**Crypto-virology attack : Ransomware**

**Abstract**

With each passing year, cyberspace is witnessing a sharp rise in the number of individuals getting connected. Such drastic increase can be attributed to a myriad of reasons. Many among those connected are unaware of the potential dangers lurking in the cyber world, which also attracts various miscreants and marginalized elements ready to stealthily creep upon an unsuspecting user, unleashing an attack until its often too late for the user, personally, to do anything himself. In this paper, we take a look at one such attack, which employs a ransomware. Ransomwares, are a type of malware, which demand ransom, in order to release the hostage, which is the victims’ precious data. This attack is denial-of-access to the victims’ data. Some ransomwares may simply lock the system, while others encrypt the target machines’ various directories, sub-directories and contained files, demanding a ransom for releasing the key necessary for decrypting the same. A popular form of unleashing ransomwares is by employing Trojans, which masks the illegitimate file. Each year witnesses an increase in the number of such attacks. In this paper, we tread on the path of creation of a simple ransomware, while doing an analysis of the same, in order to understand it better. The ransomware developed employs encrypting the target machines’ various files and demanding a ransom for the release of the decryption key.

**Introduction**

Crypto-virology is the field which ventures into the study of cryptographic techniques being employed for designing a host of malicious software, aka, malwares. It strives to explore and understand the relative power of various cryptographic tools and techniques which aim at further strengthening the menacing power of malwares. The origins of this field trace their roots back to the observation that cryptography based on public key infrastructure (PKI) could be used to create a powerful asymmetry between how an antivirus and an attacker sees and approaches a malware.

The term ‘ransomware’ stems from the combination of the words ‘ransom’ and ‘malware’. It essentially refers to a powerful form of malware which creates a hostage scenario and a demand is put forth for a ransom for securing the release of the hostage. Just that here the hostage are the important data and various files stored on the victims’ machine. They are basically of denial-of-access form of attack. Some simple forms of ransomwares simply lock out the system, while their more advanced peers aim at encrypting the users’ data stored on the infected machine. Ransom is demanded for unlocking the system, or for the release of the key which will aid in decrypting the users’ files respectively.

**Literary Survey**

[1]. This paper tries to investigate the various threats posed by ransomware. It does a comparative analysis of the various ransomwares available, to get a better understanding of the same, with emphasis on the code quality, functionalities and cryptographic primitives analysis.

[2]. This paper presented the results of a long-term study of observed ransomware attacks, and a more holistic view on the evolution of the attacks by taking various samples belonging to different ransomware families.

[3]. This paper presents the analysis of network behavior of Cryptowall ransomware using HoneyPot technology along with automatic run-time malware analytical system Maltester.

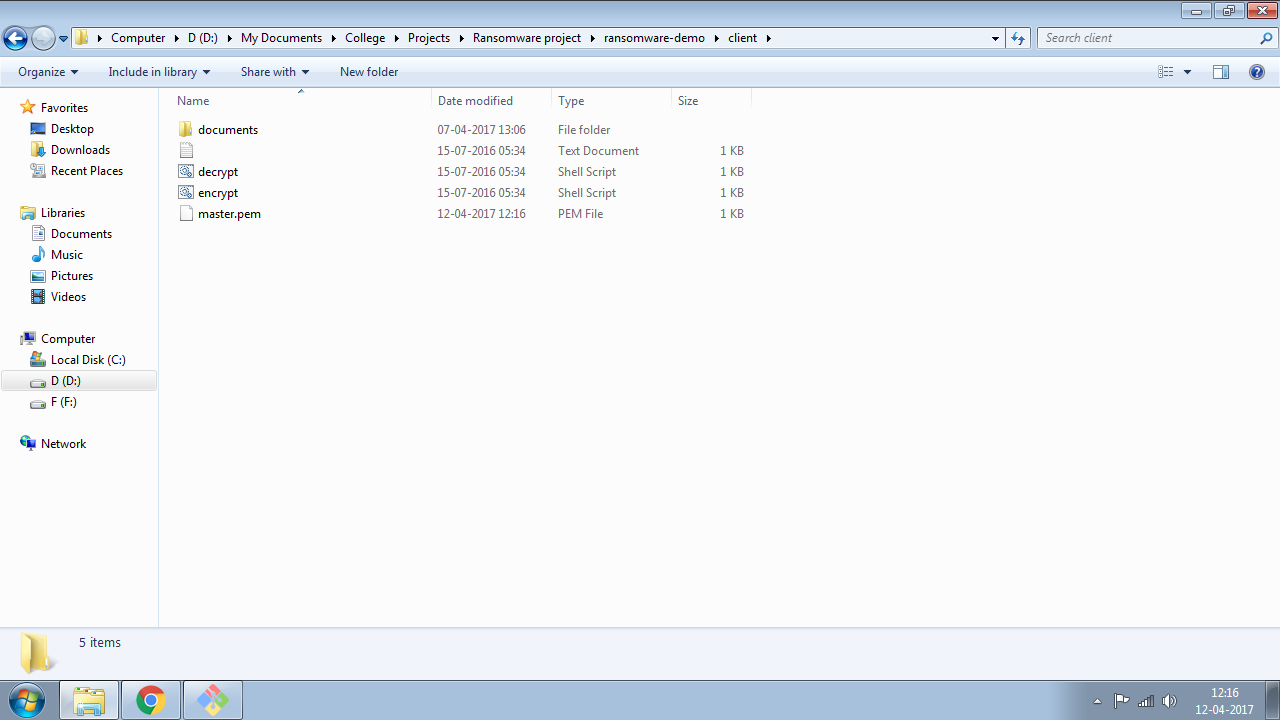
[4]. This paper examines the working of different types of ransomwares, to understand their building blocks, stumbling upon the issues they face in order to successfully develop counter-measures.

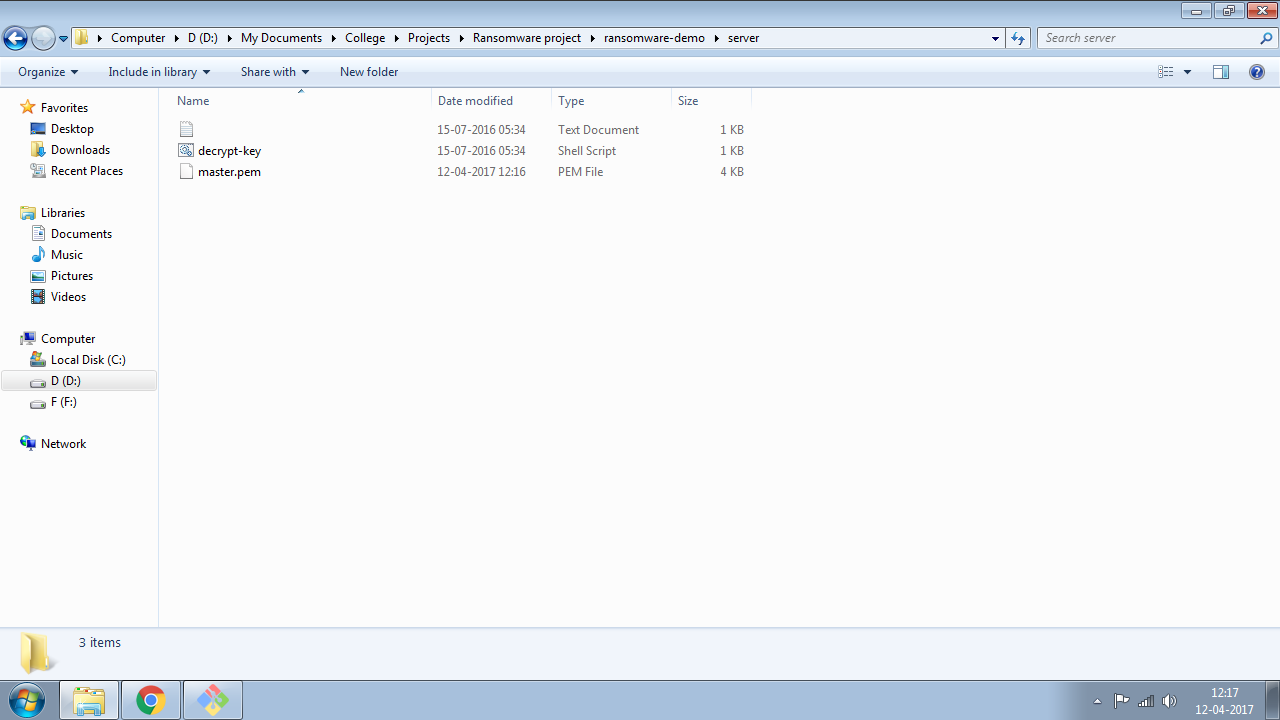
[5]. This paper presents an early-warning detection system, CryptoDrop, that alerts a user during suspicious file activity. Using a set of behavior indicators, it can halt a process that seems to tamper with large amounts of user’s data.

**Experimental Work**

First and foremost, a Command & Control (C&C) infrastructure was developed. It typically comprises of various servers and technical infrastructure used to control the malware in general and guide its actions. Modern systems, are however, independent of any fixed servers, as they were found wanting in situations involving counter-attacks. A public key encryption is employed to defeat any attempts at breaking into or spoofing into the network.

After the C&C is up and running, the ransomware is covertly deployed to the target machine. The C&C center sends a command executing a master key pair generation via RSA (“Rivest, Adi, Shamir”) algorithm 4096 bits, an asymmetric encryption technique. The public key remains with the target client, while the private key is sent back to the server.

Client Folder after creating Master Key. Documents Folder is encrypted

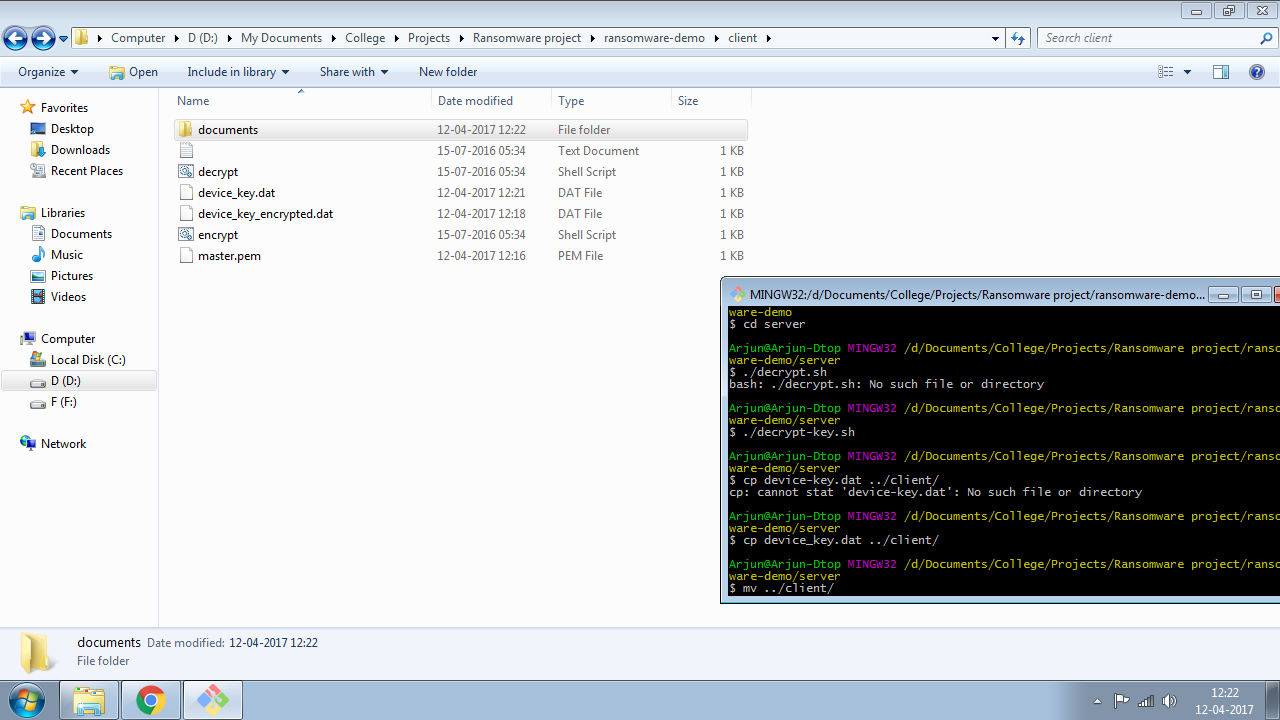
Server Folder after creating master key pair

Once the private key reaches the server, the stage is set for the execution of ransomware. The ransomware developed comprises of both encryption as well as decryption files. These files are provided the file path of, say, C drive. Encryption file, when run, will thereby encrypt all the files contained within C drive, even if present within folders. The command for the execution of encryption file is auto-sent by the C&C server through bash upon receiving the private key. The execution of this command first leads to the encryption of all files contained within the folder whose path has been provided using AES (“Advanced Encryption Standard”) encryption technique, which is based on symmetric encryption. The device key is generated for the same, and this device key is embedded somewhere within the decryption file, which is further encrypted using the master key. The master key basically, is the public key supplied to the client during the master key pair generation.

Cryptographically secure pseudo-random keys are generated, by focusing on n-bytes of ASCII characters, to properly encode the data and preserve the original key. Rand() function is used to develop random keys in the encryption process.

The user will see a message flashing demanding ransom to be paid for successful recovery of the files. And he’ll notice all his original files to have been deleted. In their place would be some newer encrypted files with completely different extensions. In this case, .shadowrun extension files are placed.

Once ransom is successfully paid and detected, the server will send the private key file, and run it through the decryption file already present at client side. It’ll spring forth the device key, and decryption process can then be proceeded with.

Decrypting the Decryption File

**Conclusion**

One can state a ransomware as : “a ransomware is a kind of malware which demands a payment in exchange for a stolen functionality”. This is, in practicality, an aspect of information technology and allied fields, which delves into the darker world of blackmailing and a means of extortion. Ransomwares started appearing near the dawn of the millennia, however, especially over the recent years, have witnessed a marked increase in their threat, which coupled with anonymous online currency sites poses a potent threat. This study was conducted just for the purpose of highlighting the relative ease with which such troublesome softwares can be developed, and the danger posed by them.

**References**

1. Alexandre Gazet – Comparitive analysis of various ransomware varii. In : Springer- Verlag France, J Comput Virol (2010) 6:77-90, DOI 10.1007/s 11416-008-0092-2
2. Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge, Engin Kirda – Cutting the Gordian Knot : A look Under The Hood of Ransomware Attacks. In: DIMVA 2015
3. Krzysztof Cabaj, Piotr Gawkowski, Konrad Grochowski, David Osojca – Network activity analysis of Cryptowall ransomware. In : Przeglad Elektrotechniczny , ISSN 0033-2097, R 91 NR 11/2015, doi : 10.15199/48.2015.11.48
4. Dzenan Bazdarevic, Michael Dubell – Building Ransomware for Fun and Academic Research Purposes. In : Chalmers
5. Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R.B. Butler – CryptoLock (and Drop It): Stopping Ransomware attacks on User Data. In : 2016 IEEE 36th International Conference on Distributed Computing Systerms.