Breaking Ransomware

Explore ways to find and exploit flaws in a ransomware attack

JITENDER NARULA
ATUL NARULA

www.bpbonline.com

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor BPB Online or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

BPB Online has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, BPB Online cannot guarantee the accuracy of this information.

First published: 2023

Published by BPB Online
WeWork
119 Marylebone Road
London NW1 5PU

UK | UAE | INDIA | SINGAPORE

ISBN 978-93-55513-625

www.bpbonline.com

Dedicated to

Our parents.
We have always seen God in them.

About the Author and Co-author

- **Author: Jitender Narula** has 20+ years of cyber security industry experience on the projects of AT&T, Citrix, Google, Boeing, SEDENA Mexico, IPolicy Networks (Tech Mahindra now), Conexant, HFCL, iiCyberSecurity, SKY, Delhi Police, Delhi University and Latin American government agencies. He has published technology articles, research and interviews in the area of cyber security on Security Newspaper (www.securitynewspaper.com), NoticiasSeguridad (noticiasseguridad.com) and contributed to the Vishvas News, which is part of Dainik Jagran (Indian Hindi language daily newspaper). Narula has also published a book on Reverse Engineering with the renowned publication house "BPB publications" with the title "Implementing Reverse Engineering".

  Media Appearance:

  https://www.securitynewspaper.com/2021/05/13/step-by-step-process-of-hacking-atms-using-black-box-atm-jackpotting/

  https://www.vishvasnews.com/english/viral/fact-check-post-claiming-good-morning-messages-can-hack-private-information-is-misleading-cybersecurity-expert-shares-steps-to-protect-your-privacy-online/

  https://www.iicybersecurity.com/intercept-satellite-communications.html

  https://www.securitynewspaper.com/2022/07/26/windows-enables-default-account-lockout-policy-for-rdp-remote-desktop-protocol-to-reduce-ransomware-attacks-based-on-brute-forcing-rdp/

  https://www.securitynewspaper.com/2022/07/04/netherlands-university-paid-e200000-in-bitcoins-to-a-ransomware-gang-now-got-its-money-back-except-now-the-bitcoin-was-worth-e500000/

- **Co-author: Atul Narula** has 16+ years of experience in the implementation of cyber security services and solutions for different companies such as Accenture, Hexaware, iiCyberSecurity, Idemia, Air Canada, Telcel, Unisys, Petronic, Sectur and Mexican and other latin american Government agencies. He is proficient in English and Spanish. He has been awarded YouTube Silver Play Button for cyber security channel NoticiasSeguridad Informatica. He has also published articles, research papers on NoticiasSeguridad (noticiasseguridad.com), Exploit One (www.exploitone.com), Cibertip (www.cibertip.com) and contributed to the Televisa Telemundo News and El Pais news.

Media Appearance:

https://www.telemundo.com/noticias/edicion-noticias-telemundo/ciencia-y-tecnologia/video/este-es-el-alcance-que-podrian-tener-las-fallas-de-seguridad-denunciadas-en-twitter-tmvo10827527

https://www.telemundopr.com/noticias/mexico/bandas-criminales-se-retan-por-mensaje-en-redes-sociales- donde-ya-presumian-excentricidades/1837462/

https://www.telemundo52.com/fotosyvideos/advierten-sobre -posibles-intrusos-que-invaden-clases-virtuales/2108065/

https://www.telemundowashingtondc.com/noticias/local/bandas-criminales-se-retan-por-mensaje-en-redes-sociales-donde- ya-presumian-excentricidades/70509/

https://elpais.com/mexico/2021-06-01/un-grupo-de-hackers-de-orige n-ruso-secuestra-informacion-confidencial-de-la-loteria-nacional.html

https://noticiasseguridad.com/tutoriales/como-robar-de-banca-telefonica-clonando-voces-de-clientes-y-hackeando-reconocimiento-de-voz/

https://www.securitynewspaper.com/2021/06/14/how-to-hack-banks-voice-recognition-system-voice-biometrics-with-deepfake-voice-cloning/

https://www.exploitone.com/cyber-security/100-urls-and-mitre-attck-techniques-that-you-should-block-in-your-firewalls-to-avoid-conti-ransomware/

https://www.cibertip.com/virus/lorenz-ransomware-hackea-la-red-empresarial-a-traves-de-sistemas-telefonicos-voip-asegura-su-servidor-voip/

About the Reviewer

Rafael Beda is a seasoned cyber security leader and professional with more than 15 years of experience in the industry. He is currently a Senior Cybersecurity professional in the Financial Market, and a Professor and Mentor in Defensive, Operations and Security Management. Rafael holds an MBA in Information Security Management and a postgraduate in Offensive Security.

Acknowledgements

First and foremost, praises and thanks to my Dad, Mom and God, for showering blessings throughout my work to complete the book successfully.

I would like to express my deep and sincere gratitude to Atul Narula, for helping in the writing of this book. I am extremely grateful for what he has offered me. I would also like to thank him for his friendship, empathy, and great sense of humor.

I am extremely grateful to my parents (Ramesh Narula and Mohini Narula) for their love, prayers, caring and sacrifices for educating and preparing me for my future. I am very much thankful to my wife and my son for their love, understanding, prayers and continuing support to complete this book. Also, I express my thanks to Dr. Shilpi Sahi, Dr. Eva Andrea & Om Narula for their support and motivating me throughout this process of writing. Once again, I would like to thank my family for putting up with me while I spent many nights on writing. I could have never completed this book without their support.

Finally, I would like to thank the team at BPB Publications for giving me this opportunity to write my second book with them.

— Jitender Narula

Preface

Ransomware has become a major threat to organizations and citizens of any nation. There is a need for experts who can help organizations and national law enforcement agencies in mitigating this risk. To mitigate ransomware risk, internal secrets of ransomware should be known to professionals. This book will help professionals across the globe to get insights of the ransomware working, its architecture and furthermore, with the help of a few examples, it is demonstrated that sometimes a flaw in ransomware design or program can lead to break its functionality. This book is divided into 5 sections. The first section talks about the basic concepts required for further chapters in this book, and covers basics related to ransomware internals, ransomware infection vectors from phishing emails, compromised websites, online advertising, vulnerabilities and many more. The second section walks over the ransomware internal details and how key management is being done by malware writers. The third section talks about the techniques used to perform ransomware analysis on a sample. The fourth section demonstrates how a loophole in ransomware can lead to further break in its functionality. The last section discusses how to respond to ransomware attacks without panicking and steps to be taken in case of a disastrous situation.

Section I: Ransomware Understanding – covers the basic concepts required to understand further chapters in this book, and the basics related to ransomware.

Chapter 1: Warning Signs, Am I Infected? – The Internet has contributed so much in the development of mankind; this was never imagined when computers were born. In those times, when smart geeks were developing good things for mankind, there were some who were involved in developing something to break it. Viruses, Trojans, and Malwares – all these buzz words were trending in the underground world. With time, malwares were weaponized and used as a tool for extortion. In this chapter, we will talk on the basics of ransomware and how hackers are infecting victims worldwide.

Chapter 2: Ransomware Building Blocks – covers details about Ransomware, its internal working and its symptoms. Terms associated with ransomwares such as Bitcoin, Crypto currency, Crypto mining, TOR and other related terms are also explained in this chapter.

Chapter 3: Current Defense in Place – Ransomware is now a major threat in the current cyber security era and it has matured over time and turned into a sophisticated attack against the organizations. There are many proposed solutions in the market to protect organizations user data against ransomware attacks. In this chapter, we will talk about the current solutions in place to protect against Ransomware.

Chapter 4: Ransomware Abuses Cryptography – presents the concepts of cryptography, different types of cryptographic algorithms and how these cryptographic encryption and decryption algorithms are fitting into the current Ransomware architectures.

Chapter 5: Ransomware Key Management – The cores of a Ransomware are its keys, which it uses to encrypt and decrypt user data. It is a prerequisite for a malware writer to implement a strong key management solution in Ransomware. Key management has evolved over time. In this chapter, we will talk about the concept of key management in Ransomware.

Section II: Ransomware Internals – covers the ransomware architectural details and how key management is being done by malware writers.

Chapter 6: Internal Secrets of Ransomware – Cryptographic libraries were introduced to add cryptographic capabilities in the applications or software. There were cryptographic libraries introduced by Microsoft. This chapter focuses on how the Cryptographic libraries are being misused by malware writers to code ransomwares.

Chapter 7: Portable Executable Insides – Critical aspect of cyber security defense involves Ransomware analysis. There are different techniques used by researchers to study Ransomware; most of them include analysis of the Portable executable file. Portable Executable (PE) files are the important file format in the Windows operating system. Thus, this chapter walks the structure of Portable Executable file format in detail.

Chapter 8: Portable Executable Sections – Analyzing imported functions by a portable executable reveals the nature of the file. This chapter focuses primarily on the import fields in Portable Executable. It explains the important concepts related to Import Directory and Import Address Table. Analysis of some Ransomware code demonstrated that the malware writers have replaced clean DLL with malicious DLL to call export functions of malicious DLL. This chapter focuses primarily on the export fields in Portable Executable. It also explains the important concepts related to Export Directory and Export Address Table.

Section III: Ransomware Assessment – gives special attention to the techniques used to perform ransomware assessment on a sample.

Chapter 9: Performing Static Analysis – Analyzing Ransomware without actually running the ransomware is where static analysis plays an important role in malware analysis. It's the primary step towards malware analysis, which gleans many details about the malware, without going over the code. This chapter talks about different techniques used for ransomware static analysis.

Chapter 10: Perform Dynamic Analysis – Sometimes static analysis does not relieve much information about the malware or ransomware. The only option left in that case is to analyze the malware in running state. For running ransomware, a sandbox environment is required. Dynamic analysis chapter walks over the techniques used to analyze the ransomware in running state.

Section IV: Ransomware Forensics – demonstrates how a loophole in ransomware can lead to further break its functionality.

Chapter 11: What's in the Memory – explains the importance of physical memory forensics during ransomware execution. Key management in ransomware is implemented using symmetric and asymmetric algorithms. Sometimes, in order to study the key management, memory forensics of ransomware process memory is required.

Chapter 12: LockCrypt 2.0 Ransomware Analysis – takes a ransomware sample and does a static analysis on the ransomware. In the preceding chapter, we study how key management plays a vital role in ransomware development. However, in this analysis, we will analyze one ransomware sample and do some static & dynamic analysis to find loopholes in the key management process of ransomware.

Chapter 13: Jigsaw Ransomware Analysis – will take another ransomware sample to analyze its internal architecture covering key management and its working. A small mistake by a ransomware developer can bring down the whole mission of underground mafia. In order to break the ransomware, we either need to break its encryption or extract keys. In this chapter, we will see this ransomware case study.

Section V: Ransomware Rescue – discusses how to respond to a ransomware attack without panicking and steps to be taken in case of a disastrous situation.

Chapter 14: Experts Tips to Manage Attacks – Ransomware has evolved over the decade and it has become the easiest way to fulfill the financial urge of the underground mafia. Shift in ransomware terror from desktop users to organization level has paved a way to new opportunities for malware writers. In the earlier chapter, we spoke about ransomware, but what needs to be done when you in your organization or at home are a target of ransomware attack. What steps should be taken to neutralize the situation?

Code Bundle and Coloured Images

Please follow the link to download the
Code Bundle and the ***Coloured Images*** of the book:

https://rebrand.ly/qezb5ry

The code bundle for the book is also hosted on GitHub at **https://github.com/bpbpublications/Breaking-Ransomware**. In case there's an update to the code, it will be updated on the existing GitHub repository.

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Section I: Ransomware Understanding

Section II: Ransomware Internals

Section III: Ransomware Assessment

Section IV: Ransomware Forensics

Section V: Ransomware Rescue

Section I: Ransomware Understanding

CHAPTER 1
Warning Signs, Am I Infected?

Introduction

Oh My God! Wired icon and different names.

I am not able to access my files. All my files are coming up with weird icons.

Why am I unable to open my important files?

This happens when you are hit by a ransomware. But what is this ransomware? It begins with the invention of computer virus or malware (new-age term for a family of viruses). Previously, computer viruses were built to disrupt another person's use of an application or system to take revenge, or just for fun. If we take a peek into the past, there are many versions of viruses or worms, like Morris Worm, ILOVEYOU, SQL Slammer, Stuxnet, and Blaster. All of these were developed to disrupt internet users, companies' or countries' computer networks or infrastructure.

With the advancement in software technologies, malware writers gradually realized that malware can be used to earn big bucks. With this, a new variant of malwares came forth, which the internet called ransomware. It is not only a malware but a real pain today for every individual and organization in the world.

Let's look at a simple example. Earlier, banks were robbed physically in a planned manner, but in today's age, banks are forced to send money to robbers over the wire because of ransomware attacks. A small file of few KBs can disrupt entire organizations, and the people behind the attack can earn millions of dollars in ransom. In this chapter, we will learn about the different types of ransomware and understand how we can protect ourselves from them.

Structure

In this chapter, we will discuss the following topics:

- Symptoms
- Proactive steps
- Immediate actions
  - o Checking the scope of infection
  - o Check which ransomware infected you
  - o Plan for response

Objectives

The objective of this chapter is to make the user aware of the ransomware attack. The first and foremost point for the user is to stay calm and not panic. In this chapter, we will talk about the proactive steps to be taken in case you are hit by a ransomware attack. There are cases when a user wants to ensure that the attack on their computer is in fact a ransomware attack. So,we will talk about the symptoms of a ransomware attack, followed by immediate remedial actions that can be taken. After taking remedial actions, we will talk about the scope of infection, along with the steps required to identify the variant of ransomware. Toward the end of this chapter, we will talk about the next plan of action to eradicate the ransomware variant from your computer.

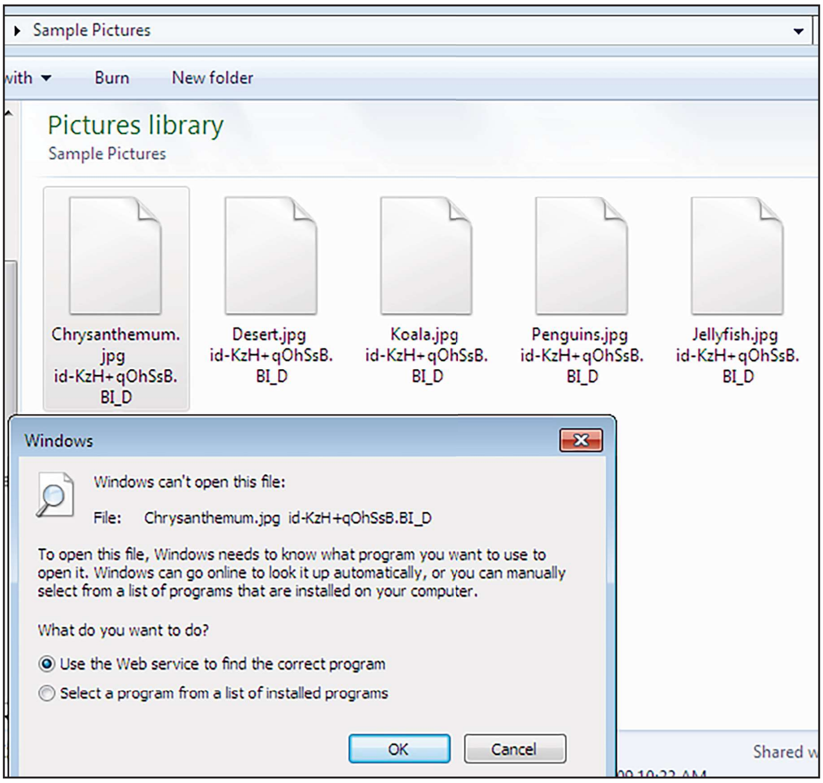
Proactive steps

If you find yourself facing this problem, what is the first step you should take to get yourself out of it? This is what we are going to discuss in this section. If you or your organization are hit by a ransomware, and you are not sure about the problem you are in, then look out for these symptoms to check if it really is a ransomware infection. In this section, we will first talk about the symptoms of a ransomware attack and then walk through the immediate action plan to prevent further infection in the network. Let’s look at a few symptoms of ransomware infection.

Symptoms

If you are facing any of the following issues, then you are infected with ransomware:

- Clicking on any file leads to something like what is shown in *Figure 1.1*:



Sample Pictures
with
Burn
New folder
Pictures library
Sample Pictures
Chrysanthemum.jpg id-KzH+qOhSsB.BI_D
Desert.jpg id-KzH+qOhSsB.BI_D
Koala.jpg id-KzH+qOhSsB.BI_D
Penguins.jpg id-KzH+qOhSsB.BI_D
Jellyfish.jpg id-KzH+qOhSsB.BI_D
Windows
OK
Cancel
Shared w

Windows can't open this file:

File: Chrysanthemum.jpg id-KzH+qOhSsB.BI_D

To open this file, Windows needs to know what program you want to use to open it. Windows can go online to look it up automatically, or you can manually select from a list of programs that are installed on your computer.

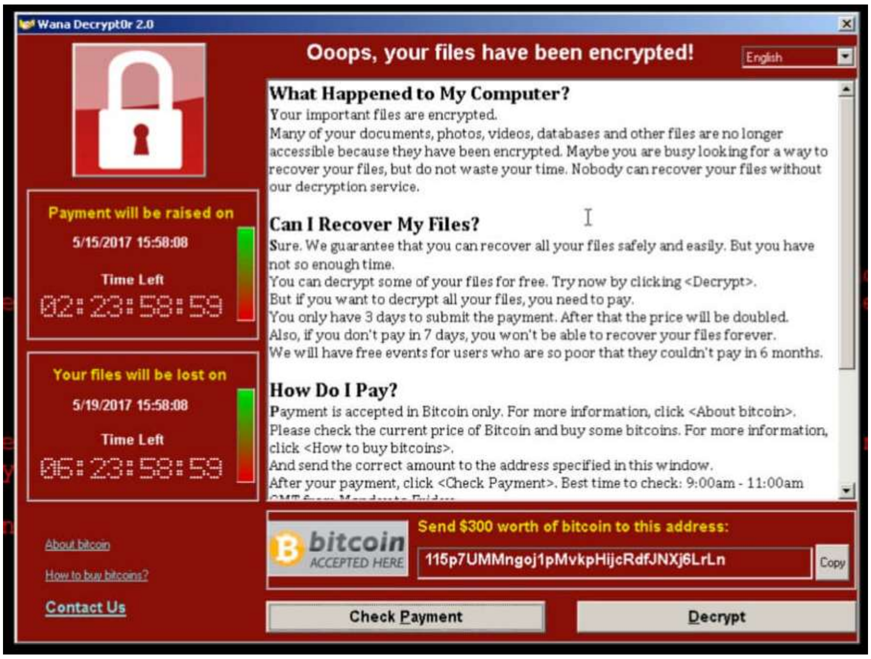
What do you want to do?

● Use the Web service to find the correct program

○ Select a program from a list of installed programs

***Figure 1.1**: Windows cannot open file*

- Some ransomware window pops up on the screen, and you cannot close the window.
- You get an alarming message on the screen to pay ransomware, and that all your all files will be deleted if not paid.
- You get something like a counter, as shown in *Figure 1.2*:



What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

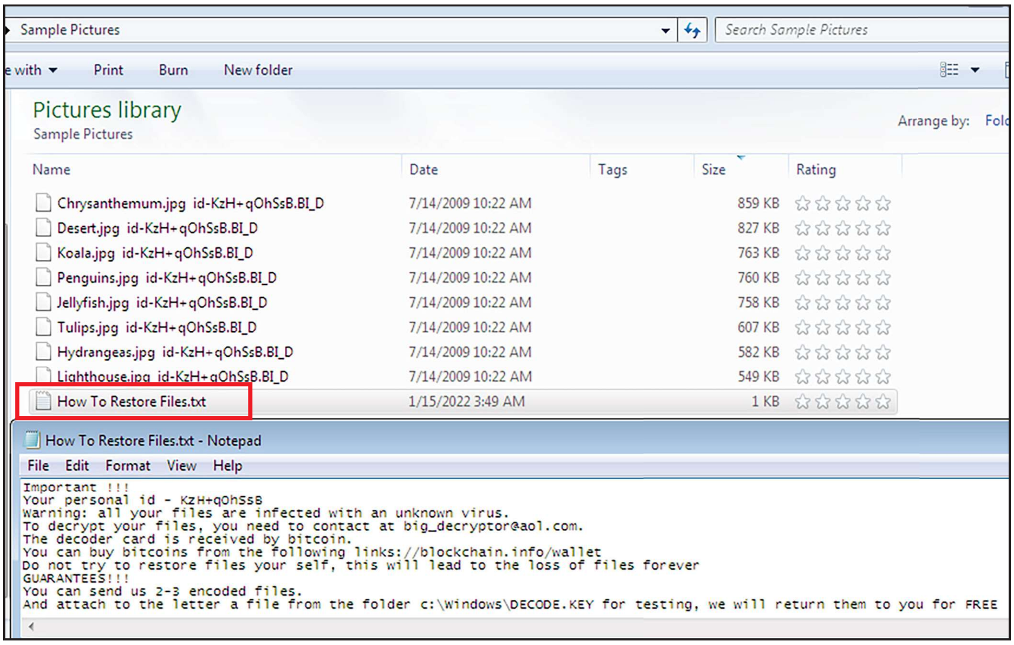
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Figure 1.2: *Ransomware screen*

- All your files in a folder are not readable, and you see a file in the same folder named "`How To Restore Files.txt`", as shown in *Figure 1.3*:



Name	Date	Tags	Size	Rating
Chrysanthemum.jpg id-KzH+qOhSsB.BI_D	7/14/2009 10:22 AM		859 KB	☆☆☆☆☆
Desert.jpg id-KzH+qOhSsB.BI_D	7/14/2009 10:22 AM		827 KB	☆☆☆☆☆
Koala.jpg id-KzH+qOhSsB.BI_D	7/14/2009 10:22 AM		763 KB	☆☆☆☆☆
Penguins.jpg id-KzH+qOhSsB.BI_D	7/14/2009 10:22 AM		760 KB	☆☆☆☆☆
Jellyfish.jpg id-KzH+qOhSsB.BI_D	7/14/2009 10:22 AM		758 KB	☆☆☆☆☆
Tulips.jpg id-KzH+qOhSsB.BI_D	7/14/2009 10:22 AM		607 KB	☆☆☆☆☆
Hydrangeas.jpg id-KzH+qOhSsB.BI_D	7/14/2009 10:22 AM		582 KB	☆☆☆☆☆
Lighthouse.jpg id-KzH+qOhSsB.BI_D	7/14/2009 10:22 AM		549 KB	☆☆☆☆☆
How To Restore Files.txt	1/15/2022 3:49 AM		1 KB	☆☆☆☆☆

```
Important !!!
Your personal id - KzH+qOhSsB
Warning: all your files are infected with an unknown virus.
To decrypt your files, you need to contact at big_decryptor@aol.com.
The decoder card is received by bitcoin.
You can buy bitcoins from the following links://blockchain.info/wallet
Do not try to restore files your self, this will lead to the loss of files forever
GUARANTEES!!!
You can send us 2-3 encoded files.
And attach to the letter a file from the folder c:\Windows\DECODE.KEY for testing, we will return them to you for FREE
```

Figure 1.3: *How to restore files*

All the mentioned situations are indicators of ransomware infections in your computer.

Immediate actions

Infected! What should I do immediately?

If you find that your personal or organization computer is showing any of the symptoms mentioned in the previous section, you have been hit by a ransomware. Following are some immediate remedial actions.

Disconnect the infected computer

The first step you should take is to immediately disconnect the computer from the network. If the computer is connected to the Ethernet network, then unplug the network cable. If you are connected to a wireless network, switch off the computer wireless interface.

Once you are disconnected from the network, unplug any storage device (external hard drive or USB) connected the computer. Do not delete any file from the computer. Additionally, don't change the name of any file, as this can harm a posterior tentative to recover the original file

Check the scope of infection

Once you have completely disconnected from the network, you will have to check the amount of damage caused. The damage can be partial or complete on important data. It can probably include devices connected to your computers like external hard disk drives or USB dives. To check the scope of infection caused due to a ransomware attack, we will check all devices in a step-by-step manner:

- First, check your infected computer. Dive into the computer drives and check whether the data in the drives is infected. If you have multiple drives, it might be possible that only your primary drive is infected.
- If you have any network drive mapped on the computer, check the data in those mapped computer drives.
- Check the data in the USB if it was connected to your computer.
- Check the data in the external disk drive if it was connected your computer.
- If your computer data is in sync with any of the cloud-based storage (like Google drive, Dropbox, Microsoft OneDrive), check the corresponding cloud storage data for any type of encryption.

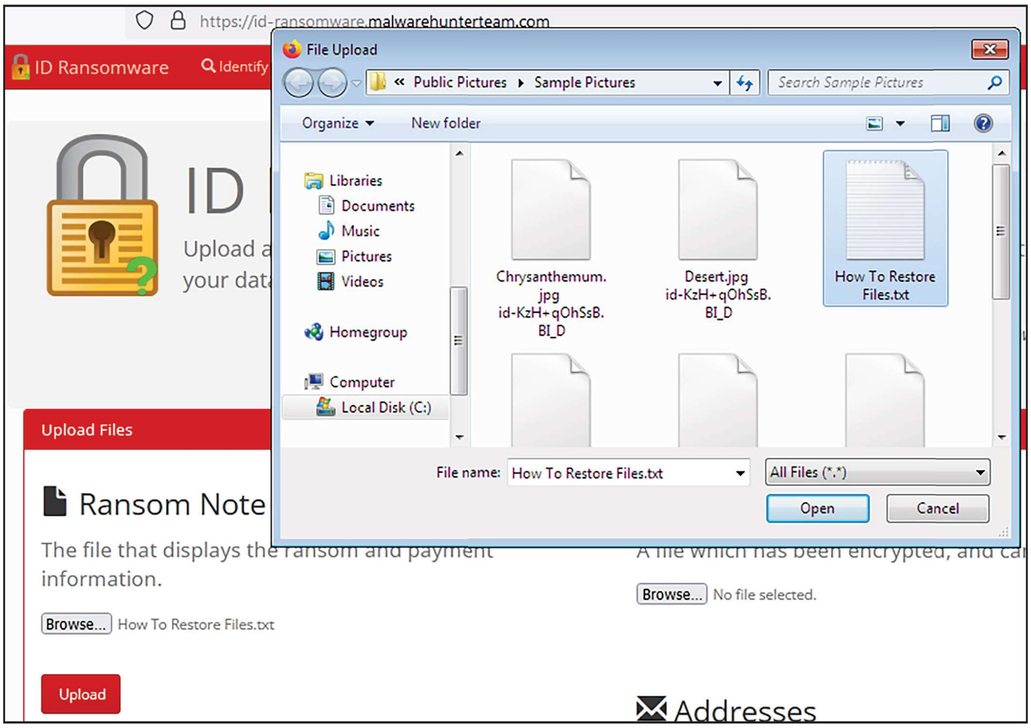
In the case of infection, our focus is to check the signs of encryption in our system. This will help us in planning further actions.

Check which ransomware infected you

Once we are able to evaluate and confirm the signs of encryptions and the damage caused, it is important to find the type of ransomware we are dealing with. This can be done by analyzing the patterns of infection on files by further doing some research on the internet to get the exact version of the ransomware. What this means is that the name of ransomware can be identified by the file extension of the encrypted files. There is an easy way out to know the exact strain of ransomware: upload the ransomware note or the sample of encrypted file on the following website:

https://id-ransomware.malwarehunterteam.com/

As you can see in *Figure 1.4*, we uploaded the ransomware note named "`How to restore Files.txt`" on the ID Ransomware website to know the exact strain of ransomware.



https://id-ransomware.malwarehunterteam.com

File name: How To Restore Files.txt

All Files (*.*)

Ransom Note

The file that displays the ransom and payment information.

Browse... How To Restore Files.txt

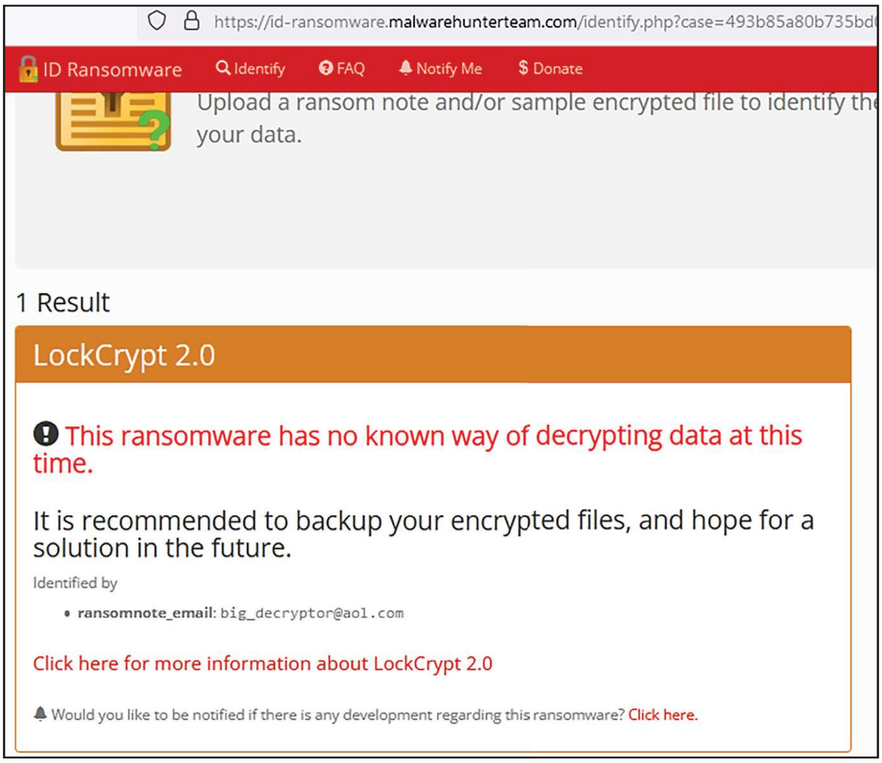
A file which has been encrypted, and ca

Browse... No file selected.

Figure 1.4: ID Ransomware

On uploading the ransomware note, we got what is shown in *Figure 1.5*. In case you are unable to identify the ransomware variant, search for the file extension that the ransomware appended to the files on the internet. You can get some clue about the ransomware variant.

As we can see in *Figure 1.5*, the ransomware identified is **LockCrypt 2.0**:



https://id-ransomware.malwarehunterteam.com/identify.php?case=493b85a80b735bd
ID Ransomware
Identify
FAQ
Notify Me
$ Donate

Upload a ransom note and/or sample encrypted file to identify th
your data.

1 Result

LockCrypt 2.0

This ransomware has no known way of decrypting data at this time.

It is recommended to backup your encrypted files, and hope for a solution in the future.

Identified by

- **ransomnote_email:** `big_decryptor@aol.com`

Click here for more information about LockCrypt 2.0

Would you like to be notified if there is any development regarding this ransomware? Click here.

***Figure 1.5**: Ransomware Identified*

In our case, we identified that the ransomware is of type **LockCrypt**, which uses AES256 for symmetric encryption and RSA-2048 for asymmetric encryption. We will talk about symmetric and asymmetric encryption in *Chapter 4, Ransomware Abuses Cryptography*.

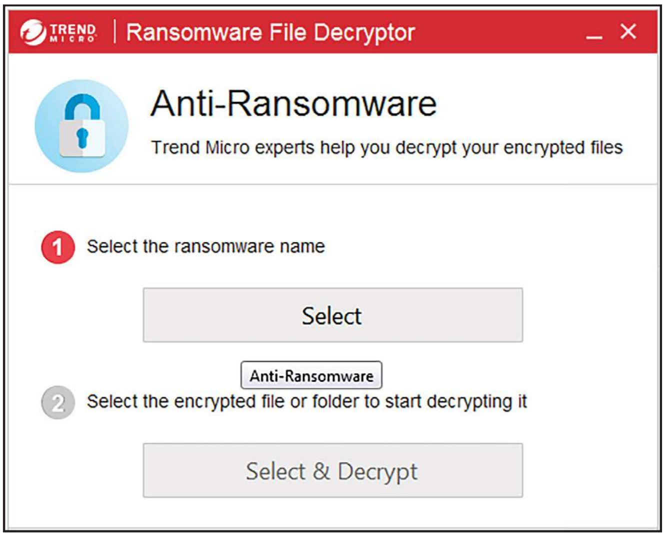
Plan for response

Now that we have identified the ransomware strain, it is time to get everything back to normal. Based on the ransomware variant,we will have to check on the internet for any decryptor for that ransomware. Ransomware decryptor is a tiny software or application that will help you to recover all your encrypted files. But before we get on to finding a decryptor, we will have to plan our course of action as listed here:

1. Check your data backup to restore data from the latest backup:
   a. In this step, we should find all the possible sources where we have backed up our data. This will help us minimize the damage caused to us, because at this point, we are unsure whether we will be able to remove ransomware to decrypt our data/files.
   b. Don't plug your backup into the alleged infected machine, as depending on the ransomware type, it can encrypt any other type of media (external HDD for example).

      Most modern ransomware are programmed to delete the windows shadow files. Shadow files are nothing but the windows restore points. If you are lucky, then your shadow files are untouched by ransomware.
   c. If you have the latest data backup, then you are good to go; recover all your data from the backup. Once your data is restored, you can run multiple scans to remove the ransomware if possible.
2. Find your ransomware decryptor on the internet to decrypt the encrypted files.
   a. Once you know the ransomware variant, there are a couple of antivirus companies that offer free decryptor for ransomware.
      i. Trend Micro Ransomware File Decryptor

      Figure 1.6 shows the Trend Micro Ransomware Decryptor interface:



Trend Micro experts help you decrypt your encrypted files

1 Select the ransomware name

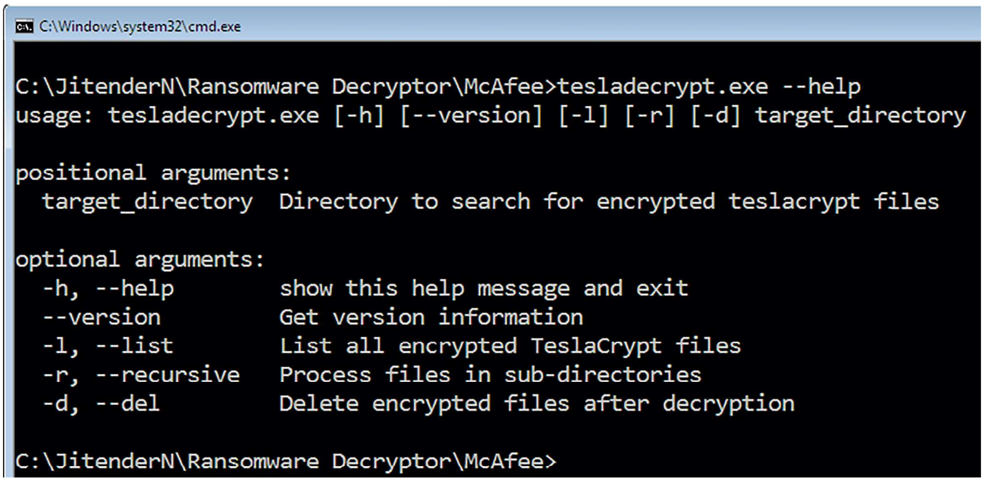
2 Select the encrypted file or folder to start decrypting it

***Figure 1.6**: Trend Micro Ransomware Decryptor*

To use this ransomware decryptor, you have to select the ransomware from the `Select the ransomware name` list and then select the files or folders you want to decrypt. Trend micro ransomware decryptor can decrypt files encrypted with TeslaCrypt V1/V2/V3/V4, CryptXXX V1/V2/V3/V4/V5, XORBAT, CERBER V1, Stampado, SNSLocker, AutoLocky, BadBlock, 777, XORIST, Nemucod and Chimera.

ii. McAfee

Figure 1.7 shows the McAfee Ransomware Decryptor:

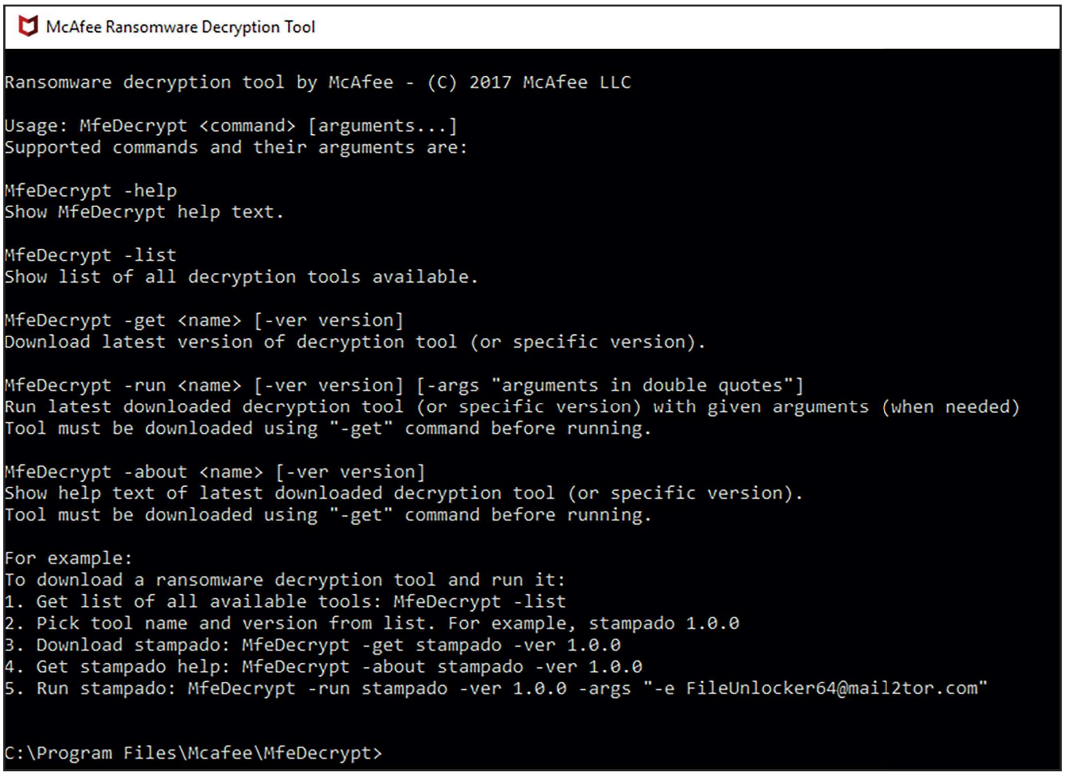


```
C:\JitenderN\Ransomware Decryptor\McAfee>tesladecrypt.exe --help
usage: tesladecrypt.exe [-h] [--version] [-l] [-r] [-d] target_directory

positional arguments:
  target_directory  Directory to search for encrypted teslacrypt files

optional arguments:
  -h, --help        show this help message and exit
  --version         Get version information
  -l, --list        List all encrypted TeslaCrypt files
  -r, --recursive   Process files in sub-directories
  -d, --del         Delete encrypted files after decryption

C:\JitenderN\Ransomware Decryptor\McAfee>
```

Figure 1.7*: McAfee Ransomware Decryptor*

This tool by McAfee is a decryptor for Tesladecrypt ransomware. Along with this decryptor, McAfee provides other decryption tools for Shade and WildFire ransomware. In this command-line tool, the user will have to provide the directory to search for the encrypted Teslacrypt files. However, this can be quite tedious for a normal user.

McAfee also provides a framework called **McAfee Ransomware Recover** (**Mr2**), which is also a command-line tool, but with a bunch of ransomware support, to download decryptor for them. This tool is shown in *Figure 1.8*:



```
Ransomware decryption tool by McAfee - (C) 2017 McAfee LLC

Usage: MfeDecrypt <command> [arguments...]
Supported commands and their arguments are:

MfeDecrypt -help
Show MfeDecrypt help text.

MfeDecrypt -list
Show list of all decryption tools available.

MfeDecrypt -get <name> [-ver version]
Download latest version of decryption tool (or specific version).

MfeDecrypt -run <name> [-ver version] [-args "arguments in double quotes"]
Run latest downloaded decryption tool (or specific version) with given arguments (when needed)
Tool must be downloaded using "-get" command before running.

MfeDecrypt -about <name> [-ver version]
Show help text of latest downloaded decryption tool (or specific version).
Tool must be downloaded using "-get" command before running.

For example:
To download a ransomware decryption tool and run it:
1. Get list of all available tools: MfeDecrypt -list
2. Pick tool name and version from list. For example, stampado 1.0.0
3. Download stampado: MfeDecrypt -get stampado -ver 1.0.0
4. Get stampado help: MfeDecrypt -about stampado -ver 1.0.0
5. Run stampado: MfeDecrypt -run stampado -ver 1.0.0 -args "-e FileUnlocker64@mail2tor.com"


C:\Program Files\Mcafee\MfeDecrypt>
```

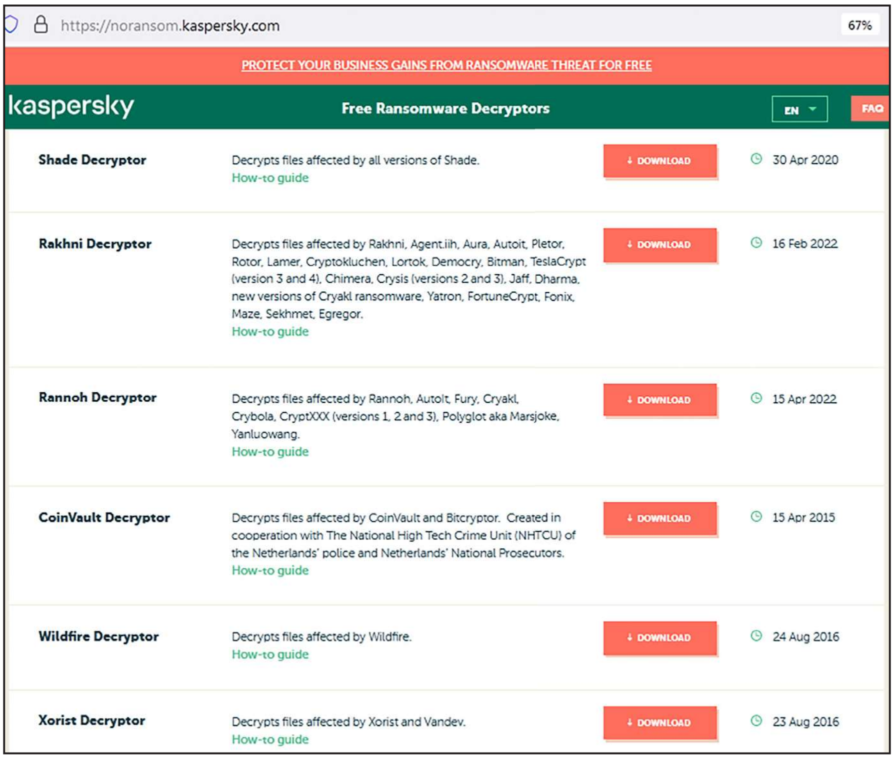
***Figure 1.8**: McAfee Ransomware Recovery*

The framework is regularly updated by McAfee as the decryption logic and keys required to decrypt files become available.

iii. **Kaspersky ransomware decryptor**

When you search for Kaspersky ransomware decryptor, you will be redirected to the https://noransom.kaspersky.com/ website, where you can see a list of ransomware decryptors available.

Figure 1.9 shows the Kaspersky Ransomware Decryptor interface:

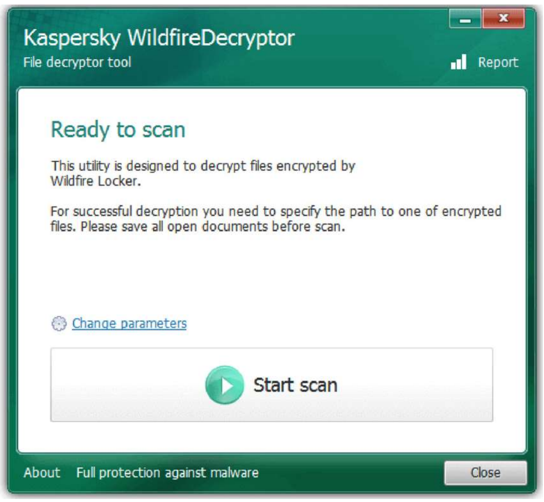

https://noransom.kaspersky.com
67%
PROTECT YOUR BUSINESS GAINS FROM RANSOMWARE THREAT FOR FREE
kaspersky
EN
FAQ

Free Ransomware Decryptors

Shade Decryptor	Decrypts files affected by all versions of Shade. How-to guide	↓ DOWNLOAD	30 Apr 2020
Rakhni Decryptor	Decrypts files affected by Rakhni, Agent.iih, Aura, Autoit, Pletor, Rotor, Lamer, Cryptokluchen, Lortok, Democry, Bitman, TeslaCrypt (version 3 and 4), Chimera, Crysis (versions 2 and 3), Jaff, Dharma, new versions of Cryakl ransomware, Yatron, FortuneCrypt, Fonix, Maze, Sekhmet, Egregor. How-to guide	↓ DOWNLOAD	16 Feb 2022
Rannoh Decryptor	Decrypts files affected by Rannoh, AutoIt, Fury, Cryakl, Crybola, CryptXXX (versions 1, 2 and 3), Polyglot aka Marsjoke, Yanluowang. How-to guide	↓ DOWNLOAD	15 Apr 2022
CoinVault Decryptor	Decrypts files affected by CoinVault and Bitcryptor. Created in cooperation with The National High Tech Crime Unit (NHTCU) of the Netherlands' police and Netherlands' National Prosecutors. How-to guide	↓ DOWNLOAD	15 Apr 2015
Wildfire Decryptor	Decrypts files affected by Wildfire. How-to guide	↓ DOWNLOAD	24 Aug 2016
Xorist Decryptor	Decrypts files affected by Xorist and Vandev. How-to guide	↓ DOWNLOAD	23 Aug 2016

***Figure 1.9**: Kaspersky Ransomware Decryptors*

These tools are easy to use as users only have to download the decryptor of the particular ransomware and click on **`Start scan`** in the Wildfire decryptor. This is illustrated in *Figure 1.10*:



Kaspersky WildfireDecryptor

File decryptor tool

Ready to scan

This utility is designed to decrypt files encrypted by Wildfire Locker.

For successful decryption you need to specify the path to one of encrypted files. Please save all open documents before scan.

***Figure 1.10**: Kaspersky Wildfire Decryptor*