ARL-SR-0447 • MAY 2021

Hands-on Cybersecurity Studies: Hidden Tear Ransomware

by Jaime C Acosta, Jennifer A Sims, Elizabeth Rubio, Ivanna Becerra, and Christopher Uriel

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

ARL-SR-0447 ● MAY 2021

Hands-on Cybersecurity Studies: Hidden Tear Ransomware

Jaime C Acosta
Computational and Information Sciences Directorate,
DEVCOM Army Research Laboratory

Jennifer A Sims, Elizabeth Rubio, Ivanna Becerra, and Christopher Uriel
University of Texas at El Paso

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
May 2021	Special Report	January 2021–May 2021

4. TITLE AND SUBTITLE
Hands-on Cybersecurity Studies: Hidden Tear Ransomware

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Jaime C Acosta, Jennifer A Sims, Elizabeth Rubio, Ivanna Becerra, and Christopher Uriel

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
DEVCOM Army Research Laboratory
ATTN: FCDD-RLC-ND
Adelphi, MD 20783-1138

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-SR-0447

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES
ORCID ID(s): Jaime C Acosta, 0000-0003-2555-9989

14. ABSTRACT
Ransomware incidents are becoming more common and more costly. This malware causes systems to become inaccessible by locking out access to user files using encryption. The Hidden Tear ransomware source code was released for educational purposes in August 2015, leading to further analyses and a better understanding of how this malware and related virtual threats work. In this report, we describe a hands-on cybersecurity exercise where participants run the Hidden Tear malware and observe its behavior using several tools and techniques. After completing the exercise, participants will have a high-level understanding of the inner workings of this malware, including infection logic, decryption information storage, and network activity.

15. SUBJECT TERMS
security awareness, web application security, security remediation, hands-on cybersecurity, Collaborative Innovation Testbed

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Jaime C Acosta
Unclassified	Unclassified	Unclassified	UU	22	19b. TELEPHONE NUMBER (Include area code) (915) 747-8012

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Contents

List of Figures iv

1. Introduction 1

1.1 Ransomware Distribution 1

1.2 Effects of Ransomware 2

2. Setup and Configuration 2

3. Learning Objectives 3

4. Exercise 4

4.1 Activity 1: Hidden Tear Source Code Analysis 4

4.2 Activity 2: Decryptor Source Code Analysis 6

4.3 Activity 3: Server Familiarization 6

4.4 Activity 4: Initiate Wireshark capture 8

4.5 Activity 5: Ransomware Live Analysis 9

5. Conclusion 12

6. References 13

List of Symbols, Abbreviations, and Acronyms 15

Distribution List 16

List of Figures

Fig. 1 Navigate to the Hidden Tear source 5
Fig. 2 Switching to code view 5
Fig. 3 Navigate to the decryptor source 6
Fig. 4 Location of terminal icon 6
Fig. 5 IP address location 7
Fig. 6 HTML directory listing 7
Fig. 7 Contents of keys.php 8
Fig. 8 Wireshark icon in Kali Linux 8
Fig. 9 Start capture button in Wireshark 9
Fig. 10 Test folder on desktop 9
Fig. 11 Files in the test folder 9
Fig. 12 Hidden Tear icon 10
Fig. 13 Encrypted files with new extension 10
Fig. 14 Ransom message 10
Fig. 15 Wireshark stop capturing button 10
Fig. 16 Ransomware decryption information captured on web server 11
Fig. 17 Ransomware decryption information captured in network packet 11
Fig. 18 Hidden Tear decryptor icon 11
Fig. 19 Files decrypted dialog 11

1. Introduction

Due to the vast amounts of knowledge, content, and connectedness that exist because of the Internet, many organizations now rely on its access for daily tasks. Adversaries have seen this ecosystem as a trove of opportunity and are actively taking advantage of any weaknesses that may reside on connected systems. For this reason, cybersecurity is critical for both service providers and service consumers. While there are numerous efforts in the field of cyber defense, security can never be guaranteed due to the complexities in the technologies, human factors, and the ever-changing nature of the domain.

A particular mechanism that adversaries are increasingly using for monetary gain is ransomware. This malware restricts access to files on a user's system by encrypting them and subsequently providing decryption information in exchange for something with monetary value—usually cryptocurrency or gift cards.

This report describes some of the steps an individual can follow to become more aware of ransomware and its impacts. It will also provide a better understanding of how to protect against ransomware using various tools. More specifically, the exercise actively (using a hands-on approach) familiarizes participants with the mechanics of a particular ransomware sample—how it encrypts and decrypts files, how to capture and analyze network traffic generated by the malware, and how to use scripts to extrapolate detailed information related to the malware.

1.1 Ransomware Distribution

The first known ransomware attack occurred in 1989. It was distributed using floppy disks with hidden files that even privileged users could not view. The ransomware would activate after the victim's computer was started 90 times.[1] Modern adversaries take advantage of the Internet for distribution, using email spam, vulnerabilities in connected systems, and even spoofed websites and browser pop-up windows, among many others.[2] Targeted platforms are not limited to server machines and desktops; mobile and Internet of Things (IoT) devices such as smart phones, medical devices, and IoT are also victims.[3] Attacks have increased in numbers and adversaries now focus more on large networked systems such as hospitals, leveraging human, process, and system weaknesses.[4]

1.2 Effects of Ransomware

Ransomware damage varies, affecting individual users to large corporations. Large corporations are often forced to limit or discontinue services due to attacks. Monetary demands are rising with ransomware; as of the end of 2020, the global loss has been estimated to be about $1 trillion.[5] At the time of this writing, an incident caused the biggest pipeline in the United States, managed by Colonial Pipeline, to be shut down by a series of ransomware attacks. This ransomware locked the machines until the demands were paid. Due to this shutdown, fuel supply was affected in many geographic areas.[6]

2. Setup and Configuration

The exercise presented in this report was set up to allow basic interaction between a server and a client machine. The server will store the ransomware decryption information while the ransomware is encrypting files on the client. The following technologies are used in the setup:

- Windows 10[7] (Version 20H2, 10.0.19042.0)
- Flare VM (virtual machine)[8]
- VirtualBox[9] (Version 6.1)
- Kali 2021.1 64-bit VM[10]
- Apache2 Web Server[4] (Version 2.4.46)
- Hidden Tear Open-Source Ransomware Trojan[11]
- Wireshark[12] (Version 3.4.0)

The Kali VM is the server machine and the Flare VM is the client machine. Both VMs are connected to a VirtualBox internal network that isolates communication between them. Windows Defender and Windows Tamper Protection are disabled, otherwise Hidden Tear will almost immediately be removed from the system. The Hidden Tear ransomware source code and all the components required for compilation are preloaded onto the Flare VM.

The web server contains a Hypertext Preprocessor (PHP) script that retrieves the data from a URL parameter and stores the information in a text file. The web service needs to be started prior to running the scenario. The entire scenario is hosted on the US Army Combat Capabilities Development Command (DEVCOM) Army

Research Laboratory (ARL) South Collaborative Innovation Testbed and made accessible to participants through a web browser.

3. Learning Objectives

The purpose of the exercise included in the next section is to launch a ransomware sample and then capture its network traffic in an isolated environment. The source code to Hidden Tear is provided on the VM to allow participants to navigate through and investigate its inner workings. The following are the general cybersecurity topics emphasized in the exercise:

- Ransomware Awareness: Malicious actors target victims through email, websites, and other seemingly trustworthy means. Therefore, it is important that users understand the potential vectors of attack and impacts. Malicious software, when executed, encrypts files in the target's computer. These files can be encrypted with very complex algorithms, and in some cases, recovery is impossible.[13] Hidden Tear, as used in this exercise, uses the well-known Advanced Encryption Standard (AES) algorithm to encrypt files.
- Vulnerabilities: Adversaries continually augment their tactics, targeting users, processes, and system weaknesses. Publicly available vulnerability and exploit databases provide mechanisms to test that systems are updated; however, they may also be used to infiltrate systems running unpatched and out-of-date software. Additionally, information security training can help users identify and report suspicious activity, such as malicious emails, and help reduce vulnerabilities.
- Sandboxes: An isolated environment that allows the execution of malware without harming the whole device.[14] Sandboxes are often used in cybersecurity as a way to execute code that could otherwise harm the host computer. They can be built in a VM and are used to collect vital information associated with malware, its impacts, and associated remediation.

Participants will learn to use the following technologies and tools while analyzing the ransomware:

- C Sharp Programming Language: Basic understanding of C Sharp syntax and how it can be used to encrypt and decrypt data, communicate to a server, and create a file. Participants will review the Hidden Tear source code and take notes on key points that make up the ransomware functionality.

- PHP Programming Language: Basic understanding of PHP syntax and how it is used to interact with a client and store the data that is being transmitted over the wire. Participants will review the PHP script saved on the server.
- Wireshark Network Sniffer: Basic understanding of Wireshark and how it is used to capture and dissect network traffic. Participants will initiate a Wireshark capture and learn how to identify salient information stored in packets.
- Kali Linux Operating System: Basic understanding of Kali Linux and its basic system administration utilities, including network interface configuration.

4. Exercise

The following exercise is presented to participants in a step-by-step fashion. All of the data and systems in the exercise are fictional and exist on isolated VMs using isolated networks.

4.1 Activity 1: Hidden Tear Source Code Analysis

Your team has found the source code of a ransomware called Hidden Tear. Your job is to extract as much information as possible from the source code. This will be done by running the ransomware and obtaining the decryption information in a sandbox environment. The following steps will guide you through the encryption and retrieval of your corrupted files. Learn as much as possible before the ransomware is launched.

Familiarize yourself with the malware's source to understand what it does and how you can defend against it:

1) Open the Hidden Tear folder on your FlareVM* desktop.
2) Navigate through the file directories to the ransomware source code as shown in Fig. 1.

Hidden-tear -> hidden-tear -> hidden-tear.sln

* FlareVM is a fully customizable, Windows-based security distribution for malware analysis, incident response, penetration testing, and so on. FlareVM is developed and maintained by FireEye.[15]

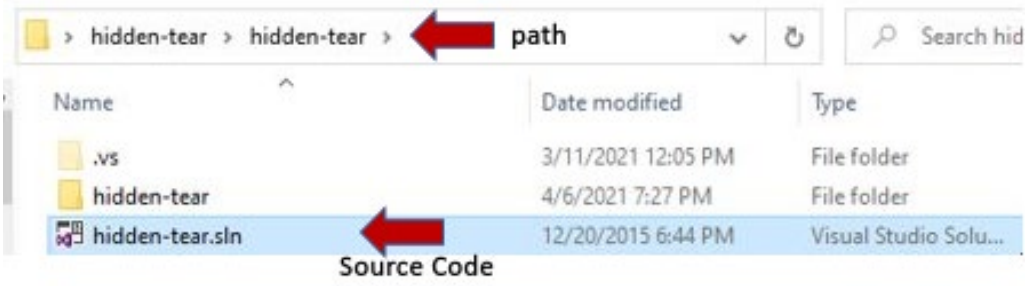

Fig. 1 Navigate to the Hidden Tear source

3) Double-click on the ***hidden-tear.sln*** file; this will start up Visual Code Studio, which may take a while to load.

4) Once Visual Code Studio has opened, right-click on ***Form1.cs*** and select ***View Code*** as shown in Fig. 2.

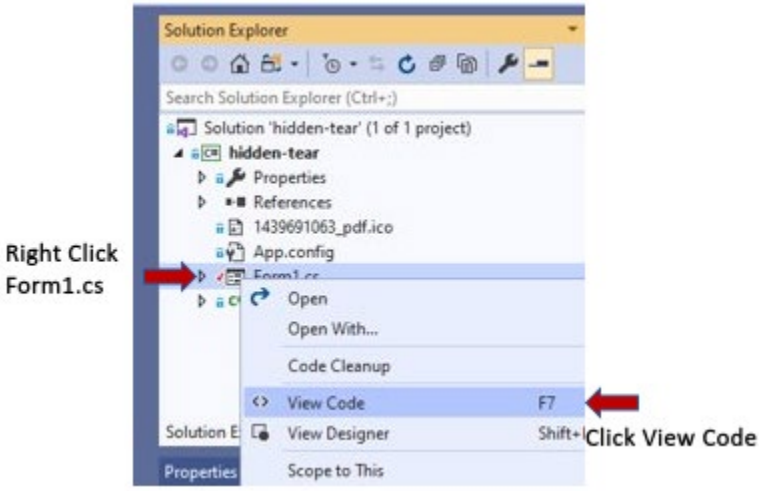

Fig. 2 Switching to code view

5) Review the source code and answer the following questions:

   a. What is the target URL?

   b. What folder gets encrypted?

   c. What is the name of the extension of the encrypted files?

   d. What encryption algorithm is used to encrypt all the data?

   e. What is the message that will be displayed to the victim?

   f. What types of files are encrypted in the folder?

4.2 Activity 2: Decryptor Source Code Analysis

Learn about the decryptor to understand what is involved in retrieving your files.

6) Navigate to your decryptor program (Fig. 3).

   hidden-tear -> hidden-tear-decryptor -> hidden-tear-decryptor.sln

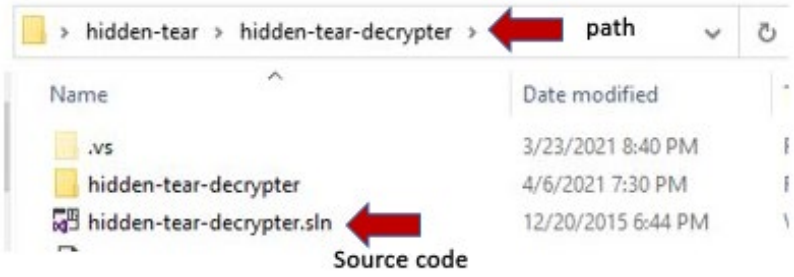

Fig. 3 Navigate to the decryptor source

7) Open the ***hidden-tear-decrypter.sln*** file by double-clicking it.

8) Review the source code.

   a. What is the folder path that will be decrypted?

   b. What is the file extension name that will be decrypted?

4.3 Activity 3: Server Familiarization

Familiarize yourself with the server's files that have already been set up.

9) Open your Kali* VM and open a terminal. This can be done by selecting the terminal icon on the taskbar near the dragon as shown in Fig. 4.

Fig. 4 Location of terminal icon

* Kali Linux is a Debian-derived Linux distribution for digital forensics and penetration testing. It is maintained and funded by Offensive Security.

10) Find the IP address of your Kali VM by typing the command ***ifconfig*** into the terminal and pressing Enter. Figure 5 shows the location of your IP address in the output.

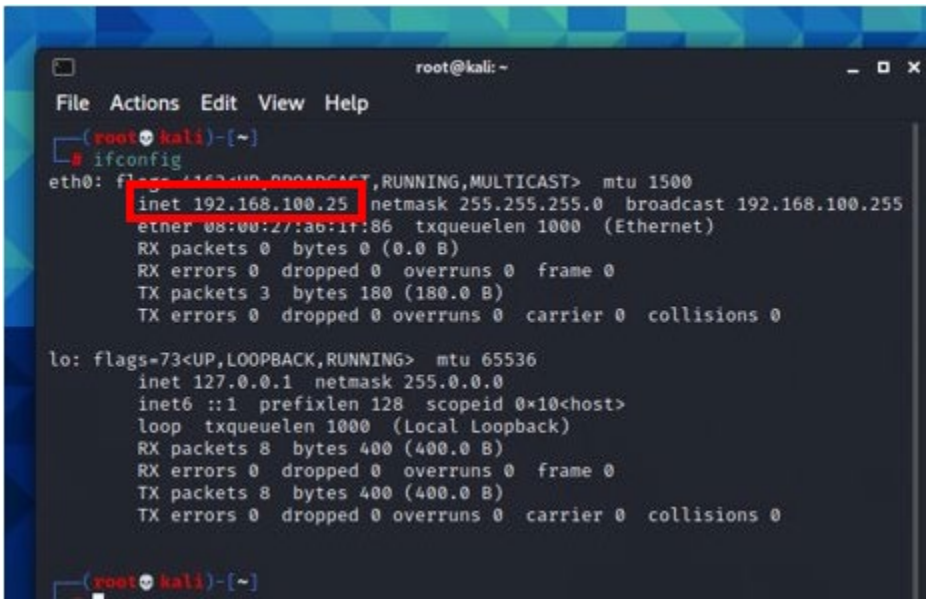

Fig. 5 IP address location

11) What is the IP address on the Kali VM?

12) Is this the same IP you found in your target URL in your source code?

13) Change the directory to */var/www/html* with the ***cd*** command. On Debian-based systems, this is the root folder for web servers.

cd /var/www/html

14) List the contents of this directory by running the following command:

ls

The results should resemble Fig. 6.

Fig. 6 HTML directory listing

15) Notice that there is a keys.php file in the directory. To see what is inside this file, type the following command:

cat keys.php

The output is shown in Fig. 7. This script will get the data from the ***info*** parameter in a Web GET request and write it to the data.txt file.

```
└─# cat keys.php
<?php
    $info = $_GET['info'];
    $file = fopen("data.txt", "a");
    fwrite($file, $info."". PHP_EOL);
    fclose($file);
?>
```

Fig. 7 Contents of keys.php

16) Check again to see the contents of this directory. Run the ***ls*** command again.

17) Check to ensure the data.txt file is empty by running the following command:

    cat data.txt

18) Now start the Apache service:

    service apache2 start

4.4 Activity 4: Initiate Wireshark capture

In order to analyze the network traffic generated by Hidden Tear, we need to start collecting using Wireshark*.

19) Go back to your Flare VM and start a Wireshark capture. Search for the name of the app in the search bar (Fig. 8).

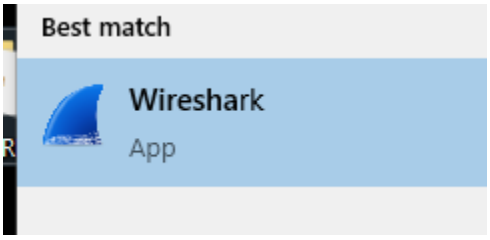

Fig. 8 Wireshark icon in Kali Linux

20) Start capturing traffic by clicking on the dorsal fin on the top left (shown in Fig. 9).

* Wireshark is a free, open-source packet analyzer. This tool can be used for network troubleshooting, analysis, software and communications protocol development, and education. Our primary use for this tool is to analyze the network traffic generated by the ransomware.

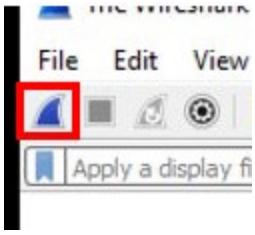

Fig. 9 Start capture button in Wireshark

4.5 Activity 5: Ransomware Live Analysis

Now you will launch the ransomware in the isolated sandbox environment. From your analysis of the source code for Hidden Tear, you know that it encrypts the folder contents of Desktop/test with the AES algorithm. Once the data is encrypted, the custom extension will show and a README.txt file will be placed into the Desktop/test folder. The information needed to decrypt the folder is sent to the target URL, our Kali server.

21) We know that the files in the ***Desktop/test*** folder will get encrypted, so first find the folder on your desktop as shown in Fig. 10.

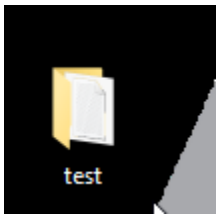

Fig. 10 Test folder on desktop

22) Double-click the test folder to reveal the contents (Fig. 11).

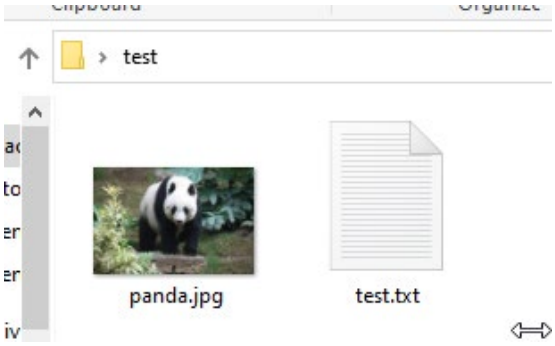

Fig. 11 Files in the test folder

23) Run the ***hidden-tear.exe*** by double-clicking on its icon (Fig. 12).

Fig. 12 Hidden Tear icon

24) After a short while, look back in the test folder. You will see that the files are encrypted with the extension from Step 5c. The files should resemble those shown in Fig. 13.

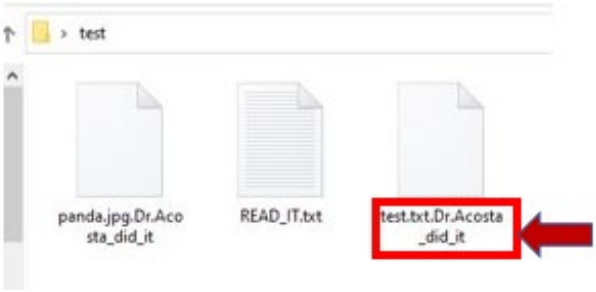

Fig. 13 Encrypted files with new extension

25) Open the READ_IT.txt file and we can see the answer from Step 5e. The output should match that shown in Fig. 14.

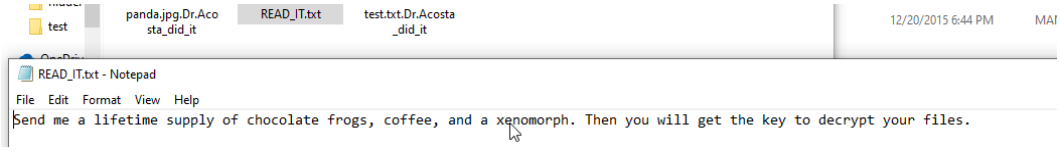

Fig. 14 Ransom message

26) Stop capturing traffic by selecting the red stop button on the top left, as shown in Fig. 15.

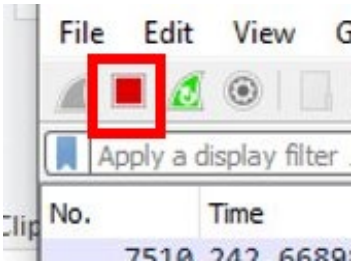

Fig. 15 Wireshark stop capturing button

27) Go back to the Kali VM and check the contents of the ***data.txt*** folder. Here we can see the decryption information that was sent to the web server. (Be sure you are in the ***/var/www/html*** directory when accessing the ***data.txt.***) The output should resemble that shown in Fig. 16.

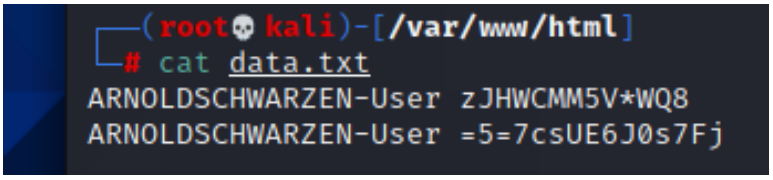

Fig. 16 Ransomware decryption information captured on web server

28) Since we had Wireshark running and capturing our network traffic, let us look through the network capture file to see if we can find the decryption information. This will be in a packet as shown in Fig. 17.

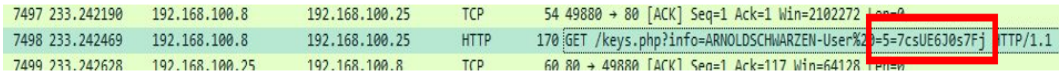

Fig. 17 Ransomware decryption information captured in network packet

29) What is the decryption information?

30) After finding the decryption information, double-click on the Hidden Tear decryptor icon shown in Fig. 18 to run the decryptor program.

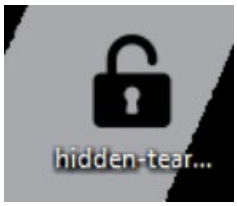

Fig. 18 Hidden Tear decryptor icon

31) After entering the decryption information, you should get a message stating that the files have been decrypted as shown in Fig. 19.

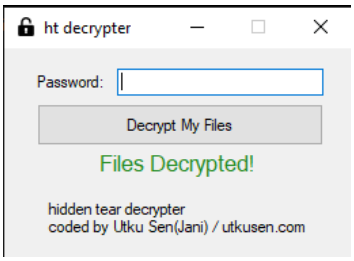

Fig. 19 Files decrypted dialog

32) Go back to the Desktop/test folder to ensure all files have been decrypted.

Congratulations! You have completed the exercise and should now be familiar with how Hidden Tear works (specifically) and how ransomware works (generally).

5. Conclusion

This exercise was designed to make participants aware of ransomware, its dangers, and how it works at a very high level. Additionally, users are able to see firsthand how ransomware encrypts files on a computer, making them inaccessible unless a ransom is paid. The network traffic captured during the execution of the ransomware was used to demonstrate how some ransomware stores passwords and decryption information on external servers instead of on a local machine, making the task of decryption nearly impossible for a victim.

The exercise only touches on small aspects of ransomware, a very specific malware that was released for educational purposes. However, many other ransomware samples act in similar ways and we hope this conveys general information related to the potential impacts and the critical need for awareness. Keeping the community aware of what attacks look like can minimize the number of victims. The FBI does not recommend paying the ransom due to the possibility of not getting the decryption information even after the payment is issued.[16]

This exercise is part of the hands-on cybersecurity studies that are used for training and awareness that fuel research and collaboration in the field.

6. References

1. Gazet A. Comparative analysis of various ransomware virii. J Comp Virology. 2010; 6.1:77–90.

2. Hull G, Henna J, Budi A. Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Sci. 2019;8.1:1–22.

3. Srikanth. Cyber criminals target IoT devices with a new malware. TechiExpert. 2021 Feb 9. [accessed 2021 May]. https://www.techiexpert.com/cyber-criminals-target-iot-devices-with-a-new-malware/.

4. Shinde R, Van der Veeken P, Van Schooten S, van den Berg J. Ransomware: studying transfer and mitigation. 2016 International Conference on Computing, Analytics and Security Trends (CAST); 2016 Dec. p. 90–95. IEEE.

5. Riley T. The Cybersecurity 202: global losses from cybercrime skyrocketed to nearly $1 trillion in 2020, new report finds. Washington Post. 2020 Dec 7 [accessed 2021 May]. https://www.washingtonpost.com/politics/2020/12/07/cybersecurity-202-global-losses-cybercrime-skyrocketed-nearly-1-trillion-2020/.

6. Jeffers M, Turton W. Ransomware attack shuts down biggest U.S. gasoline pipeline. Bloomberg. 2021 May 8. [accessed 2021 May]. https://www.bloomberg.com/news/articles/2021-05-08/u-s-s-biggest-gasoline-and-pipeline-halted-after-cyberattack.

7. Microsoft Corporation. Get a Windows 10 development environment. 2021c [accessed 2021 Feb]. https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/.

8. Flare-VM. [accessed 2021 Feb]. https://github.com/fireeye/flare-vm.

9. Oracle Corporation. VirtualBox. 2021c [accessed 2021 Jan]. https://www.virtualbox.org/.

10. OffSec Services Limited. Kali Linux downloads. 2021c [accessed 2021 Feb]. https://www.kali.org/downloads/.

11. CISSP.com. Hidden Tear ransomware is now open source and available on GitHub. 2020c [accessed 2021 May]. https://www.cissp.com/security-news/587-hidden-tear-ransomware-is-now-open-source-and-available-on-github.

12. Wireshark. [accessed 2020 May]. https://www.wireshark.org.

13. Cybersecurity & Infrastructure Security Agency. Ransomware guidance and resources. [accessed 2021 May]. https://www.cisa.gov/ransomware.

14. Merriam-Webster. Sandbox. [accessed 2021 May]. https://www.merriam-webster.com/dictionary/sandbox.

15. FireEye, Incorporated. FireEye. 2021c [accessed 2021 May]. https://www.fireeye.com/company.html.

16. Federal Bureau of Investigation. Scams and safety: ransomware. [accessed 2021 May]. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware.

List of Symbols, Abbreviations, and Acronyms

AES	Advanced Encryption Standard
ARL	Army Research Laboratory
DEVCOM	US Army Combat Capabilities Development Command
IoT	Internet of Things
IP	Internet Protocol
PHP	Hypertext Preprocessor
URL	Uniform Resource Locator
VM	Virtual Machine

1 (PDF)	DEFENSE TECHNICAL INFORMATION CTR DTIC OCA
1 (PDF)	DEVCOM ARL FCDD RLD DCI TECH LIB
2 (PDF)	DEVCOM ARL FCDD RLC ND J CLARKE J ACOSTA