



Ransomware encryption mechanisms

Rezaur Rahman

Incident Handler, BGD e-GOV CIRT

Introduction:

Ransomware is a kind of malware which cryptographically lock user files and prevent them from accessing. As content of the affected files are changed, it becomes unusable for the user. To use these files again, the attacker claims financial benefit, usually in BitCoin, and in return the decryption key is promised to be provided and with which the user will be able to perform decryption and eventually convert the files back to readable format.

But to understand how a ransomware works, first some basic knowledge in cryptography is required and an overview is given below.

Cryptography 101:

In this section, we will briefly discuss on how a encryption mechanism works and how it is used by the malware. After which, we will be able to understand at a basic level that whether we can decrypt the affected files or not.

Symmetric Key:

This encryption mechanism is dependent on a specific key. A mathematically computational process is performed

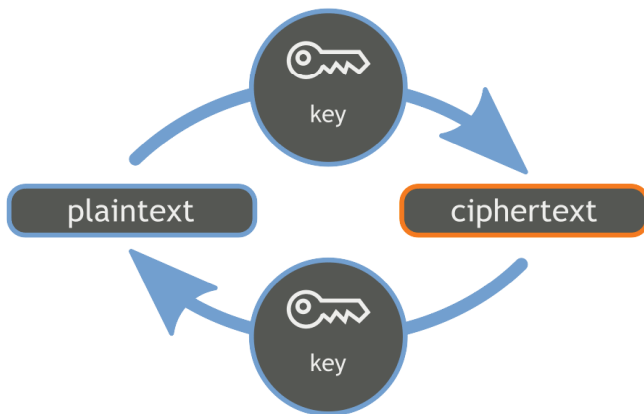


Figure 1: Symmetric encryption (Source: Wikipedia)

on the data to change it with the help of the key and reverse process is applied to revert it back to original form. This key is used to both encrypt and decrypt content of a file. This key can be considered as a lock with which you secure your personal items and those who have the key can unlock and obtain the those items. The process is illustrated in Figure 1.

This key can be any thing from numbers to symbols at any combination. The length of this key is not expected to be short so that it can not be brute forced. For those who are not familiar with brute force, it is a process by which all the character combinations are tested to discover the password.

There are many algorithms which we can use to encrypt

our data securely.

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- Blowfish
- RC4 (Rivest Cipher 4)
- RC5 (Rivest Cipher 5)
- RC6 (Rivest Cipher 6)

One of the primary problem with is method is the key itself. It is quite difficult to either transport this key from one location to another, or store it securely. Such encryption method does not provide any inherent ability to protect the key from outsiders. If the key is obtained by another person, he or she can use this key to unlock the data with ease.

However the performance benefit of this encryption mechanism is high. The data can be encrypted or decrypted extremely fast. If a user want to encrypt a large pool of data, the user will see significant reduction of time when comparing with asymmetric encryption.

Asymmetric Key:

Asymmetric cryptography is also known as public-private key encryption. The public key in this mechanism is being used for encryption and the private key is for decryption. By

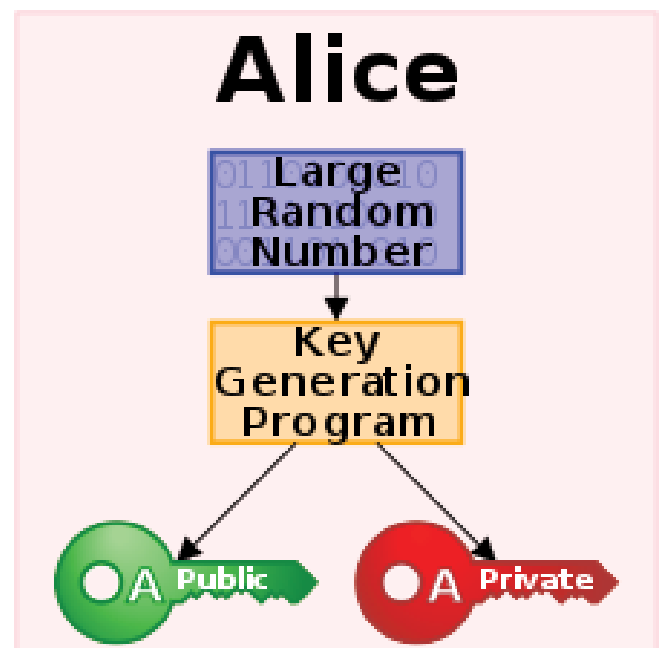


Figure 2: Asymmetric Encryption (Source: Wikipedia)

randomly generating one pair of public key and one private key, which are mathematically related, one of the key is used for encryption and another one is for decryption. »

The primary advantage of this method is that the key can easily be transported. This is because with the public key, one party can only encrypt the data thus the recipient can send his or her public key anywhere with out any issue. As the only recipient has the private key, which is used for decryption, is never being disclosed, only that recipient can decrypt the sent data and view its content. Even if the public key is disclosed to an outsider, the attacker will not be able to view the content because the attacker does not have the decryption key aka private key. Some of the common technologies are given below:

- Diffie-Hellman Key Agreement
- RSA (Rivest Shamir Adleman)
- ECC (Elliptic Curve Cryptography)
- El Gamel
- DSA (Digital Signature Algorithm)

How ransomware effects:

Such malwares usually gains access using various methods. It can range from user running a pirated software obtained from the internet to malware itself invading the user's workstations by exploiting security holes. In many cases, they tend to use chain of cascading processes to gain foothold in the victim's workstation.

Anti-virus programs can help user to identify such programs but unfortunately, in many cases they are not taken seriously and users tend to ignore the notifications rather then to investigate and find out what might happen if actions are not taken immediately. This problem is exacerbated by users allowing software like cracks and keygens to run, overriding the anti-virus's recommended actions.

If the penetration is successful, the ransomware quickly tries to encrypt user files. System files and other critical directories are ignored as if they are modified, the system will become inoperable.

In the next sections we will briefly look into the method which ransomwares use to encrypt user data.

Symmetric method:

The primary advantage of this method is the speed of encryption. As symmetric encryption is very fast, it gives users very little time to react after first detecting any abnormalities caused of the virus. But like any other symmetric encryption mechanism, the key to encrypt and decrypt is same thus if the key can be located, the process can be reversed and the original content can be obtained.

Since this key has to be stored somewhere in order to either continue the encryption process or perform decryption after receiving extorted amount, the key should be in decrypted state so that the process can continue. Researches can try to find this key and use it to decrypt user files to its original state.

Asymmetric method:

Using this scheme, a previously generated private and public key pair will be used and the public key, used for encryption only, will be hard-coded inside the malware. By this way any other decryption method is rendered impossible. Without the private key for decryption, valued files of the user will be lost.

However, this method has its own problem as the private key of this process will remain same for every user it infects thus if a ransomware is paid, the attacker will have to release the key to ensure others continue to do so to recover their files but releasing the private key means it can be used to decrypt all other systems as well.

Hybrid method:

This method, from a ransomware's perspective, is one of the most effective way to render victims files unusable. The recovery mechanism is almost impossible as they use the speed of symmetric encryption and the security of asymmetric encryption thus making the whole system almost impossible to reverse engineer.

The simplified version of this method is, firstly the malware connects to a Command & Control (C&C) system over the internet to generate a public key and private key pair. As the public key is used to encrypt, it is transported to the end user and the private key is stored inside the control server.

If the above operations succeeds, the malware moves to the next phase of the operation. It should be noted that, if the key generation process is not successful, the malware does not take any further steps. The ransomware moves to next stage by generating a symmetric key to encrypt the user files. It quickly encrypts users valuable files like personal photos or official documents and changes the extension of those files. As symmetric encryption method is fast and it targets specific file extensions, they usually perform their actions very swiftly and does not give users any chance to react.

And finally, when the malware finises encrypting all the files, the symmetric key is encrypted using the public asymmetric key. All other traces of the encrypting symmetric key is now removed from the system making the author of the C&C server the only entity who can practically decrypt the user files.

Vulnerability in ransomware:


All the algorithms are considered unbreakable but fortunately for us that the standards of those algorithms are not properly implemented inside the ransomware and consequently security researchers can take advantage of those security holes and make tools to decrypt the files.

Moreover, there are also some weaknesses which can be used against the ransomwares to make them unusable. Some of the key weaknesses which has been observed in real life scenario has been given below:

- i. Any encryption method which has been created by the author of the ransomware can be reverse-engineered.
- ii. Storing the key in the victim's computer can be obtained.
- iii. Already vulnerable algorithms used by the ransomware can be exploited to gain the key.
- iv. Without the C&C server some ransomware does not function, thus taking those servers out from the internet can stop the infection.

Conclusion:

As problems with ransomware has been discovered and exploited to gain the key and eventually to decrypt the files, more and more ransomwares are embracing more standard implementation of those algorithms thus making it more difficult to develop tools to decipher user files.

Thus obtaining files from valid sources and updating software in a regular basis must be enforced to make sure we can protect ourselves from such harmful software. Additionally, we all should keep ourselves aware of the danger and consequences if an attack happens and learn potential attack vector to keep not only ourself but also our family safe 

Feedback : rezaur.rahman@cirt.gov.bd