the Tor network," in *International Symposium on Privacy Enhancing Technologies Symposium*, 2008, pp. 63–76.

[21] "ISTR ransomware & business 2016."

[22] L. Abrams, "The Philadelphia Ransomware offers a Mercy Button for Compassionate Criminals," *https://www.bleepingcomputer.com/news/security/the-philadelphia-ransomware-offers-a-mercy-button-for-compassionate-criminals/*. .

[23] L. Abrams, "Bleeping Computer, 'Star Trek Themed Kirk Ransomware Brings us Monero and a Spock Decryptor!,'" *https://www.bleepingcomputer.com/news/security/star-trek-themed-kirk-ransomware-brings-us-monero-and-a-spock-decryptor/*. .

[24] Panda Security, "Doxware, the Scary New Evolution of Digital Hijacking.,"

http://www.pandasecurity.com/mediacenter/security/doxware-evolution-digital-hijacking/. .
[25] A. B, S. G.V.B, V. A, and S. H, "Ransomware: A Rising Threat of new age Digital Extortion," *Indian J. Sci. Technol.*
[26] M. J. Sheehan, R. Cheng, and D. Gray, "Ransomware attacks present growing threat," *Manag. Healthc. Exec.*, vol. 26, p. 7, 2016.
[27] "Proofpoing Ransomware Exploit Kits Summarization." .
[28] J. Wyke, "The zeroaccess botnet: Mining and fraud for massive financial gain," *Sophos Tech. Pap.*, 2012.
[29] Kafeine, "'Crypto Ransomware' CTB-Locker (Critroni.A) on the rise'." 2014.
[30] I. M. Shohet and S. Lavy, "Healthcare facilities management: state of the art review," *Facilities*, vol. 22, no. 7/8, pp. 210–220, 2004.
[31] "Ransomware: Profitable for Criminals, Hard to Stop for Enterprises, Citrix," *https://www.citrix.com/blogs/2016/06/15/ransomware-profitable-for-criminals-hard-to-stop-for-enterprises/*. .
[32] X. Luo and Q. Liao, "Awareness education as the key to ransomware prevention," *Inf. Syst. Secur.*, vol. 16, no. 4, pp. 195–202, 2007.
[33] "Bitcoin Innovative Payment Network and a New Kind of Money," *https://bitcoin.org/en/*. .
[34] "CoinDesk on Citrix Survey, BTC stocks in UK businesses," *http://www.coindesk.com/survey-uk-bitcoin-ransomware/*. .
[35] C. Van Alstin, "Ransomware: It's as scary as it sounds. But with security best practices, you can fight back.," *Health Manag. Technol.*, vol. 37, no. 4, p. 26, 2016.
[36] T. Yang, Y. Yang, K. Qian, D. C.-T. Lo, Y. Qian, and L. Tao, "Automated detection and analysis for android ransomware," in *High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on*, 2015, pp. 1338–1343.
[37] "Police warn of extortion messages sent in their name," *Helsingin Sanomat*, 09-Mar-2016.
[38] A. L. Young and M. Yung, "Cryptovirology: The birth, neglect, and explosion of ransomware," *Commun. ACM*, vol. 60, no. 7, pp. 24–26, 2017.
[39] G. Rhoades, "Ransomware and other malware," *The Indexer*, vol. 34, no. 3, pp. 126–128, 2016.
[40] S. Mustaca, "Are your IT professionals prepared for the challenges to come?," *Comput. Fraud Secur.*, vol. 2014, no. 3, pp. 18–20, 2014.
[41] P. R. DeMuro, "Keeping Internet Pirates at Bay: Ransomware Negotiation in the Healthcare Industry," *Nova Rev*, vol. 41, p. 349, 2016.
[42] D. P. Pathak and Y. M. Nanded, "A dangerous trend of cybercrime: ransomware growing challenge," *Int. J. Adv. Res. Comput. Eng. Technol. IJARCET Vol.*, vol. 5, 2016.
[43] "What to do if your files were corrupted or renamed by ransomware." .
[44] S. Mohurle and M. Patil, "A brief study of wannacry threat: Ransomware attack 2017," *Int. J.*, vol. 8, no. 5, 2017.
[45] N. Scaife, H. Carter, P. Traynor, and K. R. Butler, "Cryptolock (and drop it): stopping ransomware attacks on user data," in *Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on*, 2016, pp. 303–312.
[46] A. Continella *et al.*, "Shieldfs: a self-healing, ransomware-aware filesystem," in *Proceedings of the 32nd Annual Conference on Computer Security Applications*, 2016, pp. 336–347.
[47] "F-Secure. 'State of Cyber Security.'" .
[48] "McAfee Labs. Understanding Ransomware and Strategies to Defeat it." .
[49] G. V. Cormack and others, "Email spam filtering: A systematic review," *Found. Trends® Inf. Retr.*, vol. 1, no. 4, pp. 335–455, 2008.
[50] D. F. Sittig and H. Singh, "A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks," *Appl. Clin. Inform.*, vol. 7, no. 2, p. 624, 2016.
[51] FBI, "Ransomware what it is and what to do about it?," *https://www.fbi.gov/news/stories/incidents-of-ransomware-on-therise/incidents-of-ransomware-on-the-rise*. .
[52] "T. Dewan. 'Teslacrypt joins ransomware field.'" .
[53] J. A. Sherer, M. L. McLellan, E. R. Fedeles, and N. L. Sterling, "Ransonware-Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web," *Rich JL Tech*, vol. 23, p. 1, 2016.
[54] "H. Weisbaum. CryptoLocker crooks launch 'customer service' site." 2013.
[55] "No More Ransomware Project," *https://www.nomoreransom.org/en/about-the-project.html*. .
[56] "FBI Ransomware Information," *https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise*. .
[57] "Internet Crime Complaint Center (IC3)," *https://www.ic3.gov/media/2016/160915.aspx*
[58] "National Cybercrime Security Center (NCSC, U.K.)," *https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware*. .