

Review Paper on Ransomware: A Brief Study- Creation, Prevention and Awareness

Rhishav Kanjilal

Masters in Computer Applications

Jain (Deemed-to-be) University, Bangalore, India

Abstract— Ransomware is a term used to describe a class of malware that is used to digitally extort victims into payment of a specific fee. At its root can be divided into two major types of this form of digital extorter, then subdivided by their families. Those that encrypt, obfuscate, or refuse access to files, and those that block access or lock users out of the systems themselves, are the two main types of ransomware. These risks are not limited to any specific geography or operating system, and any number of devices may be subject to action. This kind of exploitation via ransomware is at risk for anything from your Android devices, iOS systems, or Windows systems. The method of compromise of the system could be different depending on the target, and the final behaviour taken will be constrained by the capacity of the system itself, but many extorters often follow identifiable patterns. The purpose of this paper is to provide a better understanding of ransomware attacks to the masses who are not accustomed to the technicalities of a ransomware: how does the attack happen or how is the file created.

Keywords: Ransomware, Prevention, Creating Ransomwares from Scratch, Malware Analysis

I. INTRODUCTION

Ransomware has traditionally been written in 1989 by Joseph Popp and is based on an initial malicious piece of code known as AIDS. This original malicious code will substitute AUTOEXEC.BAT on infected systems and allow 90 device reboots until all directories have been hidden and files can be encrypted. Further study however showed that only the filenames using simple symmetric key cryptography were scratched and eventually defeated and deleted by applications such as AIDSOUT and CLEARAID. More information about the original AIDS trojan is available in the Virus Bulletin, published by Jim Bates' work on the subject.

Crypto-currency, usually bitcoin, is the type of payment most digital extortionists are asking now though not the only method of payment needed. Criminals also use some prepaid voucher programmes, such as MoneyPak, Ukase or Pay Safe.

Ransomware really went out of fashion in the late '90s and didn't begin to return to prominence until 2005. The availability, along with more system-side computing power, of more sophisticated encryption systems helped to lead to this new ransomware era that continued to accelerate. In 2016, the attack against computer systems was one of the most frequent styles, requiring limited vulnerability exposure and minimal objective recognition. An approximate

\$18,000,000 had been accrued to one of the most familiar models, Crypto Wall (currently dead). A screen shot of one of the more recent Cryptical payment screens.

In this paper we will learn how to create a basic ransomware, how to detect the presence of a ransomware in your system and what can be done to actively defend it. The concern and necessity of this paper is merely that this can be understood and administered in more specific terms for the people who come even from a non-IT background. So not wasting much time lets jump straight to the point!

II. ANATOMY

The first stage is the creation of a ransomware virus which if we see is not that big of hassle provided the right selection of tools provided or assembled. The lethal factor lies in its core simplicity. With a proper command and grip over Python (Script) you can create, modify, modulate and design a ransomware as per your need, but it's highly recommended not to, as even the presence of a deployable ransomware in your system is considered illegal and punishable offence by the government some of which are mentioned below:

The Information Technology Act: Tampering with Computer Source documents – Section 65 Hacking with Computer Systems, Data alteration – Section 66 Publishing obscene information – Section 67 Un-Authorised access to protected system --- Section 70 Breach of Confidentiality and Privacy – Section 72 Publishing false digital signature certificates – Section 73

A. IPC and Special Laws:

Sending threatening messages by email – Section 503
Sending defamatory messages by email – Section 499
Forgery of electronic records – Section 463
Bogus websites, cyber frauds – Section 420
Email spoofing – Section 463
Web-Jacking – Section 383
E-mail Abuse – Section 500

Some Special Acts:

Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act Online sale of Arms Act

Moving on to the minimum requirements for building a simple ransomware:

- Windows, Linux, or Mac OS
- Python 3.6 or higher.
- An IDE for better workflow (recommend PyCharm).
- An executable environment.

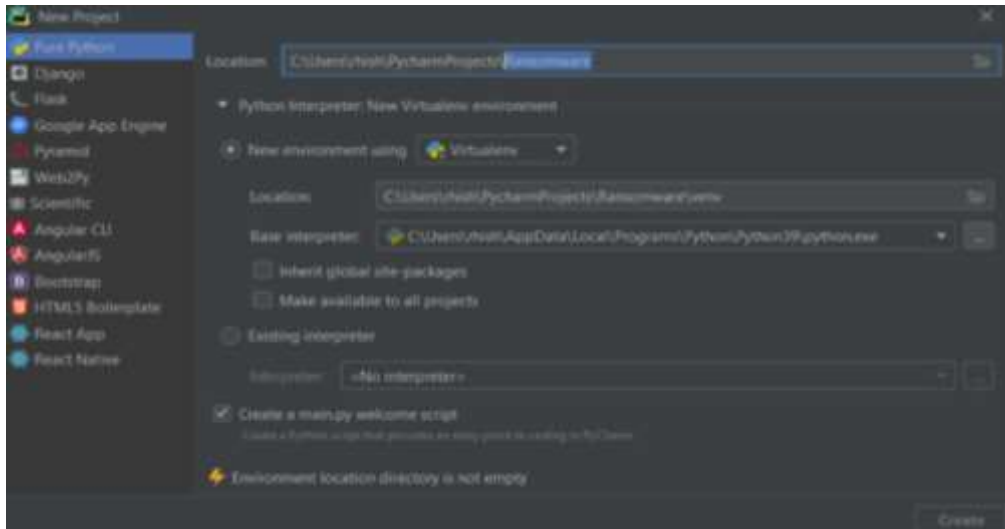


Fig. 1.2: Pycharm Ransomware project Initiation



Fig. 1.1: A screen shot of one of the more recent Cryptical payment screens

III. THE PROCESS

After the successful installation of PyCharm, run the IDE and create a new Python Project. For an easy understand ability name, it from the basic of the foundation i.e. Ransomware.

A. Code:

Once the project is created successfully, we need to import some libraries in the beginning of the code. Libraries are basically some external sheets of code that people have

already written and we are going to use them to accelerate our own development of the program. We import three basic libraries named:

- os: This will allow us to manipulate the folders
- os.path import expand user: This will allow us to go to the root directory of the operating system and can be iterated on all the files of the so recursively and encrypt them one by one.
- Cryptography. Fernet: A library from which fernet can be imported. Fernet guarantees that a message encrypted using it cannot be manipulated or read without the key. Fernet is an implementation of symmetric (also known as “secret key”) authenticated cryptography. This class provides both encryption and decryption facilities

We now create a class name ‘Ransomware’ which will be encapsulating all the activity that we are going to allow the ransomware to perform.

[def __init__(self):] is the next step where this instance is brought into existence where when create an instance of this class the function will fire and set three variables namely (i) key, which is going to be the product used to encrypt the files(lock up the system files) and can only accessed with the key. (ii) Cryptor, an object which will do the encryption. (iii) file ostentation targets, which defines the types of files that will be encrypted as per the attacker’s choice (text, zip, multimedia etc).

We then move on to the generate key module i.e. “def generate key(self):” , which basically generates the initial key via which we lock up all the files in the system as we iterate over from the top of the file system.

On successful completion of the command we then go ahead and create a fernet object “self. Cryptor = Fernet (self. Key)” passing in the key ultimately setting it as the encryption key (Cryptor is the fernet object).

Then comes the read and write modules “def read key(self, keyfile_name): makes the key readable and similarly the write key “def write key(self, keyfile_name): which generates a written format of the key that can be understood and be made readable. (In a real ransomware these two modules are not that much crucial and here it has been explained just for the sake of proof of concept).

Now we arrive in the actual working script of the program which is responsible for the entire ransomware encryption and decryption. The portion makes sure that in an so the scanning of folders start right of the core root and subsequently searching all the sub folder within a parent folder, can be numerous in number depending upon the size of data that has been stored in the pc. For all the files in the file system, we need to determine the absolute path which is the file to the path starting from the root directory and we check to see if the file extension for that specific file exists in our target files.

“If not abs_file_path.split('.')” splits it into dots which in turn will split all the file extensions at the index of -1 (special python syntax for stating the last element in the array which would be the file extension). If that file extension is there in the extension targets chosen by us, then encryption takes place: “self. crypt file (abs_file_path, encrypted=encrypted)

The next function is then called, which has been instructed as per the user’s choice in the previous step of whether to execute the encryption or decryption, by “def crypt file(self, file path, encrypted=false):”. A Boolean parameter decides the value i.e. “True” or “False”.

Once the value is executed, the file path is opened and read in of the data happens, regardless of encrypt value or decrypt value because once the file has been encrypted it is essentially

just scrambled data and we read that in and use the key which finally opens the encrypted file.

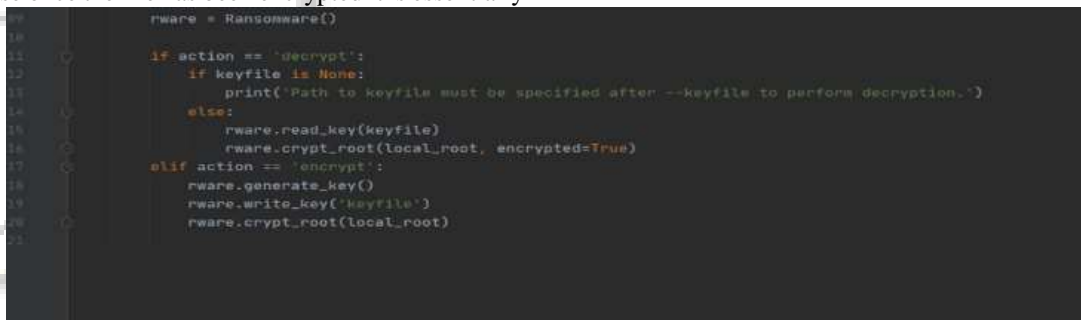
Now walking down the file path and finding all the files, we go ahead and recall the crypt file function “def crypt file(self, file path, encrypted=False):” and that crypt file function opens up that particular file “with open (file path, ‘rb+’) as f”. I

An if/else comes into play where if the file is not encrypted then encryption takes place, else it is decrypted. “if not encrypted:

- print (file contents pre encryption: {_data})
- data = self. Cryptor. encrypt(_data)
- print (file contents post encryption: {_data}) else:
- data = self. Cryptor. decrypt(_data)
- print (file content post decryption: {_data})”

We call this function conditionally depending upon the requirement. Once this step is achieved, we then head to the top of the file and write in that new data which will be coherently be the result of encryption or decryption.

There are few arguments which ensures that the ransomware can be run as command line program. If you choose to run it via the console type : “\$python3 main.py –action encrypt” and just add the parser add argument which will look for any arguments that we pass down in the command line and put a value like “encrypt” and hit run which will encrypt all the files.



```
10 rware = Ransomware()
11
12 if action == 'decrypt':
13     if keyfile is None:
14         print('Path to keyfile must be specified after --keyfile to perform decryption.')
15     else:
16         rware.read_key(keyfile)
17         rware.crypt_root(local_root, encrypted=True)
18 elif action == 'encrypt':
19     rware.generate_key()
20     rware.write_key('keyfile')
21     rware.crypt_root(local_root)
```

Fig. 1.3: Similarly, “\$python3 main.py –action decrypt –key file. /path/to/key file” will decrypt all files.

We then create an instance Ransomware class as walked above and create an if/else condition for both the conditions and in case of an encryption a key is generated(In case of a real ransomware the key will be posted on a remote server designed by the attacker until you pay the amount.

IV. METHODOLOGY

Phase one of a ransomware attack is the installation of the components that are used to infect, encrypt, or lock the system. There are a few different methods by which the original files that are used as part of the attack are downloaded to the system:

- Drive-by download: It occurs if a device installs malware or spyware automatically without the knowledge of the end-user.
- Strategic web compromise: The strategic web compromise often means watering-hole attacks (a subset of a drive-by-download used most when choosing a specific target / demographic). These rely on end-user’s strategic reassessment and are also reserved for special attacks.

- E-mails for phishing: Can be generalised, spam-free or specifically designed for your company or industry. These emails may contain links to malicious websites or attachments. Internet-accessible applications manipulation vulnerabilities in this case, networks, or Internet searches flagrantly for exploitable bugs have taken steps vs. users, such as the preceding approaches.

All the above methods have unique protection methods, even though the first three of the four need user interaction and rely on an end-user to connect and to allow or download the downloader. The fourth method, vulnerability exploitation, is much more methodical and is carried out as part of a broader assault on the entire enterprise. If strategic web compromise is the older approach that is used for targeted attacks, the most advanced method of targeted attacks is the exploitation of vulnerability. The use of browser security is a good beginning to prevent drive-in downloaders and strategic site compromising; but since these threats constantly morph, you will need something which does not rely solely on file signatures. This is where bare-metal detonation and sandboxing come together.

The best place to start phishing e-mails is at the border, review all incoming attachments in a virtual or bare-metal sandbox, until they enter the end user, where additional end-user security products can search these files once again, until they can be opened. You can also search files to see if they were previously opened and monitor connexions in the emails in addition to scanning for maliciousness.

A. How does the Destruction Begin?

Installation: If the victim system has acquired a malicious payload, the infection begins. There are several ways of producing the virus, regardless of the target system. A method of installation will basically use the technique of the download dropper where the first file is a small code to prevent detection and interact with access and control networks of the Extortionist. The executable will then receive commands to download the ransomware to the infected device for infection. The ransomware programme will instal itself on the device once it has landed on the device. In a windows setup, you set keys to make sure the mallocced starts on your computer each time on your Windows registry. For other systems, they either use unsafe app shops (usually Android devices) or stolen or legitimate iOS application creation certificates. The ransomware installation really starts to hold the adversary.

[QUICK FACT: Although mobile devices are not a major target for ransomware, they are the biggest growth area in end user technology and so we anticipate that they will increase as objectives. However, you should note that many of your end users (and maybe you too) had to gaol their telephones for unapproved apps. As you are no longer covered by walled gardens set up by several smartphone manufacturers, this increases the risk significantly.]

In a focused effort to optimise the payoff it may be more dangerous to instal, mask, pack code and use techniques. The initial installation will be used by Ransomware to spread across the affected network slowly, to be installed on any number of systems and file shares that are then simultaneously encrypted by sending instructions during the next point. It can be difficult to build. In several cases, the powerful modern crypto ransomware variants would first use some type of macro virus or exploited PDF to access the device. WSF, Java and Adobe Flash were also used. After the malware has been downloaded, the embedded code is executed, and the system is analysed to decide whether it is in the sandbox on a real computer or on an e-mail.

A second process starts when the ransomware finds it worth infecting on a computer. In that case, the second step starts, mostly covered in Windows as usual. At this stage, the malware becomes more special, typically using an MD5 hash with the computer's name, or another unique identifier such as a Mac address to make sure the extorter knows which machine is affected. The second-stage dropper can now execute a variety of scripts that can disable any



Fig. 1.4: Mehodology of a ransomware attack

native Windows security, including disabling the shade copy functionality on files and volume, disabling device recovery functionality by using something such as Credit, and eventually destroying any anti-malware and systematic logging functions. The next step will then take place. After the svchost.exe is a typical Windows operation, the control-and-control step begins.

Command-and-Control: To efficiently decide the next steps, all behaviour involves some form of command and control systems. This is the same in conventional warfare as in cyberspace because ransomware involves maintaining a certain type of communication channel to ensure these communications can take place. Think of it like this: you might have a piece of ransomware on your computer right now, lying asleep, waiting for orders, without receiving orders. When the malicious code is deployed and mounted, a ransomware attack begins to enter your command servers and check for instructions. These instructions are a variety of applications. They include everything from defining the types of files to be encrypted, how long you should wait for the process to begin, and whether you should continue to spread until the process begins. A large amount of system information, including IP address, domain name, operating system, installed browsers and anti-malware products, is documented even in a few ransomware variants. These details may allow a criminal organisation to decide not just who they compromised, but also to decide if they succeeded in achieving a high value goal, indicating that this compromise is used for more dangerous ends than simple ransomware. The more sophisticated systems such as TOR make it much harder to track the exact position of the criminals taking part in the extortion and some of the ransomware variants mount TOR customers to ensure safe communications.

[QUICK FACT: Be extremely careful while using TOR, because even if the creators say it is undetectable, but if an end user has command over end nodes then you are done for! Stay safe, stay vigilant!]

Handshake and key exchange: The malicious code installed on the victim device in virtually every ransomware case is a client, and the server of command and control run by the criminal adversary is a server. The client on your machine ensures it interacts through the prearranged handshake protocol with the right bad guy's server. For every family ransomware, which is a set of ransomwares which acts in a similar way and is often funded by the same criminal organisations, this handshake procedure is different. At its heart, however, it is how criminals can recognise the malware variant they executed and their infected device.

In some cases, as with the Clocker ransomware, all the packaging is distributed to an album on a legal website, in this case Impar. In this case, it is packed as a portable network graphics file. The next step is to generate and share valuable details after the client and the server have decided that they are a prearranged working pair. This might range from a badly performed, simple symmetric key cylinder to a sophisticated RSA 4,096-bit encryption algorithm, depending on the complexity of the ransomware. The main exchange takes place on criminal servers, while the public password is sent to the mallocced encryption component installed on the victim device. In some cases, you may be fortunate, as some of the less complex ransomware variants do not produce a

unique key every time and the use of public decrypts can reverse encryption.

B. Destruction:

At this stage, this key is now active and ready to be used for the malware on the victim's computer to lock or encrypt files on the machine. The malware would begin to encrypt all the files that were found in the command and control processes. This may include any of the formats of JPGs, GIFs, and other file styles of Microsoft Office documents. Some versions encrypt the files as well as the filenames, so you cannot even tell how far you got from the attackers and what files you lost.

C. Extortion:

When the files are secured, a screen shows the victims how they were hacked. For enforcing payment, extortionists use any variety of tools. Some ransomware variants allow you to freely decrypt a file to show that your device has a key. Other versions have increasing fees, which increase the cost until the key is removed. The standard unblocking cost for a system ranges from \$300 to \$500 bitcoins, but some of the versions for businesses cost up to tens of thousands of dollars. Some of the later versions delete files to make the ante and frighten you to pay the ransom faster. If you pay, you cannot guarantee that your files will be decrypted by the key they supply. In addition, no assurance is made that the ransomware is removed itself. Indeed, professional opponents will use your initial lending pace to assess the next target within your network, including backup, network attached storage or other operating systems essential to your business operations, along with any additional details identified by the malware within the network itself. You will then pay with an enhanced and accelerated ransom.

TO PAY OR NOT TO PAY: So, to be fair, I decided to say "NO" This is, however, an incredibly simple answer. You may have files that you just can't do without the encrypting device, you haven't backed them up, and you don't have a way to restore them – or you may consider payment if human lives are instantly on-line. Also interesting is that ransomware writers tend to know their target population and choose price points that are sufficient to facilitate payment, and that price is approximately comparable to the costs of data recovery. You should never find yourself in the position to consider paying the money if you follow the instructions provided in this paper.

Types: Today's crypto ransomware uses state-of-the-art algorithms to encrypt data on your computer or network and is in two simple flavours: symmetrical key and asymmetrical key encoding. Each strategy has many advantages and disadvantages for the extortionist. Some of the more complex versions benefit from both forms of encryption to solve each other's vulnerabilities.

Symmetric: Malware using symmetric key encryption also produces the key which is used in the encryption process using the computer as its own computer. By using symmetric coding, less device resources can be used when the malware codes the files. This reduction of overhead efficiency by the ransomware not only decreases detection opportunities by applications for process monitoring but effectively uses the infected system's CPU resources. Using a small device created key, overhead output is reduced and the

number of files you encrypt can be maximised, while using the system's own CPU. Another advantage of using symmetric key encryption is that every infected system produces a single key so that ransomware extorters can determine which deployments have succeeded and not. In addition, it requires online or offline encryption. Then the machine needs to get back online and give the key to the opponent to start the lettuce clock. The encryption key is removed from the computer and returned to the extorter. This is done to retain this key to obtain your rescue. The ransomware needs to wait until the machine gets online to do this. After an Internet link is created and the key is forwarded to the suspect, the clock normally begins.

A big downside to symmetric key encryption is it can be solved. You may use the active memory key to decrypt the files on the device when they are offline. Which makes it possible to decrypt files yourself if you are affected by a variant malware using symmetrical key encryption.

Asymmetric: The attacker will use this approach with a public and private key in the encryption process. The public key is used to encrypt the files on the infected device, and the private key to decrypt the files. These key pairs prohibit the use of forensic memory to decrypt files. You must instead rely on brute force attacks, cryptographic vulnerabilities, pay the ransom or first plan for this kind of attack. There are again two main forms of asymmetrical coding for asymmetric key ransomware: public key embedded and public key downloaded. The technique is amazingly simple in ransomware that uses an embedded public key and can be used whether the device is online. The downside of this strategy is that each attack involves the generation of a new public key. The encryption process cannot start with ransomware using a downloaded public key until the device has returned to the server and interacts with the attacker to get its public key. The benefit here is that with each infection, the attacker can use different key pairs. Another huge advantage of the asymmetrical encryption approach is the use of far bigger primes, starting at 2,048 bit and above, in its encryption algorithm.

System or Browser Locking: The other approach is machine or browser locking in the destruction time. This form of ransomware renders the infected computer or other programmes in the device useless rather than physically encrypting the data on the infected machine.

For example, a fully-screen window covering the entire user desktop is displayed in the Windows Ransomware locker. This window is generated in various ways by various variants, all of which restrict the user to just one window. Some of the most challenging forms of ransomware locker monitor the desktop of the device via a background thread to make sure the only window is working. The windows content in the ransomware locker normally depends on the location and is downloaded to ensure that they serve the victim's located material. If the device is locked, the ransomware does a variety of things to ensure it keeps it going on, including shut-down signals for other processes, kill commands for processes used to execute the ransomware and generate an on-board virtual desktop to ensure that the end user cannot get out of the virtual desktops that the ransomware produces. Most ransomware browser lock is cross-platform. As most browser-locking Ransomware is client-side, malicious web

pages will be served any time they try to close the browser or navigate away from an infected website using JavaScript to pop-Up Windows on victims' computers. The method is identical for devices such as handheld tablets or phones. The malware generates an activity window, and the malware scans periodically for the activity window.

V. GROWTH FACTORS:

While Ransomware received more publicity in recent years since the mid-2000's it has been around. Why is it now so large?

We must look at the outcomes that have been achieved to answer this question. If you think about the popularity of criminal organisations, which initially use spam and phishing camps to attack those using today's crypto ransomware with false applications or bogus antivirus (AV) software, it is easy to see how effective it is – if one community sees how much money another makes, it will then find a way to do this. It operates as an anarcho-capitalistically as possible in the free market. Indeed, markets emerged to sell mature high-end ransomware, thus reducing the barriers to accessing this lucrative criminal undertaking for criminal organisations. If you are a highly effective attack based on a mixture of human error and technological strength, criminals will find a way to make money. The accessibility of many modes of ransomware-package, online or offline-based device encryption and the simple concealment of one's paths while paying has all contributed to the use of digital extortion ransomware. In addition, because criminals have introduced new methods for the implementation and use of networked systems, businesses who must access their data are now attacked, either for legal purposes or even for purposes of life security. Criminals do not contribute 0.5 or \$100 to the settlement anymore. They charge instead hundreds or thousands of dollars, and businesses are mindful that in certain situations they are paid not to be involved in a patient's death or in loss of profits due to significant failures.

Criminals also realised that they easily extort end consumers and companies directly instead of trying to fence stolen goods. Thus, their expenses are reduced and their return on equity is increased.

VI. CONCLUSION

It is a long history of Ransomware. It passed effectively, using sophisticated cryptographic methods, from modest beginning to 5-1/4" floppy discs, not just computers, but phones and tablets.

Ransomware became more popular because it succeeded. It has evolved and changed in an environment of fitness for the survival of its creators to meet the growing requirements. These criminal organisations are moving from simple snares and disappointments to outright bribery to our fears and to our need to safeguard our records. Today, criminals are switching from targeting domestic users to corporate users whose data is considerably more important and subject to intense regulatory demands to retain precise times and access to essential data security.

Given the prevalence of Internet-connected devices such as watch, television, refrigerator and vehicles, the time before criminals begin targeting these devices is only a matter

of time. Imagine a world where you are driving to work, but you switched off your fridge overnight so your coffee cream was ruined, and your car will not begin until you pay for the ransom. It is not so distant and not so far away if we do not find ways to defend these devices from illegal actors more effectively. And as my paper has much evidently cleared the fact that to protect yourself from a threat like this, just a mere pinch of attention and alertness has to be excelled. Remember, you're just a click away from getting conned, but to click or not lies totally on you. Thus, I conclude by saying "Stay alert, stay safe!"

REFERENCES

- [1] A. L. Young and M. Yung, "On Ransomware and Envisioning the Enemy of Tomorrow," in *Computer*, vol. 50, no. 11, pp. 82-85, November 2017.
- [2] A. O. Almashhadani, M. Kaiiali, S. Sezer and P. O'Kane, "A MultiClassifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware," in *IEEE Access*, vol. 7, pp.
- [3] K. Cabaj and W. Mazurczyk, "Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall," in *IEEE Network*, vol. 30, no. 6, pp. 14-20, November-December 2016.
- [4] Ransomware Payments in the Bitcoin Ecosystem, <https://zenodo.org/record/1238041#.XzpQs-gzbc>, accessed 22. 02.2020
- [5] Ransomware samples, <https://github.com/fabrimagic72/malwaresamples>, accessed 22.02.2020
- [6] Ransomware dataset, <https://github.com/behaz/ransomware-dataset>, accessed 22.02.2020
- [7] M. Du and K. Wang, "An SDN-Enabled Pseudo-Honeypot Strategy for Distributed Denial of Service Attacks in Industrial Internet of Things," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 648-657, Jan. 2020
- [8] Ransomware dataset, <https://www.unsw.adfa.edu.au/unsw-canberra/cyber/cybersecurity/ADFA-NB15-Datasets/>, accessed 22.02.2020.
- [9] Adam Bradley, The Real Cost of Ransomware And How We Stop Paying <https://www.forbes.com/sites/adambradley1/2020/06/11/the-real-cost-of-ransomware-and-how-we-stop>
- [10] Ilascu, LockerGoga Ransomware Sends Norsk Hydro into Manual Mode, BleepingComputer, 2019, available at <https://www.bleepingcomputer.com/news/security/lockergogaransomware-sends-norsk-hydro-into-manual-mode/>
- [11] L. Franceschi-Bicchierai, Ransomware Forces Two Chemical Companies to Order 'Hundreds of New Computers', Motherboard, 2019, available at https://motherboard.vice.com/amp/en_us/article/8xyj7g/ransomwareforces-two-chemical-companies-to-order-hundreds-of-new-computers
- [12] Virustotal service, 2019, available at <https://www.virustotal.com/>

- [13] Abusing Code Signing for Profit. Chronicle, 2019, available at <https://medium.com/@chroniclesec/abusing-code-signing-for-profitef80a37b50f4>
- [14] Crypto++ crypto library, 2019, available at <https://www.cryptopp.com/>
- [15] Yara project, 2019, available at <https://github.com/VirusTotal/yara>
- [16] OpenSSL crypto library, 2019, available at <https://www.openssl.org/>
- [17] M. Dworkin, Recommendation for Block Cipher Modes of Operation. Methods and Techniques. NIST Special Publication 800-38A, 2001, available at <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf>
- [18] M. Bellare and P. Rogaway. Optimal asymmetric encryption. In, R. Rueppel editor, Advances in Cryptology - Eurocrypt'94, Lecture Notes in Computer Science, volume 950, pp. 92-111. Springer Verlag, 1994.
- [19] D. Boneh, Twenty Years of Attacks on the RSA Cryptosystem. Stanford University, 1999, available at <https://crypto.stanford.edu/~dabo/pubs/papers/RSA-survey.pdf>
- [20] Young A., Yung M., Cryptovirology: Extortion-based security threats and countermeasures. In Security and Privacy Proceedings, IEEE Symposium, 1996, pp. 129–140.
- [21] Young A. Building a Cryptovirus Using Microsoft's Cryptographic API. In Proceedings of the International Conference on Information Security, 20
- [22] D. O'Brien (2017). Ransomware 2017, Internet Security Threat Report, Symantec.
- [23] D. Nieuwenhuizen (2017). A behavioral-based approach to ransomware detection, MWR Labs Whitepaper, <<https://labs.mwrinfosecurity.com/assets/resourceFiles/mwri-behavioral-ransomware-detection2017-04-5.pdf>>, data retrieved 01.04.2018
- [24] McAfee, (2017). McAfee Labs Threat Report.
- [25] N. Sacife, H. Carter, P. Traynor and K. R.B Butler (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data, IEEE 36th International Conference on Distributed Computing Systems
- [26] K. Savage, P. Coogan, and H. Lau (2015). The Evolution of Ransomware, Symantec, Security Response.
- [27] A. Bhardwaj, V. Avasthi, H. Sastry and G. V. B. Subrahmanyam (2016). Ransomware Digital Extortion: A Rising New Age Threat, Indian Journal of Science and Technology, Vol 9(14).
- [28] M. Wecksten, J. Frick, A. Sjostrom and E. Jarpe (2016). A Novel Method for Recovery from Crypto Ransomware Infections, 2nd IEEE International Conference on Computer and Communications.
- [29] M. H. U. Salvi, & M. R. V. Kerkar (2016). Ransomware: A cyber extortion, Asian Journal of Convergence in Technology, 2(3).
- [30] A. Zahra and A. S. Munam (2017). IoT Based Ransomware Growth Rate Evaluation and Detection Using Command and Control Blacklisting, Proceedings of the 23rd International Conference on Automation & Computing, University of Huddersfield, Huddersfield, UK, 7-8.
- [31] CheckPoint (2017). Ransomware: Attack Trends, Prevention, And Response, White Paper.