Journal of Engineering Science and Technology
Special Issue on ICCSIT 2018, July (2018) 24 - 33

A REVIEW OF LATEST WANNACRY RANSOMWARE: ACTIONS AND PREVENTIONS

SOHEIL ASKARIFAR, NOR AZLINA ABD RAHMAN*,
HASBULLAH OSMAN

School of Computing and Technology,
Asia Pacific University of Technology and Innovation,
Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia
*Corresponding Author: nor_azlina@apu.edu.my

Abstract

Among the different types of cyber-attacks ransomware can be considered as one of the most critical attacks. Ransomware is a malicious software that encrypts and capture system files and data until payment of a ransom is delivered by the victim. Recently, there has been a series of cyber-attacks by a well-known offender called WannaCry ransomware, this entity displayed multiple dangerous ransomware intrusions. This paper will discuss on how cybercriminals bypass computer defensive system, and how WannaCry, as well as other types of ransomware, affect overall computer systems. Furthermore, reviews on preventive measures will be considered, that how businesses should counteract against ransomware attacks. This will serve as guidance to control damage in the worst-possible scenarios, i.e., when the computer system has already been infected and data has been held.

Keywords: Bitcoin, Computer crime, Cybercrime, Malware, Network security, Ransomware, WannaCry.

1. Introduction

In May-June 2017, the WannaCry ransomware attack affected more than 150 countries which resulted in damages of up to $1 billion in one week. The scope of its damages has included at least 100,000 organizations around the world [1]. This ransomware was one of the largest and most damaging attacks in the history of cybercrime. Organizations affected include The National Health Service in Britain, FedEx, Japanese car manufacturer Honda, a speed camera company in Victoria, Australia, and Germany's Deutsche Bahn. The Russian Ministry of Interior reported that 1000 of its computers were damaged by these attacks [1]. Based on Fig. 1, [2] statistics published by various security companies revealed that the greatest number of computers and organizations affected were in the Russian Federation. Other countries who were also severely affected included Ukraine, Taiwan, Philippines, Egypt, and India. Ransomware attacks can be identified when a computer is locked which prevents the ordinary use or when files are encrypted and cannot be accessed without decryption. In the case of less complex ransomware, a security professional with relevant skills can decrypt the files and recover them. However, in case of WannaCry ransomware, the difficulty lies in its self-replicating nature and the fact that the attackers encrypt each file using a different key. Every key is further encrypted using another public key, which means that the ransomware authors hold the private decryption key. Security professionals call this as 'hybrid cryptography'. The effort involved in decrypting such complex cryptography is highly laborious and time-intensive [3].

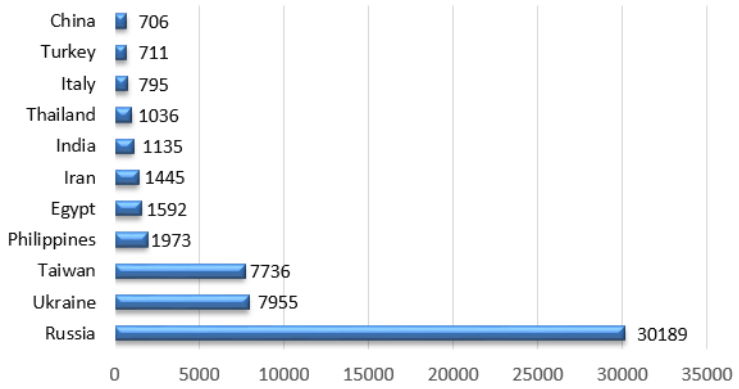

Fig. 1. Top countries affected by WannaCry as recorded by ESET.

WannaCry is not an unfamiliar type of modern ransomware that can baffle security agencies, antivirus software, and organizations equipped with a skilled security team. However, there is a concern because of the widespread downtime that the ransomware was caused, which led to billions of dollars in financial and economic losses as a result. Despite Microsoft having released patches for vulnerability, still, the ransomware exploited the Windows operating systems [4]. Another concern regarding WannaCry being an example of exploit-turned-ransomware that is developed by the NSA, then leaked by the Shadow Brokers hacking group and is available to anyone with marginal technical knowledge and the inclination to use it for disruption. Malware that contains a simple worm component which can cause significant widespread damage is a problem with

implications that need to be addressed [5]. As stray attacks of WannaCry continue to surface despite timely measures by Microsoft, cyber security software companies, and organizations themselves need to be properly educated on the modus operandi of ransomware authors, as well as timely preventive measures, and steps for damage control in situations where systems are already infected. A pressing question for businesses in the case of successful attacks will be whether to pay the ransom to restore normal operations. As in most circumstances, the losses in downtime can be significantly more expensive than the price of the ransom.

2. Ransomware Propagation and Prevention Evasion

Overall, ransomware attacks may be spread along different routes, but all strains of ransomware employ similar tactics to hold critical files hostage. A strain like Cerber target users through phishing campaigns. The notorious Crypto Locker and Crypto Wall are distributed via exploit kits and spam [6]. The most common exploit kit that has currently been in use is known as Angler. Figure 2 [7] shows how ransomware infection happen. The Angler Exploit kit uses HTML and JavaScript to identify the victim's browser and installed plugins, which then allows the attacker to independently select the user that has the most chances of being successful. Using various obfuscation techniques, the Angler is constantly evolving to evade detection by security-related software products [8].

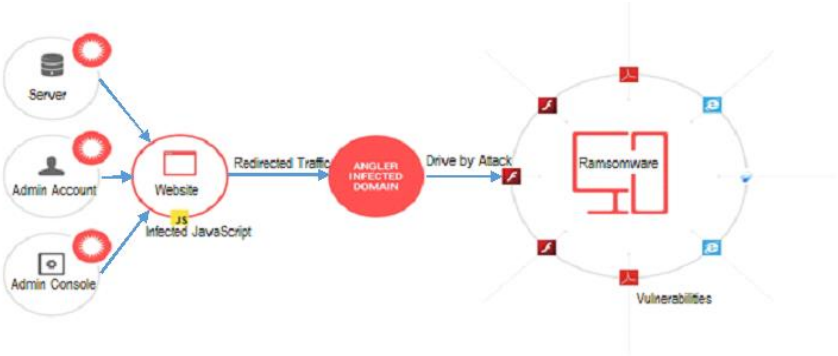

Fig. 2. Angler exploit kit [7].

Ransomware like WannaCry can also be loaded with other malware and, be delivered by an exploit kit, this then follows by the software where it silently installs and executes. Users may unknowingly download ransomware by visiting affected or malicious websites. As in many cases involving WannaCry, the ransomware may arrive in the form of an email attachment through spam email. In order for the malware to affect a system, the user must click on or download the attachment or file for the program to run. Despite the presence of free antivirus programs like Windows Defender (for Windows users) or paid antivirus software, it is possible for downloaded ransomware to pass the computer's defenses and infect the system. Antivirus software maintains a massive database of the digital signatures of known viruses. The software scans the computer for these digital signatures, and if found infecting files, the antivirus software makes attempts to quarantine and delete the relevant files. Figure 3 shows an example of files that have been encrypted by WannaCry.

Viruses that are new or unknown may not have their 'fingerprints' stored in antivirus databases. Some malware also modifies or encrypts their source code, making detection impossible for antivirus. In such cases, new ransomware can get past antivirus. Several tools and approaches can be used to prevent and detect the new malware:

- 'Sandboxing' - running suspicious files or new software in an isolated area – may keep the important files in the PC protected, but it may not always be a feasible option [9].
- Heuristic analysis is a more sophisticated approach of detecting previously unknown viruses, carried out through algorithms, matching file system events with known malicious behavior patterns to identify suspicious activity and commands.

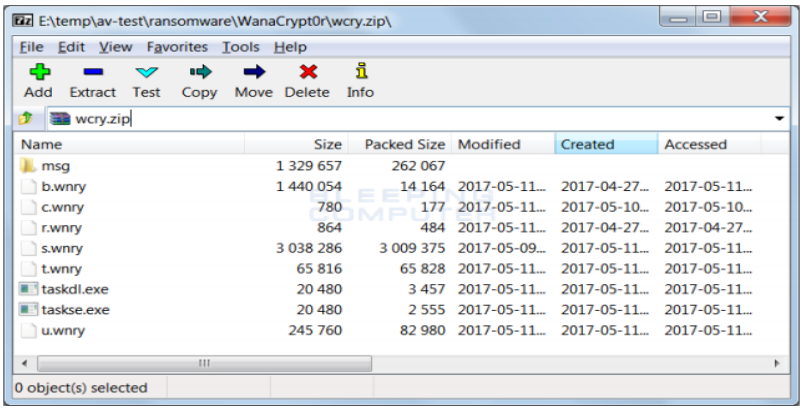

Fig. 3. Files being encrypted by WannaCry.

Most modern antivirus software uses a combination of heuristic analysis and signature methods to detect ransomware [10]. However, this software may not always be effective in identifying an unknown ransomware with encryption capabilities. In order for ransomware to be effective, it needs to be able to avoid detection until the encryption process is over. Many security solutions look for signs of strange DNS/Network flows, unusual directories like TEMP/Recycling Bin etc., and send notifications to the organization's security team. Ideally, the analyst should be able to catch these alerts and identify them as malware or ransomware threats and accordingly carry out remediation. However, response times for security teams can run into minutes, much longer than the encryption rates of many ransomware [11]. The ransomware's speed of encryption is also particularly significant since network shares are also affected swiftly, and an organization's entire network can be compromised in a short period of time with catastrophic results. Furthermore, Verizon's Data Breach Investigations Report (DBIR), mentions that 99% of malware is modified after the first attack and unleashed again in a slightly modified form, thereby evading detection [12].

3. Potential Effects of Ransomware Attack on Digital Assets

The name 'WannaCry' (aka Wcry, WanaCrypt0r, WannaDecrypt0r, etc.) is derived from the name of the malicious software that appears on infected systems, accompanied by a ransom note, together with, a countdown to the deadline for the

payment of Bitcoins, and the Bitcoin address to which the payment is to be made. The systems most affected by WannaCry have been those using older versions of Microsoft Windows for which Microsoft no longer offers support. Systems carrying unlicensed Windows operating systems have also been affected on a large scale particularly in China. Systems carrying Windows 7, Windows 8, Windows XP, and Windows Server 2003, have exclusively been affected. WannaCry works by exploiting vulnerabilities in certain versions of the Windows operating system. It searches for 176 different file types, encrypts them and appends them with the WCRY file extension. Typical file types an accompanying ransom note demands a payment of $300 in bitcoins for the release of the files, which, if not paid, this rate doubles after three days [13].

What makes it particularly disruptive is its use of what is called a "hybrid cryptosystem" for encryption – using a different key for each encrypted file followed by a public encryption key. WannaCry uses the ETERNAL BLUE exploit to launch its attacks, which is an SMB (Server Message Block) vulnerability. SMB is a Windows OS feature and network protocol that is used for file sharing, for providing access to serial ports, printers and other communication on a network. The SMB vulnerability was first discovered by the NSA, according to Wikileaks publications, and Microsoft subsequently disclosed it in a March bulletin labeled MS17-010. A patch was created by Microsoft who announced that PCs running Windows Defender with the Automatic Update option when activated would be protected against any attacks on TCP port 445, which is the port that runs the SMB since Windows 2000. The first known instance of WannaCry's successful attack was on May 12, 2000. Organizations had two months to update the patches provided by Microsoft, but most them failed to do so, leaving them vulnerable to the WannaCry attacks. There is recent evidence that suggests that organizations take an average of 100-120 days to update patches for vulnerabilities, this is due to various factors, including the lack of automation to handle the sheer volume of attacks that hackers direct at them through automation [14].

4. Ransomware Protection Techniques

In the wake of WannaCry, there was some success in efforts to stop its spread – and many of them were accidental. In one instance, a British researcher named Malware Tech accidentally stopped the malware from spreading by simply registering a domain name. Others discovered that blocking TCP port 445 also stopped the spread of WannaCry, but not for long [15, 16]. The consensus is that prevention is the best tactic against ransomware and its costly fallout, particularly since there is no guarantee that paying a ransom as demanded will make the encrypted files accessible again. There is also a risk that paying the ransom could make the victim vulnerable to further malware attacks. A combination of protective measures and vigilance may help managers and businesses avoid the consequences of ransomware-related downtime [17]. These are:

a. Disabling SMBv1

There is a vulnerability in implementations of Server Message Block 1.0 (SMBv1). This vulnerability enables an exploitation by a remote attacker to take control of an affected system. WannaCry ransomware spread using flaws in the ancient SMBv1 protocol, which Windows still enables by default. Disable SMBv1 able to minimize the vulnerability of the system.

Figure 4 below shows windows features on how to disable SMBv1.

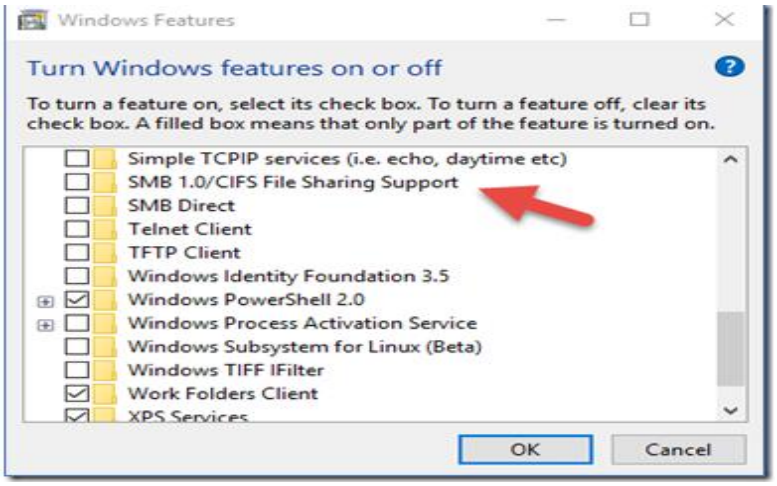

Fig. 4. Disable SMBv1.

b. Keeping software and antivirus updated.

The best practices in protecting individual and organizational computer systems from viruses, malware, and ransomware begin with keeping operating systems and software updated with patches. Using a free or paid antivirus that employs a combination of heuristic analysis and signature analysis is also necessary, especially against the growing volume of automated malware attacks. Whereas Windows Defender for Windows Systems is a reliable option for average users. There are reasonable security companies like Kaspersky Lab, Cisco, Trend Micro and others offer sophisticated antivirus software that uses behavioural analysis to detect ransomware and other malware. Similarly, to operating system software, it is necessary to keep antivirus databases updated with data on the latest malware.

c. Keeping critical files backed up.

Creating backups of critical files and storing copies offline will eliminate a desperate scenario in which the ransomware authors must be paid to release hostage data. Further, storing these files offline will ensure that they are not affected by ransomware on your computer. The external backup drive should be removed and stored off-site to create an 'air-gap', leaving the backup unconnected to any network or computer. This step assumes an attack and prepares for it [18]. Ransomware can be a threat to cloud backups as well as network drives, in addition to local drives. An example is the KeRanger ransomware targeting Mac computers, which contained a function to encrypt backups with TimeMachine, an OS X backup software.

d. Avoiding suspicious links and downloads.

Hackers and cybercriminals today are more sophisticated compared to the days when mass spam phishing scams were common. Attacks are much more targeted, with hackers going so far as to checking social media

accounts and creating fake email addresses, pretending to be a contact, and sending an email in order to lead the victim into clicking on an infected link. Accessing such links on personal computers or mobile devices at work can make an employee who is vulnerable to such attacks, a conduit that compromises sensitive business data through nodes on the network. Businesses can increase security awareness through workplace campaigns, stressing on the avoidance of clicking on suspicious links containing attachments from unexpected senders.

e. Using a pop-up blocker.

A simple but effective solution at the individual level in organizations is to employ a pop-up blocker, this has been recommended by the FBI (Federal Bureau of Investigation). Also, data should only be downloaded from trusted sites.

f. Avoiding giving administrative privileges to user accounts.

Businesses and managers must tactfully take the step of restricting administrative rights at the endpoints. This is one of the four strategies by The Australian Government's Department of Defence recommendations. This will assist maintaining security for malicious code and for users with administrative rights accessing sensitive data or making significant changes to applications and operating systems, whether intentionally or not. An environment of restricted administrative privileges is also easier to manage and support. The appropriate way to restrict privileges is to identify tasks that require such an action to be taken such as identify authorized staff members for the task, create separate accounts for them with the least amount of privileges required to carry out duties, re-evaluate the needs of individual members to have privileged access to major events such as a security incident or when they leave their job.

g. Using GPO restrictions for greater control.

Using Group Policy Object (GPO) to restrict access is a highly effective and affordable method of restricting malware in general and ransomware from being installed. GPO can be used to restrict software, websites, and devices to improve security in a business network.

5. Actions to Overcome Ransomware

The trends of ransomware in recent years have increasingly shifted towards crypto-ransomware. In the past, malware attacks were in form of misleading applications posing as antivirus, recommending that the user to "fix" a certain problem with their system by making a payment. Later, locker-type ransomware locks the systems without deleting or encrypting files. Once the malware was removed, the files could be recovered [19]. The rise in crypto-ransomware is in the scenario where files are encrypted and there is the threat of deletion if non-payment of ransom is conveyed. Even after the malware has been removed, the encrypted files continue to be inaccessible. In the case of sensitive files with no backup, the only option for the victim may be to pay the ransom.

Published cases in which the ransom was paid due to losses in downtime include the case of the Hollywood Presbyterian Medical Center, which was affected by

ransomware in 2016 [20]. The hospital staff spent ten days without access to their computers, having to rely on paper charts and fax machines. The hospital ended up paying a $17,000 ransom in bitcoin [20]. Nonetheless, payment does not guarantee that the files captured, will be decrypted. There were no reported cases that paying the ransom would lead to decryption, on the contrary, there were cases reported in which no decryptor keys were sent after payments. In the case of a ransomware infection, the sensitivity of the data infected will determine the course of action. The ransomware reports to cybercriminals who operate under the anonymity of The Dark Web using Bitcoins that leave no trace. This allows them to make easy money without the fear of legal repercussions. Law enforcement agencies recommend not to give in to the demands of criminals, if possible, or else it can encourage rather than stop the behavior [17].

6. Damage Control in the Worst-Case Scenario

Preparation for worst-case scenario is the best contingency plan that need to consider by all businesses of all sizes, since Real-time backup in which encrypted files are backed up will not help. Instead, businesses must have a robust backup process in place which they can use to roll back to a few days before the infection and restore data and apps at the local and server levels. Backups must only be restored after the ransomware has been completely removed from the systems. Businesses have access to numerous freeware and paid solutions to help them remove ransomware [17]. These free applications include:

- **AVG's Decryption Tools**

  AVG offers a host of free decryption tools for specific ransomware, including Legion, Bart, BadBlock, Apocalypse, TeslaCrypt, and SZFLocker.

- **Trend Micro's Lock Screen Ransomware Tool**

  As is evident, Trend Micro's anti-ransomware tool is designed to detect and get rid of the type of ransomware that causes a locked screen.

- **Avast**

  Avast provides a decryption and installation wizard, as well as 16 tools for malware including Jigsaw, CrySIS, Xdata, Globe, HiddenTear, and others.

- **Kaspersky**

  Kaspersky's free anti-ransomware tool offers some level of preventative protection against a variety of malware, suitable for small and medium business owners.

- **Malwarebytes anti-ransomware**

  Malwarebytes took over CryptoMonitor and the resulting tool prevents ransomware from encrypting files on the PC.

- **Kaspersky Decryptors**

  Kaspersky offers a host of free decryptors that may help you decrypt ransomware and free important files. These include the Wildfire decryptor, Shade, CoinVault, Rannoh, and others.

All these software offers limited protection on their free versions, whereas the licensed paid versions offer the full protection package.

7. Conclusion

The Wanna Decryptor malware strain has been highly publicized but only several types of ransomware that were mitigated in recent times This is due to most attacked victims by ransomware tend to proceed with payment even though they are not sure whether the attacker will decrypt their files when the payment is done. This will encourage the attackers to form more attacks using ransomware as they are able to gain more money. The FBI's Internet Crime Complaint Center reports that between April 2014 and June 2015, there were over 992 CryptoWall-related complaints received, leading to over $18 million losses [21]. Ransomware authors will continue to exploit vulnerabilities in devices, software, networks. Preventive care is necessary at to protect from such attacks. At the same time, more research is needed to produce more powerful ransomware decryptor like Paybreak, which observe encryptions keys, stores them, and retrieves them to decrypt files after an attack. It is also necessary to rely on multi-layered automated security solutions for combating crypto-ransomware, which have automated creation and dissemination processes and therefore stay one step ahead of security professionals.

Abbreviations

DBIR	Data Breach Investigations Report
DNS	Domain Name System
FBI	Federal Bureau of Investigation
GPO	Group Policy Object
HTML	Hypertext Markup Language
NSA	National Security Agency
PC	Personal Computer
SMB	Server Message Block
TCP	Transmission Control Protocol

References

1. Cambridge, E. (2017). Fedex and Russian interior ministry are among 45,000 computer systems hit by worldwide cyber-attack that has crippled NHS. Retrieved June 24, 2017, from https://www.thesun.co.uk/news/3549746/ fedex-russian-interior-ministry-worldwide-cyber-attack-nhs/.
2. We Live Security. (2017). ESET WannaCryptor detections (top countries). Retrieved June 24, 2017, from https://www.welivesecurity.com/2017/05/17 /wannacryptor-wasnt-the-first-to-use-eternalblue/.
3. Kolodenker, E.; Koch, W.; Stringhini, G.; and Egele, M. (2017). PayBreak: defense against Cryptographic Ransomware, in ASIA CCS '17. *2017 ACM on Asia Conference on Computer and Communications Security*. 599-611.
4. Microsoft. (2017). Microsoft security bulletin MS17-010 – critical. Retrieved June 24, 2017, from https://technet.microsoft.com/en-us/library/security/ ms17-010.aspx.
5. Alfred, Ng. (2017). Hackers behind stolen NSA tool for WannaCry: more leaks coming. Retrieved June 24, 2017, from https://www.cnet.com/news/ hackers-behind-stolen-nsa-tool-for-wannacry-more-leaks-coming/.
6. Symantec Corporation. (2016). An ISTR special report: Ransomware and businesses 2016. Retrieved June 24, 2017, from https://www.symantec.com/

content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf.

7. Zaharia, A. (2016). What is Ransomware and 15 easy steps to keep your system protected. Retrieved April 26, 2017, from https://heimdalsecurity.com/blog/what-is-ransomware-protection/.
8. Brunau, C. (2016). How Ransomware is spread. Retrieved April 27, 2017, from https://www.datto.com/blog/how-ransomware-is-spread.
9. Craig, P. (2017). What is a Sandbox? And why do I need one to defend against advanced threats? Retrieved June 24, 2017, from https://news.sophos.com/en-us/2016/04/13/what-is-a-sandbox-and-why-do-i-need-one-to-defend-against-advanced-threats/.
10. Zeltser, L. (2015). How antivirus software works: Virus detection techniques. Retrieved June 24, 2017, from http://searchsecurity.techtarget .com/tip/How-antivirus-software-works-Virus-detection-techniques.
11. Emsisoft. (2017). Spotlight on ransomware: Ransomware encryption methods. Retrieved June 24, 2017, from http://blog.emsisoft.com/2017/06/21/ransomware-encryption-methods/.
12. Verizon. (2017). Data breach investigations report. Retrieved June 24, 2017, from http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf.
13. Securelist (2017). WannaCry ransomware used in widespread attacks all over the world. Retrieved June 24, 2017, from https://securelist.com/wanna cry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/.
14. Kenna Security. (2015). How the rise in non-targeted attacks has widened the remediation gap. Retrieved June 24, 2017, from https://www.kennasecurity.com/resources/non-targeted-attacks-report/.
15. The Province. (2017). The latest: researcher who helped halt cyberattack applauded. Retrieved June 24, 2017, from http://www.theprovince.com/business/latest+cyberattack+german+rail+schedule+boards/13367124/story.html.
16. ZDNet. (2017). WannaCry: Why this ransomware just won't die. Retrieved June 24, 2017, from http://www.zdnet.com/article/wannacry-why-its-ransomware-that-just-wont-die/.
17. Zhanhui, L.; Abd Rahman, N.A. (2017). A review on Ransomware trend of attacks and prevention. *International Journal of Applied Engineering Research*, 12(16), 6193-6201.
18. McAfee Labs. (2016). Understanding Ransomware and strategies to defeat It. Retrieved June 24, 2017, from https://www.mcafee.com/in/resources/white-papers/wp-understanding-ransomware-strategies-defeat.pdf.
19. Paganini, P. (2016). Ransomware: How to recover your encrypted files, the last guide. Retrieved March 14, 2018, from http://securityaffairs.co/wordpress/53438/malware/ransomware-recover-guide.html.
20. The Guardian. (2016). Los Angeles hospital paid $17000 in bitcoin to ransomware hackers. Retrieved March 14, 2018, from https://www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-center.
21. PCWorld. (2017). How to protect and recover your business from Ransomware. Retrieved June 24, 2017 from http://in.pcmag.com/feature/104593/how-to-protect-and-recover-your-business-from-ransomware.