International Journal
Information Technology Applications (ITA)

Volume 12, Number 2, December 2023

RANSOMWARE ATTACKS AND DEFENSE AGAINST THEM

Miloš Vydarený

Abstract:

In this work, we focus on analyzing the current situation from the perspective of ransomware attacks. In the first part, we describe various types of ransomware and strive to provide a brief characterization of each. From the information gathered through the analysis of the issue, we present currently used software solutions and mention educational resources describing this type of attack, which can serve as a proper informational tool for those unfamiliar with the subject. With the knowledge acquired, we will create a set of preventive methods and procedures aimed at preventing the infection of information systems by ransomware. After implementing preventive solutions, we focus on detecting specific ransomware and on further obtaining information about their functionality and weaknesses based on the use of selected malware analysis methods. The knowledge obtained is then used to introduce measures to minimize their impacts.

Keywords:

Ransomware, Malware, encryption, security, Antivirus, attacks.

Introduction

Ransomware is a type of malicious software, or malware, that prevents the user from accessing computer files, systems, or networks and demands a ransom to restore access to the data. Ransomware attacks can cause costly disruptions to operations and loss of important information and data. An attack with this type of software often manifests only after infection. When infected, users typically do not know that their computer has been compromised by this software. It is usually discovered when they notice that their data is inaccessible or its content is corrupted, and they are then informed about the attack through a pop-up window or by finding a text document left by the attacker outlining what has happened on their computer, along with a specified form of payment method.

Types of Key Management For a successful attack, the ransomware must encrypt the user's data in such a way that the user cannot restore it themselves while ensuring a way for its recovery if the ransom is paid. Therefore, choosing the right method of key management is one of the primary elements for a successful ransomware attack. Symmetric Encryption In this type of encryption, the ransomware uses the same key for both encrypting and decrypting data. Currently, because of this property, symmetric systems are not often used as standalone encryption forms. They are most commonly found in less professional ransomware with a smaller number of infected devices, where protection can be established within a few days. One of the most used algorithms is AES (Fig.1). One of the main advantages of symmetric encryption is its speed. This property is highly sought after in this type of application when it is necessary to encrypt a large volume of data in the shortest possible time.

It is mainly because the ransomware needs to encrypt as much data as possible before an antivirus program might detect a certain pattern in file access and subsequent modification. It might also notice excessive use of cryptographic API. Thus, the more data we are able to encrypt before placing it into quarantine by the antivirus (Fig.2), the better.

One of the main disadvantages of symmetric encryption in this application is that poor hiding of the key can lead to its subsequent discovery. Immediately after encrypting the data, actions must be taken to ensure that the used key is moved out of the user's reach.

One method could be hiding the key on the user's disk. Subsequently, the attacker can send a decryption program capable of finding and using this key to decrypt. More often, however, the method used is such that the symmetric key is present on the victim's computer only during the encryption of files, after which the key is deleted from the computer and sent to the attacker's server. This method has a fundamental problem in that if the victim's PC does not have current internet access, the program can encrypt the data without sending the key to the attacker, meaning that no one can access it, resulting in the data being lost. Some ransomware using this method employs a strategy where they only encrypt if they can connect to the attacker's server, where key collection occurs, and if they do not connect to the server, the encryption process does not occur.

Asymmetric Encryption Asymmetric cryptography, also known as public-key cryptography, uses a mathematically related pair of keys, e.g., a public key for encryption and a mathematically paired private key for decryption (or vice versa). The RSA algorithm is an asymmetric cipher favored by ransomware. Currently, with the right choice of key length, it is not possible to break the encryption, i.e., to obtain the private key within a reasonable time frame, relying solely on the public key and knowledge of the algorithm. When properly implemented, this approach offers greater flexibility to attackers and prevents reversing the encryption without knowledge of the attacker's private key. This implementation usually requires a connection to the internet to function correctly due to sending the generated private key to the attacker's server. Sometimes, the method is also used where the attacker generates one private and one public key before distributing the ransomware, with the public key directly implemented into the ransomware code. The disadvantage of this method of implementation with the public key written directly into the code is associated with the existence of only one private key for decrypting data on all infected devices. Once one user obtains this key, they can make it public, thus making this ransomware irrelevant. However, the main disadvantage for attackers is the fact that encryption with asymmetric cryptography is slow and increases the size of the cryptogram compared to the corresponding plaintext. The encryption process is lengthy, and encrypted data require more storage space on the host.

When encrypting with RSA, we would need to chunk the data into blocks based on the length of the public key, e.g., when using a key with a length of 2048 bits, we can encrypt data with a size of 256 bytes. However, this comes with a problem if we wanted to encrypt data of size 230 bytes, as they would become 256 bytes when encrypted. This way, we could quite significantly occupy space on the disk when encrypting large volumes of data, which is not a desired phenomenon. For this reason, asymmetric encryption is mainly used to encrypt the symmetric key used to encrypt the data on the target PC. This procedure is called hybrid encryption.

1 Hybrid Encryption

Generally, it is known that recent ransomware has employed a hybrid approach combining the previous two models to utilize the best of both types. The user's data are encrypted with a symmetric cipher for speed, while the symmetric key used for encryption is then encrypted using the attacker's public key. This public key is most often part of the ransomware code.

Steps of the Attack Using Hybrid Form

A Ransomware accesses the target person's PC and launches. Most commonly, it gets onto the PC due to the user's actions (phishing, social engineering). Penetration into the PC without the user's fault happens very rarely, most often with the use of exploits.
B Ransomware uses the cryptographic API available on the host to generate the encryption key, very often using AES-256.
C Ransomware encrypts this newly generated symmetric key using the public key (e.g., RSA-2048) contained in the ransomware code and then sends this encrypted key to the attacker. If internet connectivity is unavailable, the key is stored on the disk (the person with the infected PC may have access to it, due to its worthlessness in encrypted form) and then sent when internet access is detected.
D The user's data are encrypted using the symmetric key.
E Subsequently, the ransomware securely deletes the unencrypted symmetric key located on the infected PC. This key is usually never written to the disk; it is stored only in the operational memory during the file encryption period.
F The user is presented with the ransomware's graphical interface with the expectation of paying the ransom.

Crypto Ransomware

This is one of the most widespread types of ransomware. Its primary method of attack involves penetrating the target person's computer through social engineering or phishing. The simplest way to access this type of software is through files and URLs sent via dubious emails or chat applications. Most often, it is a program that masquerades as another file or program. The main functionality of this "software" is to gain access to the user's data for the purpose of encrypting them. In most attacks of this type of ransomware, the user will still be able to use their PC. Thus, the attacker's intent is not to completely disable the target system, but only to encrypt the data and then inform the user of the ransom amount that must be paid within a certain time limit to restore the encrypted data. These types of ransomware achieve non-disabling of the infected system by selecting such components for encryption where no critical system files are located, or by filtering file extensions, e.g., .dll. If the user does not meet the ransom payment deadline, the data may be deleted or remain in encrypted form. The behavior in this scenario is purely based on the implementation chosen by the attacker in the code. What happens to the data after the time limit expires is not guaranteed just as what happens to them after paying the ransom. In many cases, even after paying the ransom, we may not receive the key to decrypt the data. The reason is that some circulating ransomware is currently available online without any attacker managing and caring for the decryption of data, or even collecting the ransom. This means that the money, which the victim sends, for example, to a Bitcoin wallet, may remain locked there forever, because the attacker may no longer have access to its private key.

WannaCry Ransomware

WannaCry (Fig.3) is the most famous representative of crypto-ransomware. The program reached users in the form of an EXE file through emails or downloading dubious files. However, its spread primarily involved the use of an exploit that worked on the Microsoft Windows platform. The exploit arose due to a faulty implementation of the Server Message Block (SMB) protocol, which helps various nodes in a network communicate, mainly when sharing files on the network. This unpatched version of the implementation allowed the running of programs on other computers on the network using specially crafted packets (EternalBlue exploit). Immediately after launching on the target PC, the malware begins to search the network for other PCs on port 445 with an unpatched version of the SMB protocol.

This network spread makes WannaCry ransomware one of the most widespread. It is an attack where a user can be infected even without their own fault, as the ransomware spreads automatically through the network and seeks out other vulnerable systems. Due to the speed and scope of this spread, WannaCry became globally known and extraordinarily costly ransomware that affected a large number of organizations and individuals worldwide. WannaCry uses asymmetric encryption to block access to files on the infected computer, while demanding a ransom be paid in bitcoins for the victims to obtain the decryption key and restore their data. The severity of the attack was emphasized by the fact that many hospitals, large companies, and government organizations were among those affected, which in some cases had serious consequences for providing healthcare and other critical services. The WannaCry case highlighted the importance of regular software updates and the need for robust security protocols in organizations.

Further steps included in the prevention and response to ransomware like WannaCry include:

- Software Patching: Immediate application of security patches to software and operating systems to prevent the exploitation of known vulnerabilities.
- Data Backup: Regular backup of important data on separate and secure media can limit the damage caused by a ransomware attack, allowing quick recovery without the need to pay.
- Employee Education: Strengthening security awareness among employees so they can recognize and avoid suspicious emails and links that may contain malicious content.
- Use of Security Tools: Implementation and maintenance of antivirus software and a firewall, as well as the use of intrusion detection and prevention tools (IPS/IDS).
- Network Segmentation: Dividing the network into smaller segments can limit the ability of ransomware to spread in case it enters the internal network.

Creating a comprehensive and layered security approach is key to protecting against ransomware attacks. Integrating preventative measures with response strategies ensures that organizations can effectively respond to threats and minimize potential damages caused by these attacks.

```
private static String secretKey = "boooooooooom!!!!";
private static String salt = "ssshhhhhhhhhh!!!!";

public static String encrypt(String strToEncrypt, String secret)
{
    try
    {
        byte[] iv = { 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 };
        IvParameterSpec ivspec = new IvParameterSpec(iv);

        SecretKeyFactory factory = SecretKeyFactory.getInstance("PBKDF2WithHmacSHA256");
        KeySpec spec = new PBEKeySpec(secretKey.toCharArray(), salt.getBytes(), 65536, 256);
        SecretKey tmp = factory.generateSecret(spec);
        SecretKeySpec secretKey = new SecretKeySpec(tmp.getEncoded(), "AES");

        Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
        cipher.init(Cipher.ENCRYPT_MODE, secretKey, ivspec);
        return Base64.getEncoder().encodeToString(cipher.doFinal(strToEncrypt.getBytes("UTF-8")));
    }
    catch (Exception e)
    {
        System.out.println("Error while encrypting: " + e.toString());
    }
    return null;
}
```

Fig.1. Example of encryption using an AES 256 key.

Fig.2. Modern antivirus applications.

Fig.3. Wannacry ransomware warning, ransom demand.

Conclusion

Addressing ransomware requires a comprehensive approach that includes legal, technical, and ethical aspects. Organizations should consider all the consequences of paying the ransom and focus on prevention, detection, and rapid response to cyber threats. At the same time, they should comply with applicable laws and regulations in their jurisdictions and maintain open communication with stakeholders about their security measures and procedures for addressing attacks.

Acknowledgement

This contribution was made with the support of Mr. Ralf Wunschov-Train Consult Korneuburg, Austria, and the training center Wifi Wien Währinger Gürtel, Vienna.

References

[1] Bratvogel, K., (2022). Network Fundamentals. HERDT-Verlag. 227 p, ISBN 978-3-98569-047-3.

[2] Matoušek, D., (2016). C++ without prior knowledge. p.19-30, ISBN 978-80-251-4640-8.

[3] martin.haller@patron-it.cz Retrieved online, May 2024, https://martinhaller.cz/ransomware/prednaska-zalohy-ktere-nepreziji-ransomware/

[4] martin.haller@patron-it.cz Retrieved online, May 2024, https://martinhaller.cz/ransomware/postrehy-ze-zasahu-pri-ransomware-utoku/

Authors

Miloš Vydarený
Faculty of Informatics, Pan-European University, Bratislava, Slovakia
xvydareny@paneurouni.com
His research interests include the field of cybersecurity, the topic of cryptography, ethical hacking and the complete area of computer networks from their design, implementation, deployment, and protection.