ENCRYPTING VIRUSES

[1]Omkar Darekar, [2]Dnyanesh Mohite

[1]Cyber Security Analyst, [2]Cyber Security Analyst,
Security Intelligence & Operation,
Nuance Communications (A Microsoft Company), Pune, India

Abstract: **Encrypted virus is a computer malware that has become a serious threat to global business in the last five years. An encrypted virus is defined as a computer virus / malware that can encrypt the payload and make it difficult to detect. Ransomware and Crypren are examples of encrypted viruses that encrypt victims' files. Encrypted viruses use encryption methods to hide them from malware (antivirus) scanners. Shuffle the code to prevent detection. However, all encrypted files in your computer system require decryption, so you can use anti-malware integrated with decryption to detect viruses. Encrypted virus-related variants are characterized by encrypting files on infected computer systems and networks, while some variants delete files or computer networks / systems. It is intended to block access to. When infected, the encrypted virus modifies existing registry entries and destroys system processes that can interfere with encryption. To perform encryption on a computer system / network, an encrypted virus can probably start performing numerous activities on the host computer, perhaps starting by checking if the virus propagates in a virtual environment. increase. If the confirmation is positive, the virus may delete itself and the file will not be encrypted. However, in a real operating system, when an encrypted virus invades your system, it will begin encrypting your files.**

***Index Terms*—Virus, Encryption, Decryption, Malware, cryptography, trojan, cracker.**

I. INTRODUCTION

A. What is encryption?

Encryption is a method of scrambling data so that only authorized parties can decrypt it. Technically, it's the process of converting human-readable plaintext into incomprehensible text, also known as ciphertext. In short, encryption modifies the readable data to appear randomly. Encryption requires the use of an encryption key, which is a set of mathematical values agreed upon by both the sender and the recipient of the encrypted message. Encrypted data looks random, but the encryption is done in a logical and predictable way, so the party who receives the encrypted data and has the correct key decrypts the data. It can be converted back to plain text. True secure encryption uses very complex keys, so it is unlikely that anyone else will brute force or crack the ciphertext. That is, guess the key. Data can be encrypted "on save" when saved. Or "on the go" if transferred to another location.

B. What is decryption?

Decryption is a cybersecurity technique that makes it difficult for hackers to intercept and read data that they do not have permission to read. This includes converting encrypted or encrypted data or text to its original plain format that can be read and understood by computer applications. This is the opposite of encryption and should prevent anyone except those who have a matching decryption key from reading the encrypted data.Encryption protects the data, but the recipient must have the decryption or decryption tools needed to access the original data. Decryption is the process of decrypting data that can be performed manually, automatically, or with the best decryption software, unique keys, passwords, or codes. This transforms unreadable or incomprehensible data into the original text file, email message, image, user data, and a directory that users and computer systems can read and interpret. Example, assume 2 x = y. The function's key is then fixed and you can map all possible values of x and y. In short, this is what happens during decryption. The example shown is one that could be easily solved using "bruteforce" methods.

II. WHAT IS AN ENCRYPTED VIRUS?

An encrypted virus is a computer virus that encrypts its payload with the intention of making detecting the virus more difficult. However, because anything encrypted needs a decryptor or a key an antivirus can use the decryptor as the method of detection.

In other words Encrypting Viruses are a form of computer virus that can cause significant problems if they are identified. The world depends on computer systems for their daily work. Once the device is infected, the encryption virus begins to encrypt all important and sensitive documents and files stored on your computer or laptop, which can make the files unusable or unreadable. Therefore, it is considered one of the most dangerous viruses. be deleted, which may result in data loss or an automatic factory reset, which may involve deletion of all accounts and all important information. Use encrypted ransomware. This has become the most popular variant. Malicious code encrypts everything on your computer and keeps it for ransom. Currently, most ransomware uses the AES RSA encryption method, which is very difficult to crack. Ransomware viruses encrypt data as if it were actively encrypted. However, it is hidden in another file that needs to be unlocked before it can be decrypted. Viruses that cause ransomware can encrypt files without your knowledge and without your consent. An encryption key is generated offline and inserted into malware before it is sent for an attack, or embedded in malware sent during an attack. Once the data is encrypted and the ransom is paid, the virus will create a tutorial to recover the decryption key. You will be redirected to a page where you can download the decoder you needIf the malware contains a fraudster's request not to pay for the decryption, the infected file controls the affected PC. Once the ransomware has been identified as the file encoder that encrypted the file and you know which encryption strand is used, you can look for a decryption method that can restore access to the file. The underlying problem is that the files are still encrypted even after the virus has been removed. Antivirus programs often encrypt data, but cannot decrypt files after infection. In some cases of ransomware, the file is encrypted, disrupting the network connection, forgetting where the malware came from, and cannot be detected and removed until the antivirus software returns the file.

III. HOW ENCRYPTED VIRUSES WORK

From the beginning, virus writers have sought to implement the evolution of virus code. One of the easiest ways to hide the functionality of the virus code was by encryption. The first known virus to implement encryption was the cascade in DOS4. The virus starts with a certain decryption function, followed by the encrypted virus itself.. leasi, start; Decryption position (dynamically set)This decryption because the SP register (stack pointer) is used as one of the decryption keys. Note that the feature has a debug protection feature. Cascade provides itself to the document, so if two host packages are the identical size, SI will give the identical value. but, if the host software size is specific, the SI (decryption key 1) will exchange. The SP sign up is an easy counter for the range of bytes to decode. observe that decryption proceeds in key duration words (2 bytes).however, the decryption function is shifted forward via 1 byte every time. This complicates the decryption loop, however its reversibility remains the same. note that a simple XOR is very useful for viruses, as XORing the identical value doubles the initial fee. recall encrypting the man or woman P (0x50) with the key 0x99. 0x50 XOR 0x99 is 0xC9 and 0xC9XOR 0x99 reverts to 0x50. It's why virus writers love easy encryption-they're lazy! you may avoid implementing two specific algorithms, one for encryption and one for decryption.

```
mov     sp, 0682        ; length of encrypted body (1666 bytes)

Decrypt:
xor     [si],si ; decryption key/counter 1
xor     [si],sp ; decryption key/counter 2
inc     si      ; increment one counter
dec     sp      ; decrement the other
jnz     Decrypt ; loop until all bytes are decrypted
```

```
Start:  ; Encrypted/Decrypted Virus Body
```

Fig. 1. Encrypt

From an encryption point of view, such encryption is susceptible, but early antivirus applications had little choice but to pick out an identity string from the decryption characteristic itself. However, this precipitated many issues. several extraordinary viruses can also have the same decryption characteristic, however they will have absolutely one-of-a-kind functions. through detecting the virus with the decryption characteristic, the product cannot become aware of the variant or the virus itself. More importantly, non-viruses like anti-debug wrappers may also have similar decryption abilities before the code. As a result, viruses that use the equal code to decrypt themselves are complicated.

```
    add     edi,ebp     ; Adjust according to base
    mov     ecx,0A6Bh   ; length of encrypted virus body
    mov     al,[key]    ; pick the key

Decrypt:
    xor     [edi],al    ; decrypt body
    inc     edi ; increment counter position
    loop    Decrypt     ; until all bytes are decrypted
    jmp     Start       ; Jump to Start (jump over some data)

DB    key     86          ; variable one byte key
```

```
Start:                    ; encrypted/decrypted virus body
```

Fig. 2. Decrypt

This kind of simple code evolution technique appeared very early inside the 32-bit home windows virus. W95 / Mad and W95 / Zombie use the same era as Cascade. The simplest difference is the 32-bit implementation.

IV. EXAMPLE OF ENCRYPTING VIRUSES

Ransomware and Crypren are said to be examples of the encrypted virus that encrypts the sufferers' files. Ransomware is a type of malware that become first invented and implemented by means of young and Yung at Columbia college in 1996, which might be utilized by the cybercriminals, with the aid of hazard if the computer gets inflamed with the ransomware it'll help in blocking the get admission to to the machine or its records. Crypton is a ransomware type of the virus which is venomous software which can silently input into your computer device.

These encrypting viruses input into the pc networks through e-mail, junk mail, attachments, etc. compared to the diverse different viruses the encrypted virus is tough to be detected. At instances it's far very important to put in an antivirus that allows you to assist in detecting and in removing the feasible encrypting viruses because in large corporations wherein there are a massive range of tasks and dates which are being stored within the pc devices if get destroyed due to the encrypting viruses it may result There are the ultra-

modern security strategies in order to help in protecting the computer machine from such viruses. This admin account has to be used for browsing thru the internet pages, it must be finished by way of creating a separate consumer account with a purpose to be used for doing maximum of the online paintings.

A. Encrypted Virus Distribution

The introduction of the state-of-the-art encrypted virus is maximum probably due to the ever increasing digital surroundings. Cybercriminals that purchase and distribute malware are probably to make use of the most common processes, together with dangerous redirects, junk mail campaigns, and software installations, among others. Even as maximum encrypted virus infections are opportunistic and spread through informal contamination techniques which includes those described above, in rare instances, the perpetrators of these cyberattacks act explicitly concentrated on a particular sufferer or pc device/network. While hackers get admission to crucial systems to extort cash from the victim, this may happen (s). Over the preceding half of decade, encrypted virus types have won data exfiltration, involvement in allotted denial of provider (DDoS) cyberattacks, and anti identification traits. For example, one type of Ransomware is known to erase files regardless of whether or not the ransom is paid. Users can lock cloud based backups in other versions, regardless of whether the system automatically backs up their files in realtime. Different types claim to be the property of law enforcement agencies. The victim is required to pay a fee for committing a crime or engaging in illegal activities such as accessing obscene content on their computers. These renowned versions can determine the actual location of the victims to quote the name of a nearby law enforcement agency acquainted with the victims to appear legitimate to the victims. Users are urged to pay money to scammers without thinking about whether any law enforcement agency will remotely shut someone's computer or demand penalties to unlock it.

B. Encrypted Viruses Threats

Encrypted viral threats are files, statistics, or device settings which have been altered by way of infectious software program or a computer virusThese viruses gather access to a pc machine with the aid of loading themselves onto computing device apps or crawling up from under the running system's surface. they may then delete or change device settings, replacing them with phony ones designed to steal personal and financial statistics. as soon as the system has been compromised, it's essential to dispose of the malicious documents and restore them to their original state. This is when a backup application for an infected file machine is available, as these software solutions will let you run a healing scan and restore the damage. When IT workers find out that their structures were compromised, they often flip to an encrypted viral risk event reaction approach. With these infections, it is crucial to keep an actual time database of infected documents so that new infections may be addressed quickly. One way to do this is to use an access database or ADR. A console application, such as the gadget restore software program, is any other alternative. The primary technique is simpler to apply and greater realistic for novice users, whilst the second method is more ideal to IT experts who need to restore a backup in real time. The installation of a backup utility for encrypted report stations, in contrast to putting in an file server (additionally called the "ADR"), relies upon totally at the software program dealer. It's important to contact the company to determine whether the required software can manipulate encrypted malware threats. The switch of personal information from one cell tool to some other might be tough. This is mainly true while dealing with virus payloads that are encrypted. safety is commonly a huge trouble while using a phone or pill. the various secret data packets dispatched via those gadgets will very indeed now not be encrypted. Therefore, the records are more likely to fall into the wrong fingers. Consequently, it's essential to keep all touchy information safe always. A cozy storage and distribution mechanism enables businesses to cope with capacity non-public statistics theft from their networks. This is in particular crucial given the chance of random encryption. encryption on cellular gadgets can significantly assist defend your corporation from surprising attacks. Decryption should be achieved frequently to maintain facts integrity. Whether or not the cutting-edge shape of mobile tool encryption meets those requirements, or whether a corporation wishes to build a framework for more suitable protection, relies upon numerous elements.

C. Encrypted Virus Payload

Encrypted virus payloads can be extra difficult to find than exceptional varieties of malware that use desired anti-malware software program applications. The virus may additionally make an effort to absolutely encrypt machine / network intrusions. This means that if you suspect an encrypted virus, you could take away it clearly earlier than it complicates the entire detection and removal technique. Security researchers have proposed using a security policy that stops payload invocation to avoid malware infections. but, this does not guard the entire system. it's far crucial to properly re-upload your business enterprise's records, as a few attackers use encrypted viruses to scouse, borrow or delete files from the victim's pc gadget / community. laptop structures blanketed via the contemporary safety updates from software program companies can help mitigate the ones network vulnerabilities. Every other opportunity is cyber hygiene. This indicates be careful when clicking on hyperlinks or e-mail attachments and avoid public networks if possible. The inflamed pc additionally wishes to be disconnected from the network.

V. THE FUNCTIONALITY OF ENCRYPTING VIRUS

Cybercriminals use encrypted ransomware. this is the most commonplace type due to the fact it's miles hard to break the encryption and put off the malware. All facts stored for your computer is encrypted with malicious code for ransom purposes. most contemporary ransomware uses AES-RSA encryption, that is extraordinarily tough to crack. The ransomware virus encrypts a document as though it has been actively encrypted, but in reality the record is hidden in any other document and after the defined set of conditions is unlocked. watch for it to be decrypted. inside the case of ransomware, the virus can encrypt files without your consent without your know-how. Encryption keys are generated offline and embedded in malware before they are despatched for an assault, or embedded in malware that is sent at some point of an attack. As soon as the report is encrypted, the virus creates a tutorial to get a decryption key that may be used if you pay the ransom. you will see a hyperlink to download the required decoder. If the document includes a fraudster's request now not to pay the value of decryption, the inflamed document will hijack the computer tormented by the encrypted virus. As soon as the ransomware is recognized as the record encoder that encrypted the document and which particular encryption strand is in region, you could discover a decryption mechanism that could assist repair and get admission to the report. i

will do it.but, trying to decrypt a record without first doing away with the malware can cause the report to be encrypted once more. In case you are not sure with which ransomware you have been hit, a ransomware tool referred to as Crypto Sheriff can identify the virus through analyzing one of the encrypted files. The function of the encryption is easy: The checksum and the decryption stubs are calculated with XOR keys within the feature frame. This is the maximum critical variety that is generated throughout the complete malware due to the fact it is vital to get better the record while the encryption set of rules is used to alternate the authentic code. Once you get a deal with the cryptographic key, the encrypted nation is displayed, followed by means of MoveFileWithProgressW, this means that that one has been encrypted. The actual problem is that the files remain encrypted even after the virus is eliminated. Antivirus packages regularly encrypt records, however cannot decrypt documents after contamination. it could be reported encryption ransomware that still affects your community connection. As a result, the malware is simply too forgotten to be detected and eliminated until it's miles back with the aid of antivirus software. A is a symmetric set of rules. That is, the same key used for encryption is used for decryption. Asymmetric encryption is a greater at ease form of encryption. That is because the simplest one birthday celebration knows the personal key, at the same time as both events know the public key. The alternative part encrypts the statistics with the "public key" and also you decrypt it with a unique "personal key" which you own. The ransomware begins by means of taking the general public key, that is embedded in the executable document itself, and uses it to encrypt the key or password with a random number. The ransomware makes use of this to take over the encryption key and encrypts it with the passing — in text and password as random numbers, after which uses brute pressure to decrypt the virus by means of itself, instead of trying to repair the encrypted key by itself. At the time of writing, there aren't any files which might be encrypted through this virus. regrettably, anti malware and security gear cannot restore encrypted files, nor can they put off or restore the harm of the ransomware. alternatively, ransomware assaults on Android devices surged as cybercriminals realized that many had been unaware that smartphones could be attacked.

A. What can you do to prevent infection?

First, do not use your admin account to surf the internet. Create another user account with limited system privileges and use that account to perform most of the work onlineSee previous blog posts on this topic for more information. Next, pay attention to the attachment that opens. Email attachments are a common attack vector and for good reason. Because you can easily send and receive important documents, you can easily overlook the fact that these attachments may contain malware that can infect your system once opened. Therefore, it is important to think about the source of the attachment before opening it. As a rule of thumb, never open attachments from strangers. And even if you receive an attachment from someone you know, agree with yourself and make sure they actually sent it to you. Third, Check if your e-mail or webmail carrier routinely scans for viruses. If no longer, switch to one which does. For my part, Gmail is a tremendous webmail service with sturdy security functions and protection from a variety of threats. Fourth, don't observe hyperlinks from emails, except you are certain they can be depended on. links can be used to deliver malware for your device. And given that a hyperlink isn't always a chunk of code, it won't be detected by your email provider or malware scan. if you receive a suspicious electronic mail containing hyperlinks from a recognized supply, contact that individual and ask if they sent you the email. if they didn't, it can suggest that their device is infected and is spamming their touch list. If in doubt (and unluckily you should always achieve this), send the link in question to a service inclusive of VirusTotal.com. There you could add documents or test links for malicious content material. And sooner or later, don't randomly download all of the free packages you could discover and cross across the internet. absolutely positioned, unfastened is not often "unfastened"And these applications are regularly a source of malware. So before you download the latest "free weather toolbar" or different widget from an unknown web page, do some homework. frequently you could discover whether or no longer a loose software is on the level just by googling it.

VI. CONCLUSION

Encrypted viruses are propagated via several methods. Most of these methods are user initiated and prompt computer users to click links with malicious content, email spam, infectious attachments, or even legit attachments combined with infected codes. Computer users can be fooled into accessing malicious or malware-infected websites. In other cases, security experts ask computer users to confirm the source of the email and do not download the emailed attachments, as simply downloading the virus-infected file will cause the infection. I advise you to. The encrypted virus can be transmitted in other ways as well. For example, if a virus is introduced into a victim's computer system as a malicious program (crack, patch, key generator software). Attackers can propagate malware via malvertising or drive-by downloads and require little or no human intervention to enable propagation.

REFERENCES

1. M. Z. Hasan, M. Z. Hussain and Z. Ullah, ”Computer Viruses Attacks and Security Methods”, LGURJCSIT, vol. 3, no. 3, pp. 20-25, 2019.
2. R. Tahir, ”A study on malware and malware detection techniques”, International Journal of Education and Management Engineering, vol. 8, no. 2, pp. 20, 2018..
3. A. Mohanta and A. Saldanha, ”Malware Analysis Lab Setup”, Malware Analysis and Detection Engineering, pp. 25-50, 2020.
4. J. Menn, ”Exclusive: Russian antivirus firm faked malware to harm rivals - Ex-employees”, [online] Available: http://www.reuters.com/article/us-kaspersky-rivals-idUSKCNOQJ1CR20150814.
5. Dan Price, ”Types of Email viruses”, October 2016, [online] Available: https://www.makeuseof.com/tag/types-computer-viruseswatch/.
6. Aishwarya Khaire, Alok Goyal, Anita Thengade and Devaj Mitra, ”Virus Detection Techniques and Their Limitations”, International Journal of Scientific Engineering Research, vol. 5, no. 10, pp. 24-27, October 2014, ISSN 2229-5518.
7. R. Tahir, ”A study on malware and malware detection techniques”, International Journal of Education and Management Engineering, vol. 8, no. 2, pp. 20, 2018.
8. M. Z. Hasan, M. Z. Hussain and Z. Ullah, ”Computer Viruses Attacks and Security Methods”, LGURJCSIT, vol. 3, no. 3, pp. 20-25, 2019.