Step by step how to deal with ransomware: a practical case

by Washington Almeida

Every day we read news or receive information about a new type of crime in the digital environment. The criminals are becoming more and more sophisticated in their methods of attacks, making use of the resources that the information technology offers. In this scenario, the attack of the moment is known as ransomware. Various methods are used by cyber security experts around the globe in the fight against ransomware. A step-by-step forensic approach on how to deal with ransomware is where this article seeks to contribute. I finish the article performing an interesting enumeration attack against the criminals' website, hidden inside DeepWeb on TOR network, which made it possible to reveal their TOR exit node and other hidden IP address.

In history, the use of cryptography began to arouse interest in times of war, such as during the Cold War, when the United States and Soviet Union used these methods to hide their actions and movements from each other, encrypting their messages with a key, preventing who did not have the key from reading it, which forced the enemy to use methods to attempt breaking the encryption codes.

With the advent of the Internet, the cryptography service has evolved into several digital services, ensuring security for e-mail services, e-banking infrastructure, web services, among others, widely used by the world population in the present days.

Unfortunately, digital criminals have figured out a way to use this sophisticated service for illicit purposes. First, they invested time attempting to break down encryption protocols to gain access to valuable information. At the present time, they make use of this technology to extort their victims. In other words, a service created to offer security, today can be also a digital threat.

Every day we read news or receive information about a new type of crime in the digital environment. The criminals are becoming more and more sophisticated in their methods of attacks, making use of the resources that the information technology offers.

In this scenario, the attack of the moment is known as ransomware. Various methods are used by cyber security experts around the globe in the fight against ransomware. A step-by-step forensic approach on how to deal with ransomware is where this article seeks to contribute.

I finish the article performing an interesting enumeration attack against the criminals' website, hidden inside DeepWeb on TOR network, which made it possible to reveal their TOR exit node and other hidden IP address.

Acknowledgment note:

It is very important to mention the companies and professionals who work hard and serious, contributing all the time to our complex forensics work. In this regard, I reserve special thanks to the company called "UTI dos Dados" (http://www.utidosdados.com.br/) located in the municipality of Barueri/SP and its competent team, led by its Chief Technical Officer Wellington Rodrigues da Silva who kindly ceded the infected equipment, and worked with me in the phases of identifying and recovering the data, making it possible to work in a real-scenario to be shared with Pentest readers.

What is ransomware?

In a simple definition, ransomware is a class of malware designed for the purpose to block the victim's access to their data, encrypting them and requesting a payment in Bitcoin currency so that the data can be decrypted. In other words, instead of stealing your information, the ransomware authors hold your data hostage, forcing the victims to pay for the data rescue.

Infection Vector:

Most ransomware is spread through e-mail systems with a document attached to the message. In this scenario, the victim can find two main types of attachments. The most common is a Word document with malicious macros attached. When the file is opened, the victim will be invited into enabling macros by telling the user if the document is not being displayed correctly the user needs to enable the macros. The second type of attachment is an executable file disguised as another file extension. This attachment takes advantage of the default Windows configuration that does not display the last extension. Therefore, at first glance, a user would see a jpg file with all its characteristics when, in fact, the file is an executable file. See my video in my YouTube channel at URI https://www.youtube.com/watch?v=2Kt2p9r_b4E where I explain in detail how hackers make use of this technique.

In my research, I observed other infected vectors by P2P networks where users share files, downloading illegal software protected by intellectual property, attaching infected media devices in the computer, downloading freeware or shareware from unverified websites and also when users visit any suspicious links, like pornographic or torrents, among others.

A real-scenario

When the computer ceded by "UTI dos Dados" starts (thanks Wellington again), the user proceeds with the logon and after that, the following screenshot is presented to the user shown in Figure-2 below:

Figure 1: Ransomware in action.

This is a real scenario brought to Pentest readers and we will analyze this screenshot in more detail as we move forward in our work.

Forensic approach

There is a very strong reason to address the issue with a forensic approach: the Preservation process.

This point is especially important because of the right to the full defense and contradictory present in Brazilian legislation. Also, this analysis may be requested by the other party to be analyzed by their technical assistant.

The preservation process should provide the capacity of reproduction of the analysis at any time by another forensic expert in the field of knowledge. See in Figure 2 below how I see the preservation process inserted in the Forensic process framework.

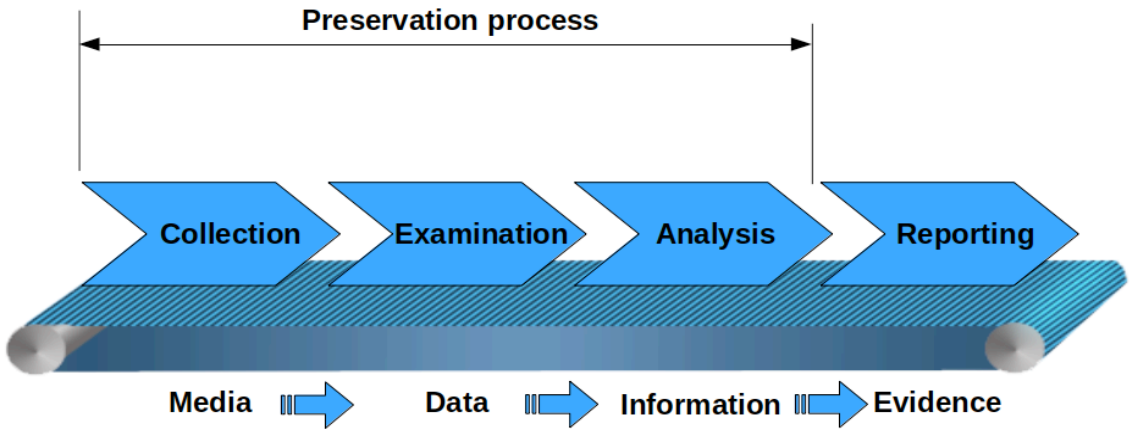

Figure 2: Preservation process inserted in the Forensic process.

Additionally, at any time, a judge may require a complement of the forensic analysis.

Note that the preservation process is not only important in dealing with technical issues but also with regards to the legal aspect. This makes digital forensic work a multidisciplinary activity where professionals in the Information Technology and the Legal areas need to work together to address cases properly.

In addition, the forensic approach proves to be a good tactical plan because it is impossible to get an accurate idea of the damage to the victim's computer during the first contact with ransomware.

Once we have defined the concept of the digital forensic process and the reason for choosing the method, let us go ahead and start our work.

Preserving the evidence

Our work starts with media imaging, which is different than media cloning. Under a Linux environment, the forensic expert can perform this step using the utility dcfldd or dd as following:

```
┌─[root@parrot]─[/home/wash/Apps/ransomware/data]

└──╼ # dcfldd if=/dev/sbc of=ransom.iso
```

This command will create a forensic image named ransom.iso which will be used for our analysis. It is mandatory to extract the hash of the RAW image file just afterwards using the MD5 and SHA1 that are the most commonly used in digital forensics. The result of performing the hashing check will go through the chain of custody. An example of a Linux command line to generate image's SHA1 hash is shown below:

```
┌─[root@parrot]─[/home/wash/Apps/ransomware/data]

└──╼ # sha1sum ransom.iso
```

There are several parameters that can be used with the dcfldd but the command line presented above is the simplest one since our work is concentrated in dealing with ransomware.

Dealing with ransomware in Digital Forensic Framework

Digital Forensic Framework is a software developed by Arxsys and the DFF community. The documentation and packages to download are available in the Arxsys website at URI http://www.arxsys.fr.

As part of the Linux Parrot Security OS 3.4 distro, I launch the DFF GUI interface and load the evidence ransom.iso image file into it as shown in Figure 3.

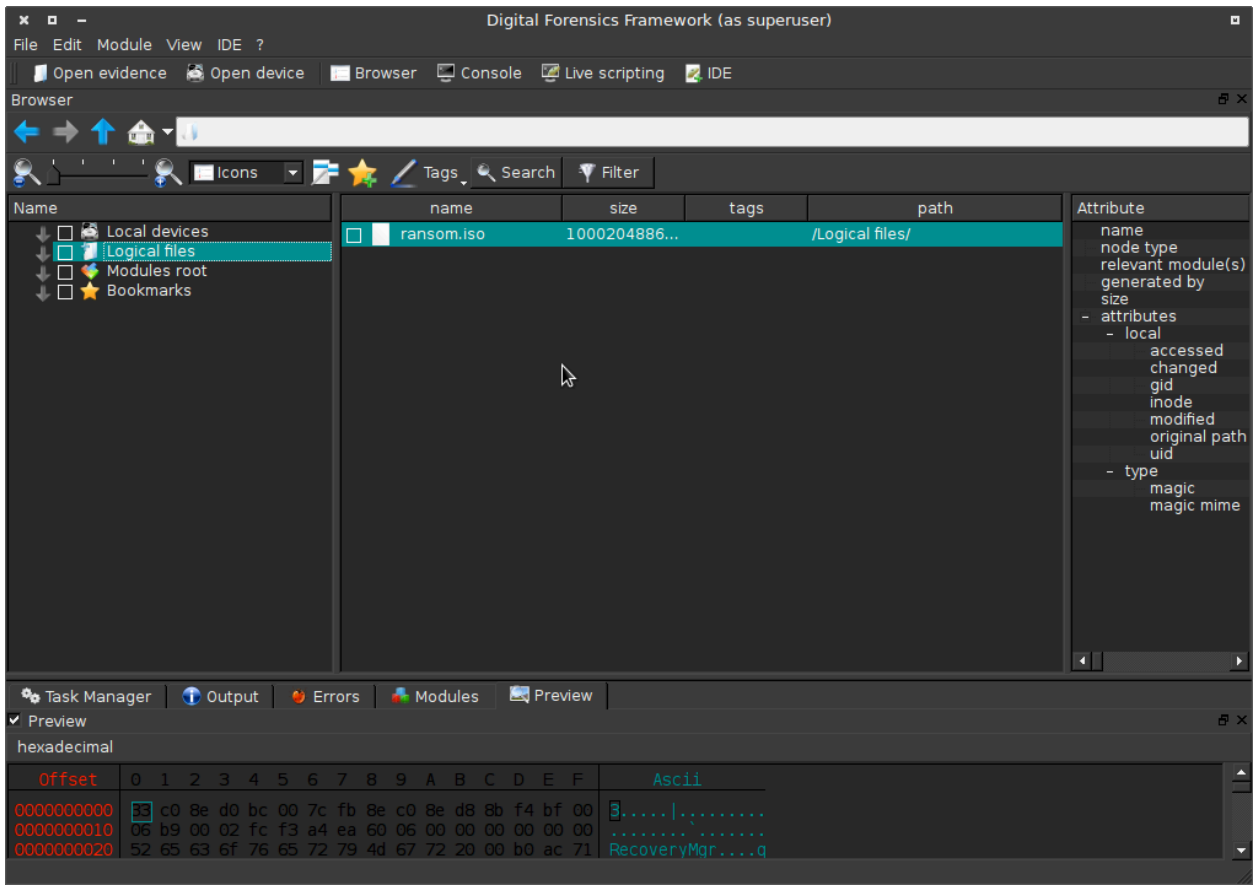

Figure 3: Loading RAW image into DFF GUI.

Once the image is loaded into the DFF environment, we need to reconstruct the partitions found in the volume so that we come to be able to access the data inside each partition. Double clicking in the ransom.iso the DFF partition module will be automatically loaded as shown in the figure 4.

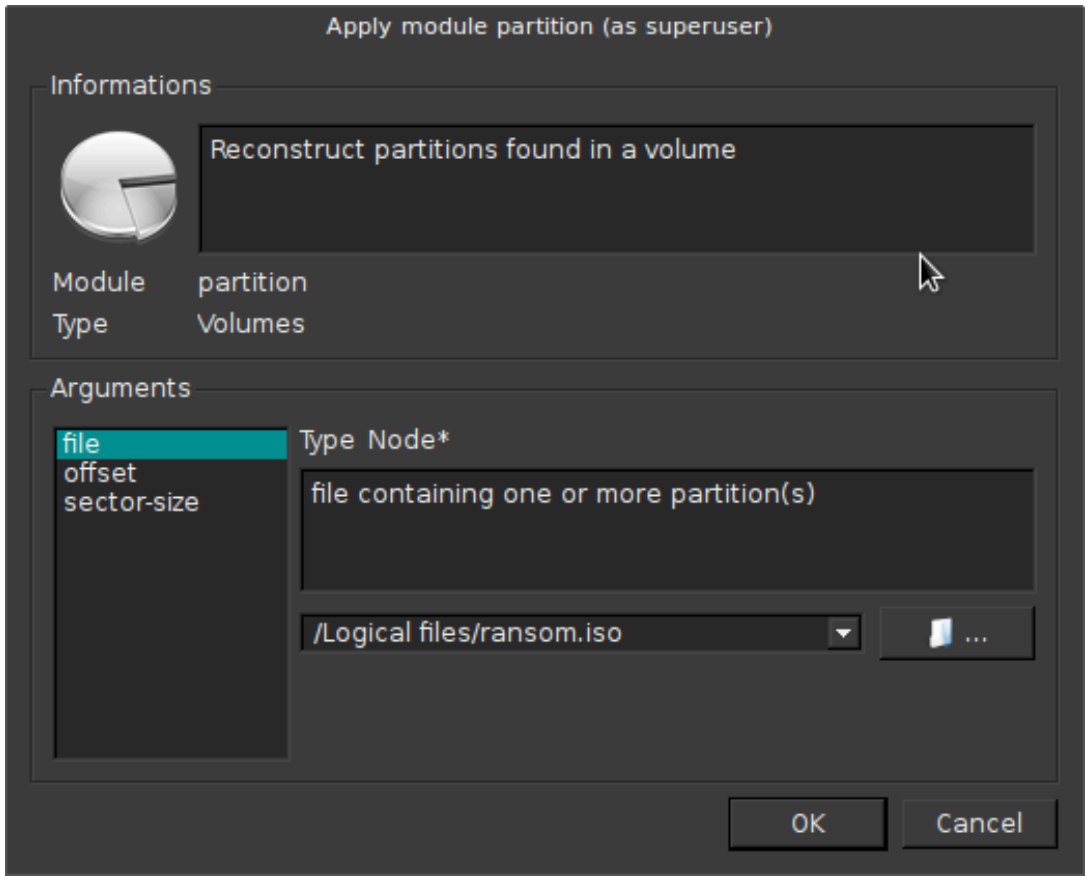

Figure 4: Reconstructing the partitions.

Depending on the partition size, the reconstruction task can take longer. After reconstructing all partitions, as shown in figure 5, the forensic specialist can explore the content of each partition.

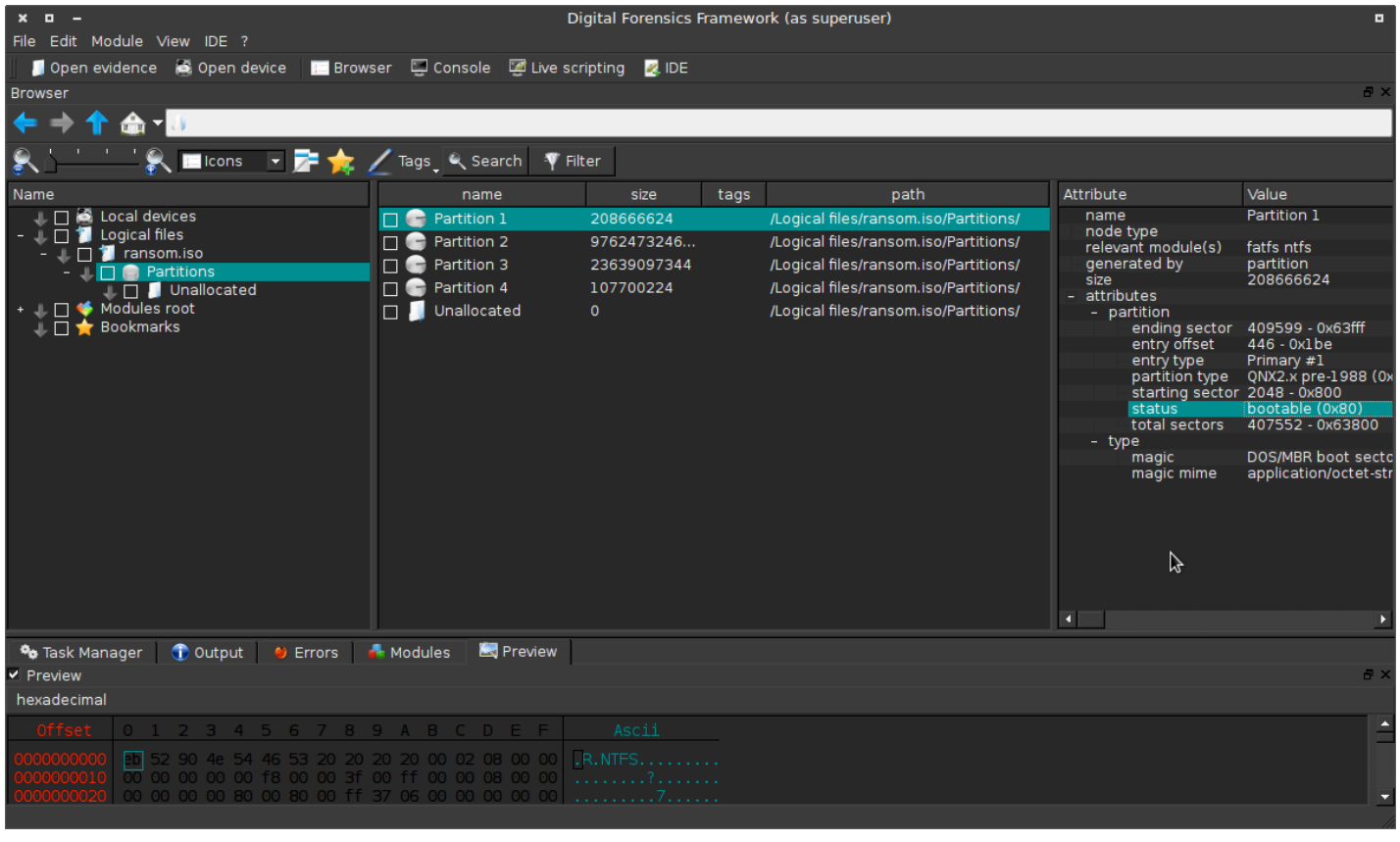

Figure 5: Disk partitions reconstructed.

As we can see, the first partition with the 0x80 status is the bootable one. Let's check the integrity of this partition.

Investigating the reserved files of the bootable partition we can realize that all files were not infected with some kind of malware.

When we analyze the partition boot sector, our interest is based in the byte offset and its field length. The operation system first looks at the 8 bytes at 0x30 to find the cluster number of the $MFT, then multiplies that number by the number of sectors per cluster (1 byte found at 0x0D) and the number of bytes per sector (2 bytes found at 0x0b). This value is the byte offset to the $MFT, which stands for Master File Table.

The advantage of working inside the DFF or similar tool is that we can extract each file separately, right clicking on the file of our interest and extracting it from the RAW file to an outside folder in another system. When performing this approach, the reader can check the hash of the RAW image and certify that it remains the same value no matter how many times we have to perform the extraction operation.

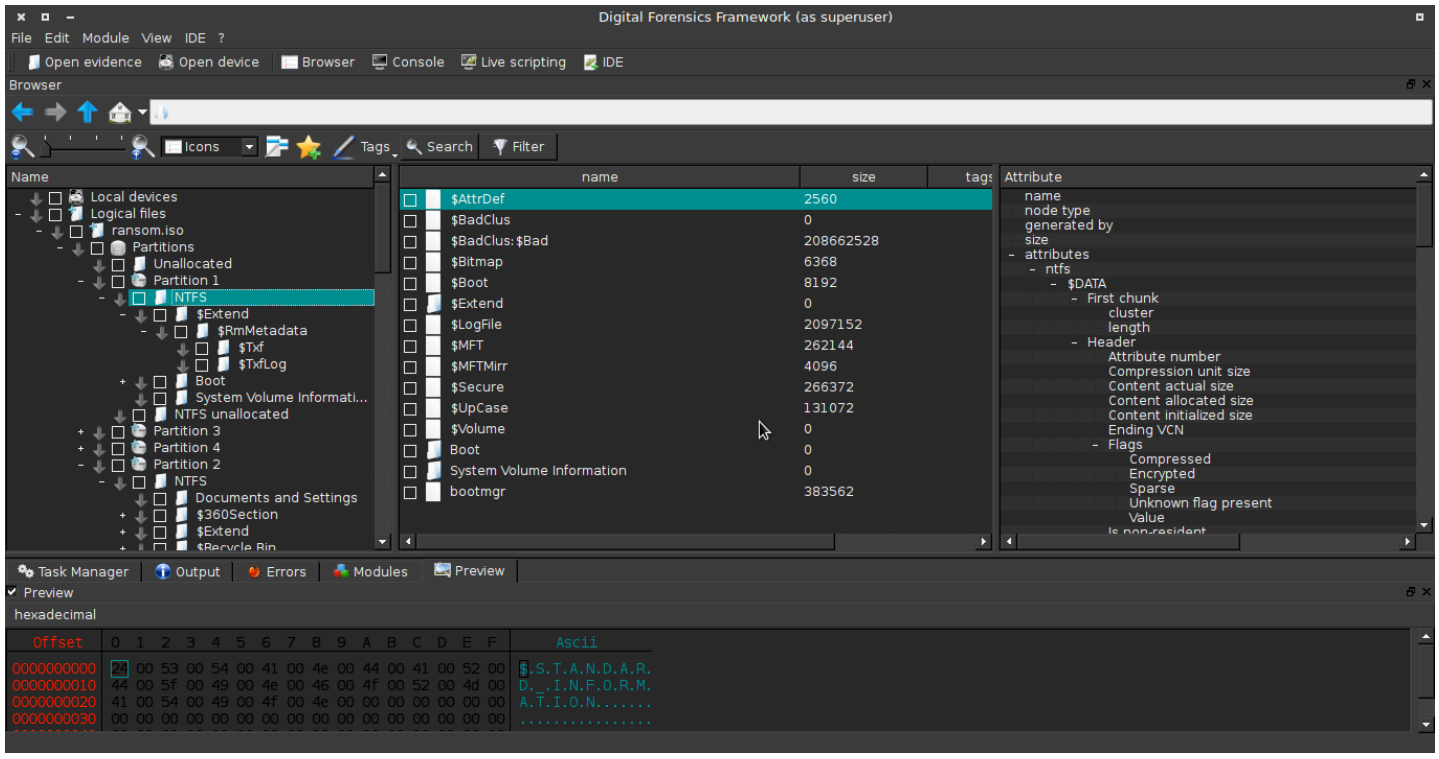

Figure 6: Verifying bootable partition.

After finishing the work in the bootable partition, let us check the Partition 2 where the file system is hosted.

I start having a look in the binary files inside boot folder and continue by analyzing each file and I can verify none of them are infected as shown in the figures 7 and 8 below.

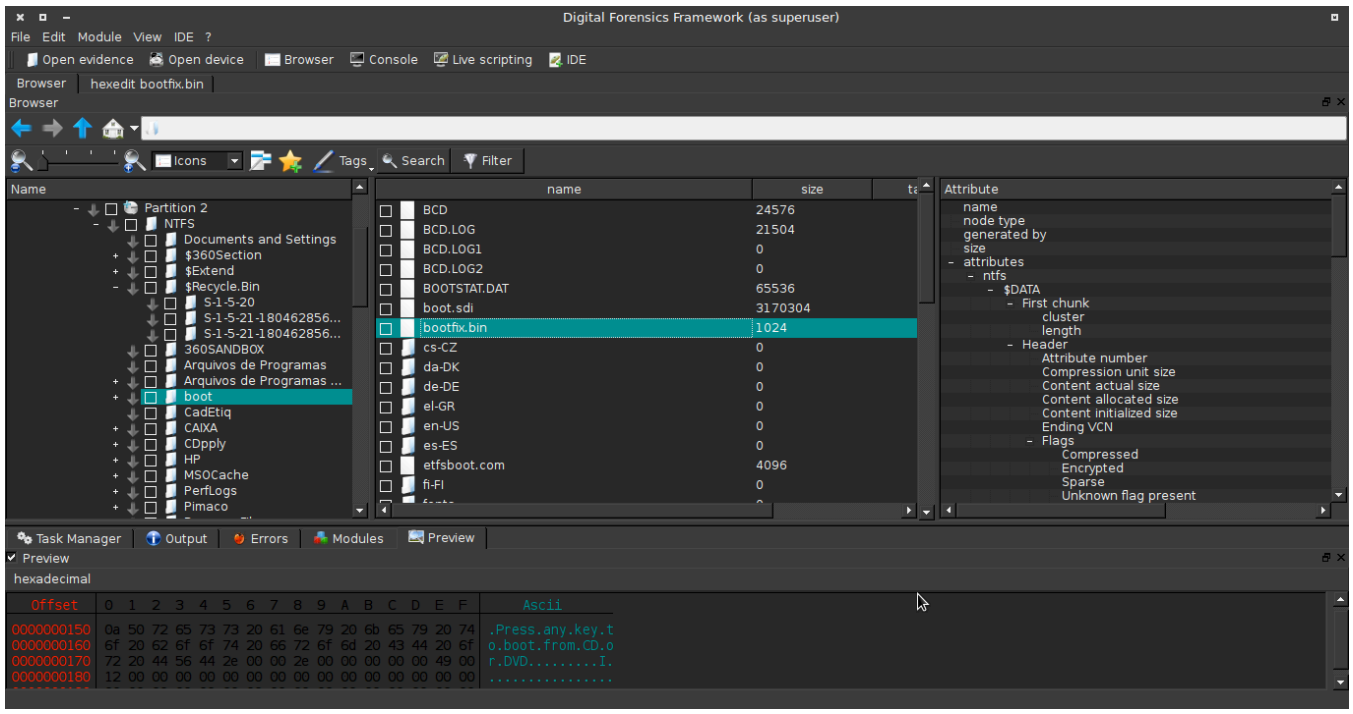

Figure 7 : Binary boot files ok.

At this point we can say that the ransomware starts working when the MS Windows core services start. So we can turn the computer on in safe mode and locate the MS Windows core services, identifying suspicious services where the ransomware are operating and neutralize it.

But before starting the machine in safe mode to manually remove the ransomware, let's have a look inside the user profile folders in order to collect more information about the criminal's actions. It is important because we have to help law enforcement identify who is acting in a criminal way in the worldwide network.

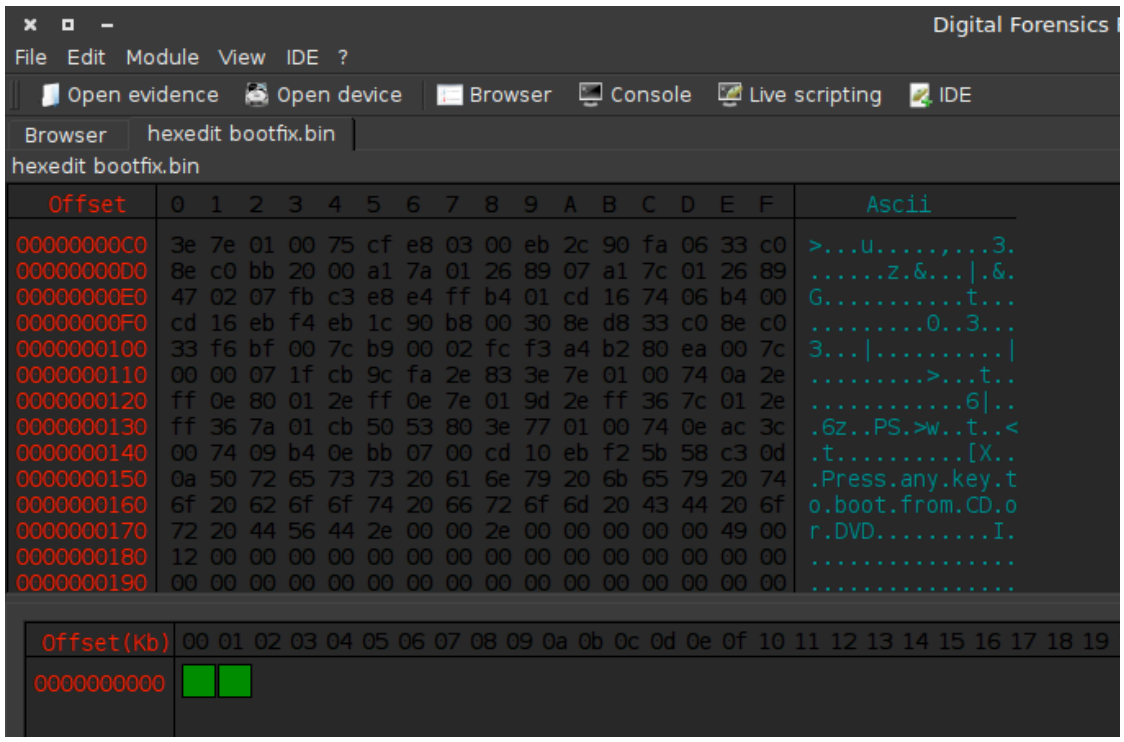

Figure 8: Analyzing binary files signatures.

So I invite the reader to join me and analyze figure 9 together.

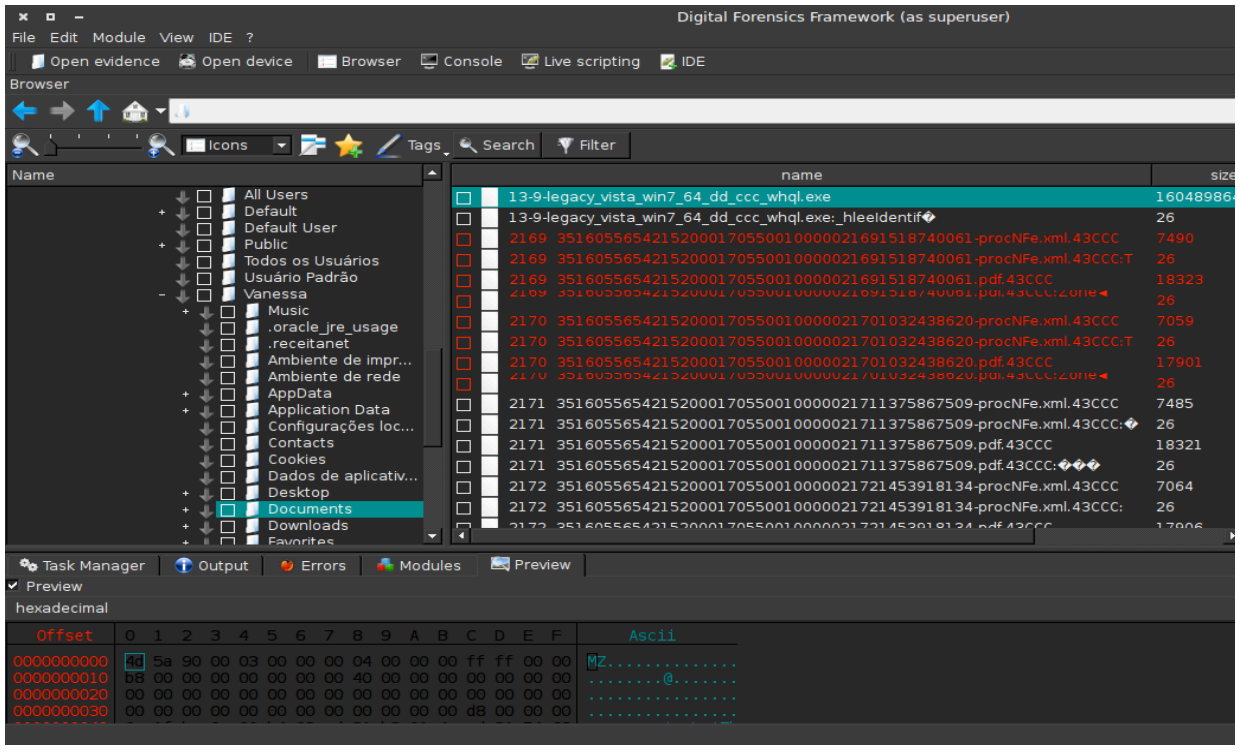

Figure 9: Analyzing files inside user folders.

At first glance, we noticed lots of files presented in red and white colors. The files presented in white are those that are visible to the user inside the folder. The files identified in red are those ones that have been deleted and are able to be recovered. Observing the files in more detail, we can realize the files are identified with a second extension .43CCC just after the original extension.

All those files have been encrypted by ransomware and the victim cannot work with them anymore.

Now let us have a look in the figure 10. Two files catch my eye inside the Documents folder: @65AE7A9A96C0.txt and @65AE7A9A96C0.html. These files compose the content of what is presented to the victim and it was shown in figure 1 in the beginning of this article.

After carefully analyzing them, I could certify that the HTML file does not have any threats. It just formats the text inside the @65AE7A9A96C0.txt file to be shown to the victim.

There are these two files in all folders where the content is completely encrypted.

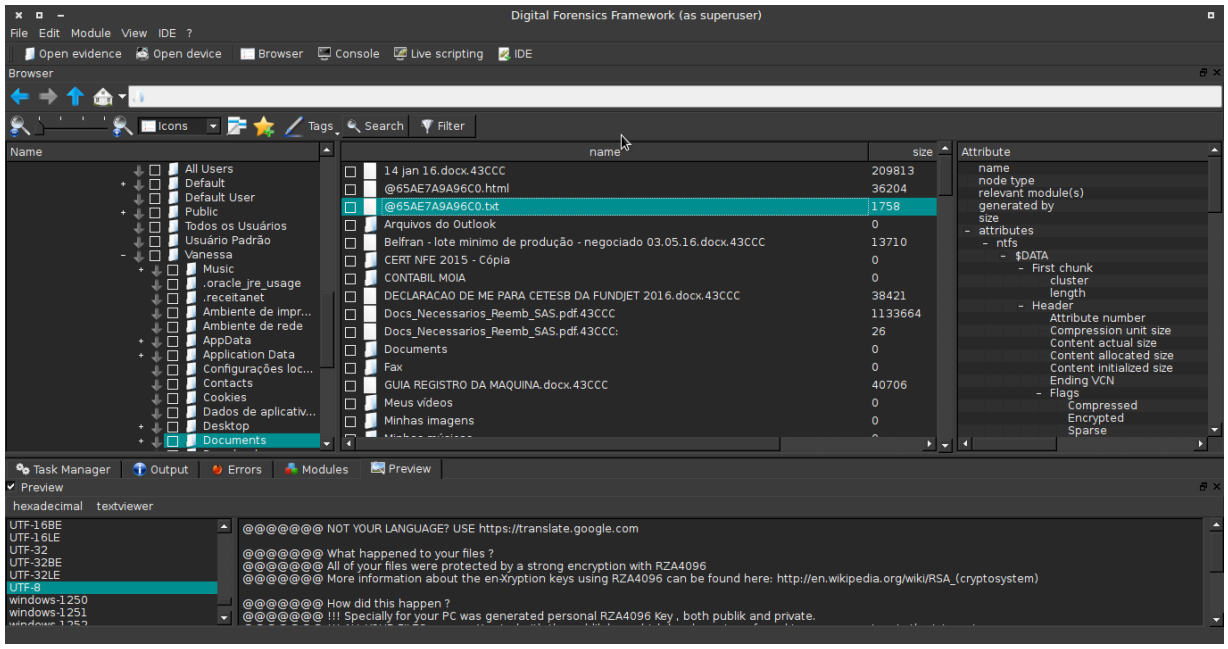

Figure 10: Ransomware files.

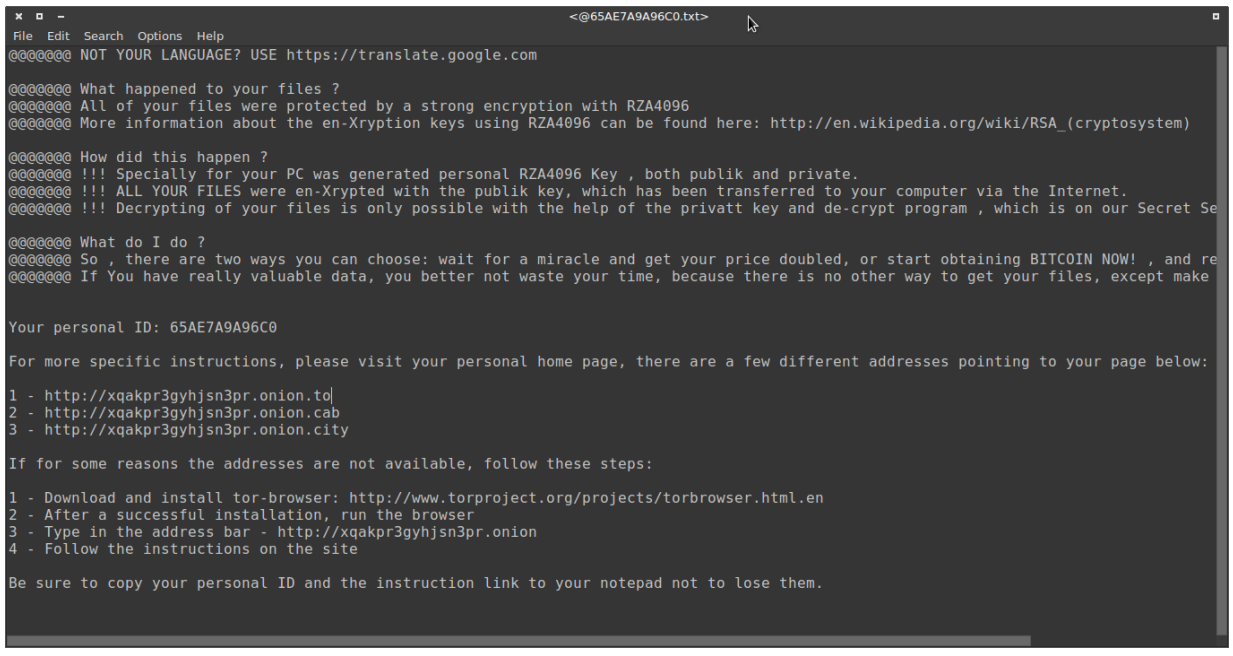

Figure 11: Ransomware message in the @65AE7A9A96C0.txt file.

Following the instructions in the @65AE7A9A96C0.txt file we are invited to visit a web site located inside the TOR network, also known as DeepWeb.

Figure 12 shows us the main page of the criminal's portal located at http://xqakpr3gyhjsn3pr.onion waiting for the victim's visit.

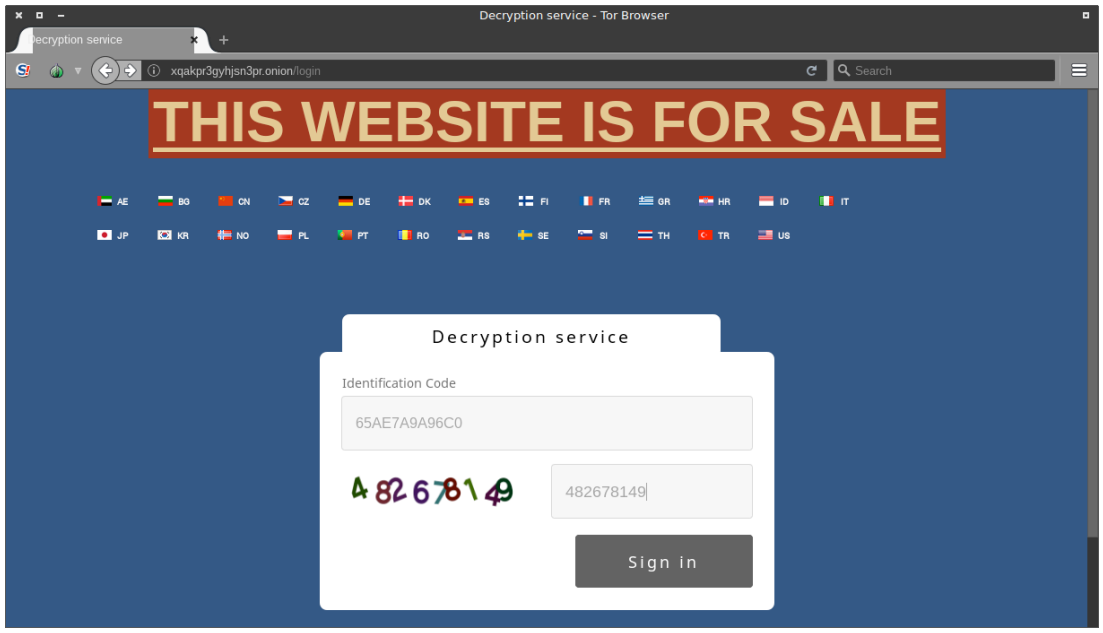

Figure 12: Criminal's web site located inside DeepWeb.

Then we fill in the blanks with the identification code followed by captcha and click in the "Sign in" button, after which we are redirected to the page shown in figure 13.

Figure 13: The clock is ticking to do the payment.

Following the instructions below, we learn the Bitcoin address where the criminals inform the wallet number as shown in figure 14.

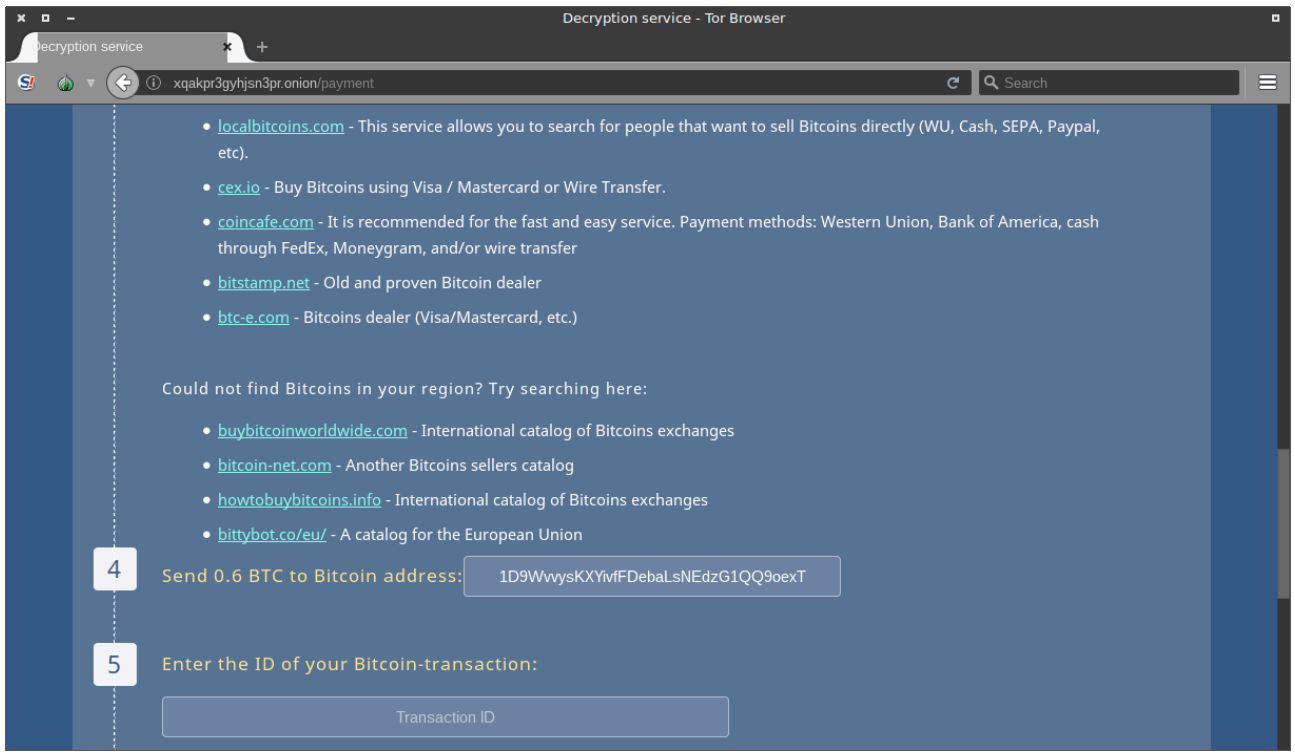

Figure 14: The criminal's wallet informed to victim.

At this point, the decision is to pay nothing to the criminals! Thus, we have to manage the MS Windows environment and try neutralizing the ransomware.

Managing MS Windows to neutralize the ransomware

Now that we have performed the forensics analysis and preserved the evidence, we will initialize the machine in safe mode to check each initialization Windows core service.

Pressing F8 key when initializing the MS Windows operating system, we will be invited to choose the boot options as exhibited in the figure 15.

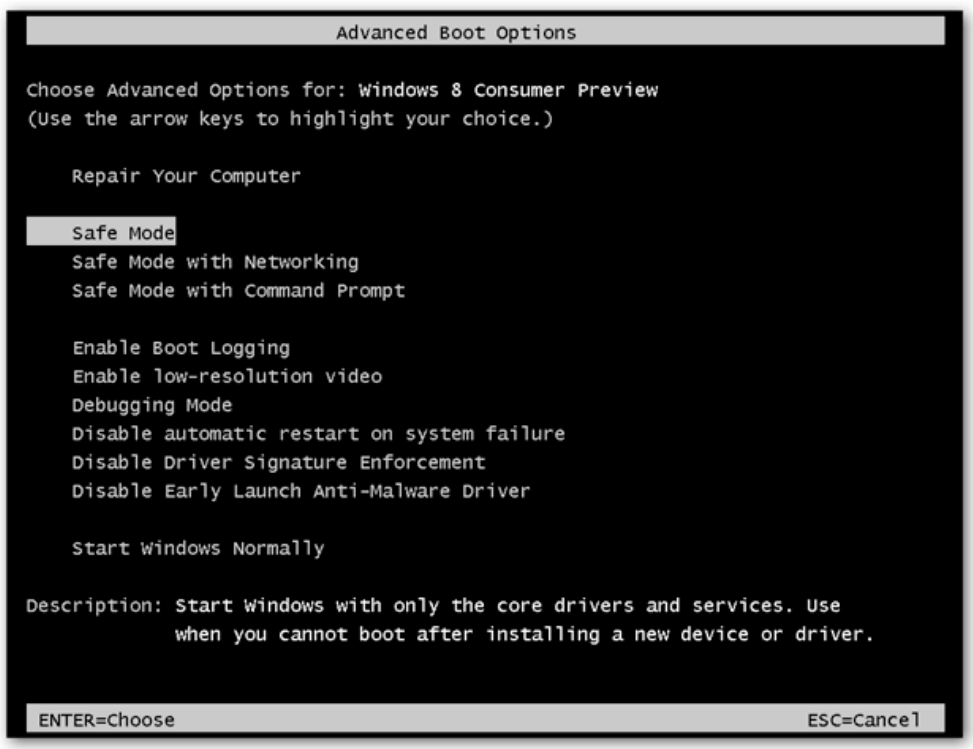

Figure 15: MS Windows Advanced Boot Options.

After loading MS Windows in safe mode, I press the buttons “Windows” + “R” together. This will open the “Run” box. Then I type “taskmgr” in the blank to launch the Task Manager.

Inside the Task Manager, we have to switch to the Process tab and identify the processes that are part of the ransomware. At this point, it is important to understand there are several types of ransomware and not all of them affect the same system components. As we deal with the various types of ransomware every day, we learn about its operation mode and, of course, it helps us to identify the main actors in this theater.

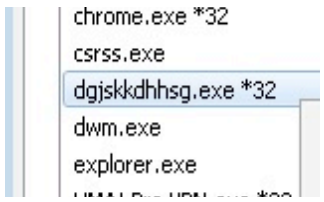

Figure 16: Ransomware processes infecting Windows environment.

Two actions are important at this point: Locate the folder where the file is hosted and finish the malicious process identified in the Task Manager.

After that, it is necessary to look for hidden files in the system. To do that, I open any folder, click in “Organize” button, choose “Folder and Search Options”, select the “View” tab, select “Show hidden files and folders” option and finally uncheck the box “Hide protected operating system files”, finishing the task by clicking in the “Apply” and “OK” buttons respectively.

Then we still have tasks to perform. Now we need to locate the ransomware in the services startup location. Depending on the OS (x86 or x64) it can vary. So I have to open Windows Registry and check the following entries:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Services
```

Each suspicious service must be excluded from the registry entries above.

After that, we have to exclude the suspicious executable file inside the folder %appdata%, %LocalAppData%, %ProgramData%, and %WinDir% if found it there. So we just navigate to these folders and delete the malicious program inside it.

Also, we must delete all the content inside the %temp% folder, no matter which file extension or folder you find inside it.

The forensic specialist can alternatively use the Windows program named msconfig to double check the execution point of the ransomware.

Recovering the encrypted files

The first and best method to recover the encrypted files is to restore your data from a recent backup, supposing that you have one.

Alternatively, we can try to restore the files via Volume Shadow Copies. Sometimes this approach can be possible because some kinds of ransomware encrypt the files first and makes a copy of them, encrypts the copy and then deletes the original ones. If this is the scenario you are facing, you may try to use Shadow Explorer software to recover your original files.

In my research, I realize the recent versions of ransomware are prepared to handle this situation by completely eliminating the Volume Shadow Copy content so that this option is not available to the victim.

Also, it is important to have in mind that the ransomware names in your machine might be different as they usually are generated randomly, that's why you should run any professional scanner such as SpyHunter to identify malicious files.

It is entirely possible that you have fifteen cases of ransomware and each of them has different executable file names in each one, even if they are the same type of ransomware.

Identifying real IP addresses inside TOR network

Now it is time to work on getting information about the criminal's resources since we are always committed to contributing to the justice.

The Pentest Magazine reader may be aware that it is almost impossible to identify the IP address inside the TOR network although the TOR network is not perfect on providing anonymity. However, it is quite complex to identify the real IP address of a service hosted inside the TOR network.

So let us negotiate some packages with the criminal's website in order to see what kind of information we can get.

Analyzing the website source code of each page and inspecting carefully all its elements as shown in figure 17 I realized there is a flaw in the way the application is handling the information.

To be more specific, I found out the criminal's website has a vulnerability identified as OSVDB-630. I have knowledge of some tools that can help me in this situation.

What follows in figure 18 is a simple enumerate attack very helpful to identify the IP of the TOR exit node used by ransomware authors.

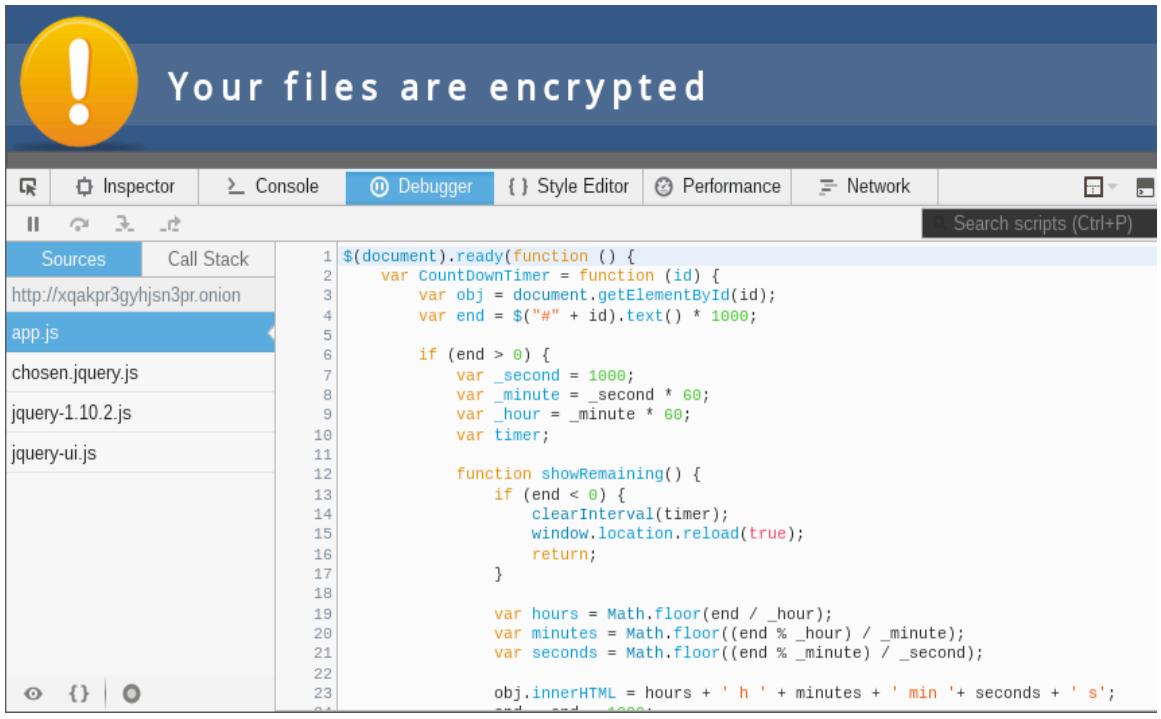

Figure 17: Performing a complete code analysis of the criminal's website.

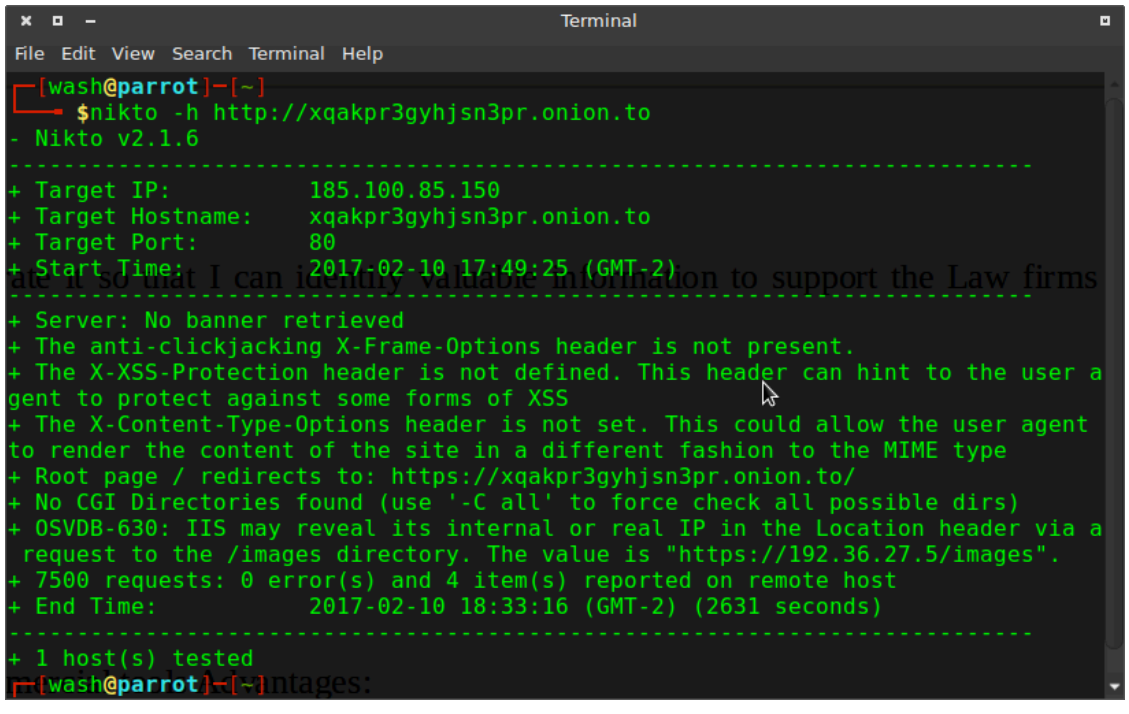

Figure 18: Enumeration attack against the web server authors.

The Pentest reader can realize in figure 18 that initially the URI was identified by an IP address 185.100.85.150 provided by TOR tunnels, but due to a flaw in the IIS server of the criminal's where a request was done in the IMG folder and the locations header returns the real IP address, which is the TOR exit node whose IP is 192.36.27.5.

From one day to another, the target IP addresses will be inverted. See the date in both figures 18 and 19. This is the way the TOR tunnels work.

As we have the other IP address today, I will check the domain xqakpr3gyhjsn3pr.onion.to in order to get some information of the services running behind the website.

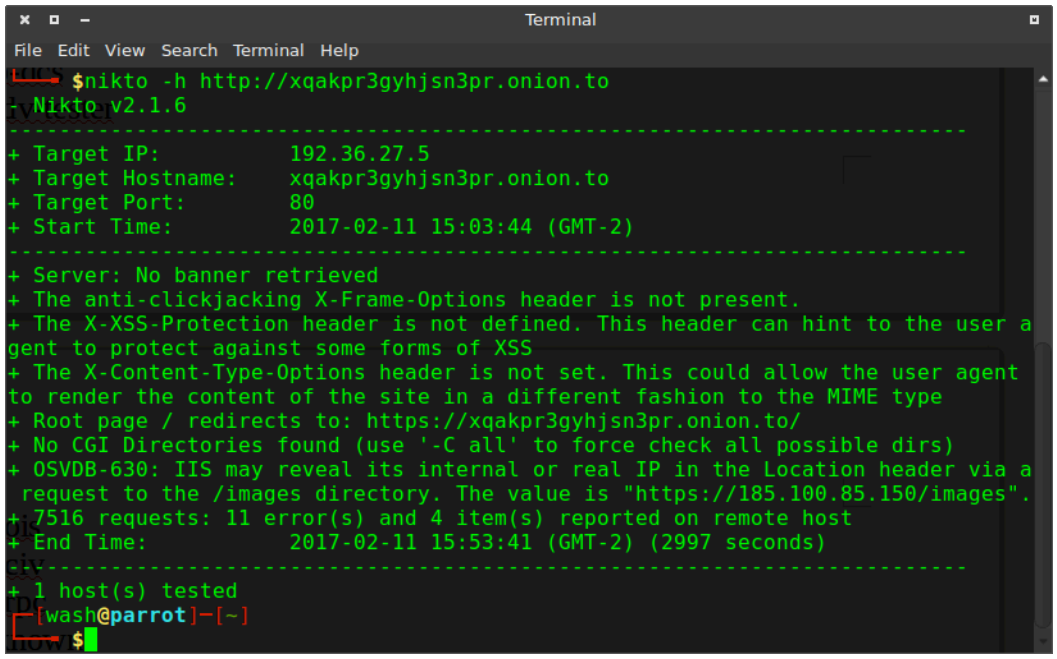

Figure 19: Enumeration attack against the web server authors in the next day.

While navigating in the website https://xqakpr3gyhjsn3pr.onion.to and monitoring the traffic with wireshark, I could realize the traffic passing through AS number 200651 located in Romania as shown in figure 20 below, whose IP address is 185.100.85.150.

AS stands for Autonomous System. I believe that one of the best definitions to Autonomous System can be found in the RFC-4271 that describes the BGP protocol, but in a few words it defines how to route packets from one AS to other AS using an inter-AS routing protocol.

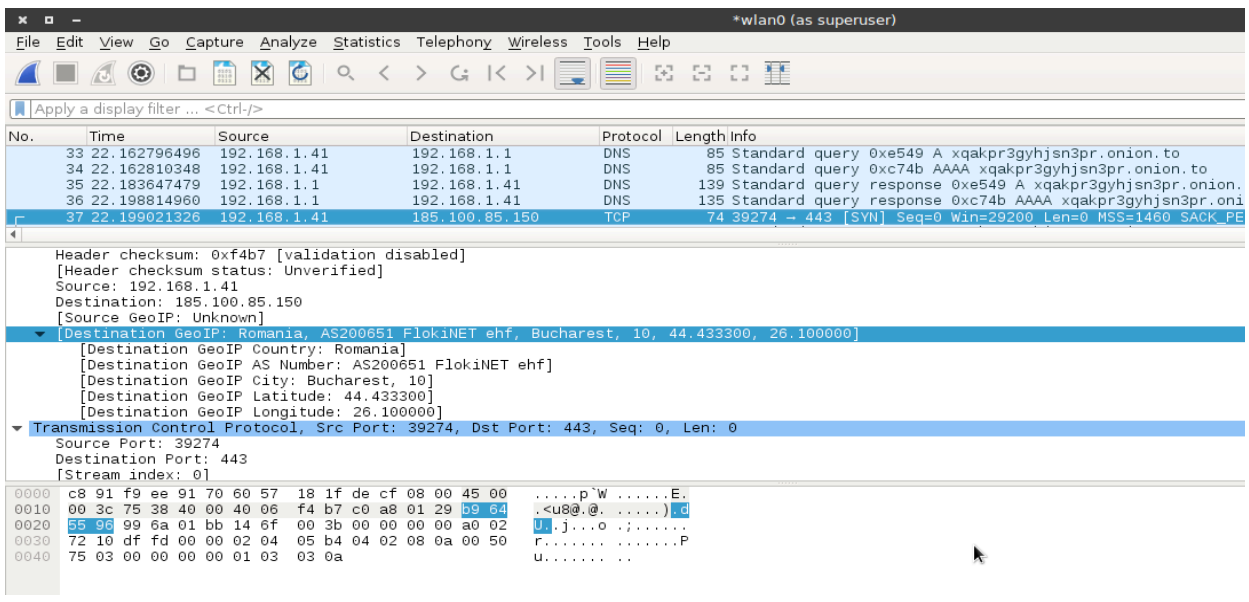

Figure 20: Identifying the AS200651 located in Romania.

Now pay attention in the frame 78 in the figure 21 below. The package identifies the IP address 40.20.35.114 negotiating TLS data with my port number 41106 as if this IP was the AS24961 located in Germany (Source).

This IP address is new in our scenario. I only had access to this information because I was monitoring all my traffic since I started navigating the criminal's web site.

Much more interesting is what we can find outside the frame 78 using the command line whois against the same IP address 40.20.35.114.

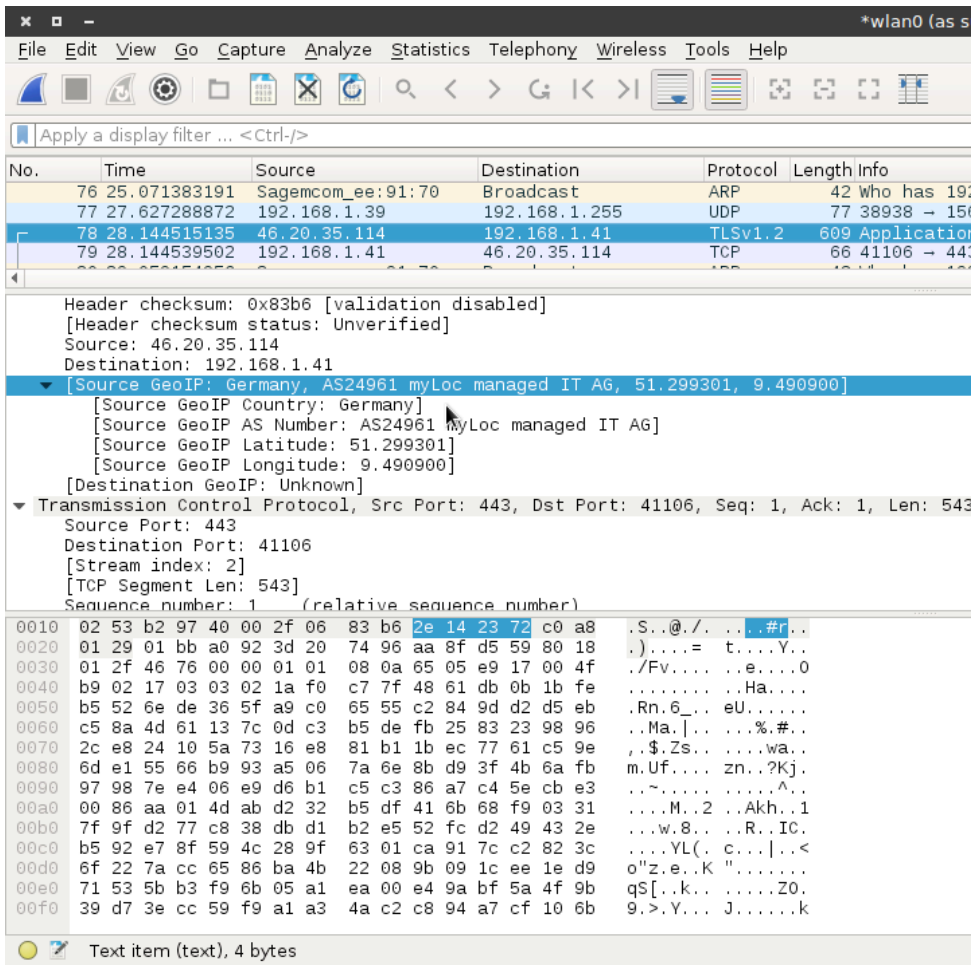

Figure 21: Identifying the AS24961 located in Germany (TOR exit node).

When launching whois against the IP address 40.20.35.114 we can see the following information (some info removed from the result):

```
NetRange:    40.0.0.0 - 40.63.255.255

CIDR:        40.0.0.0/10

NetName: LILLY-NET

NetHandle:   NET-40-0-0-0-1

Parent:      NET40 (NET-40-0-0-0-0)

NetType: Direct Assignment

Organization:    Eli Lilly and Company (ELILIL)

RegDate: 1991-04-23

Updated: 2015-02-23
```

```
Ref:    https://whois.arin.net/rest/net/NET-40-0-0-0-1

OrgName: Eli Lilly and Company

OrgId:       ELILIL

Address: Lilly Corporate Center

City:        Indianapolis

StateProv:   IN

PostalCode:  46285

Country: US

RegDate: 1988-09-13

Updated: 2012-11-02

Ref:    https://whois.arin.net/rest/org/ELILIL

OrgTechHandle: HENDE42-ARIN

OrgTechName:  Henderson, Dave

OrgTechPhone: +1-317-277-9636

OrgTechEmail: henderson_dave_g@lilly.com

OrgTechRef:  https://whois.arin.net/rest/poc/HENDE42-ARIN
```

Wow. This IP address is not located in Germany, it is located in the United States, instead!

Putting it all in a nutshell, the forensic specialist has to deeply analyze the information when an illicit is involved in order to provide differential support to law firms and judges.

The goal with this exercise is to show to the Pentest reader that following the hosts in deepweb requires the kind of analysis that take longer.

The good thing is that nothing can be hidden and we can exploit the resources inside deepweb in the same way the criminals do with their victims.

The ransomware black market

Researching and working with ransomware over the years, we realized that this market will still bring many challenges to the legal and information technology areas. There is a booming black market, developing sophisticated graphics suites for the generation of new types of ransomware. The HANSA

portal located in the deepweb is one example. The site markets a graphical interface specialized in ransomware generation.

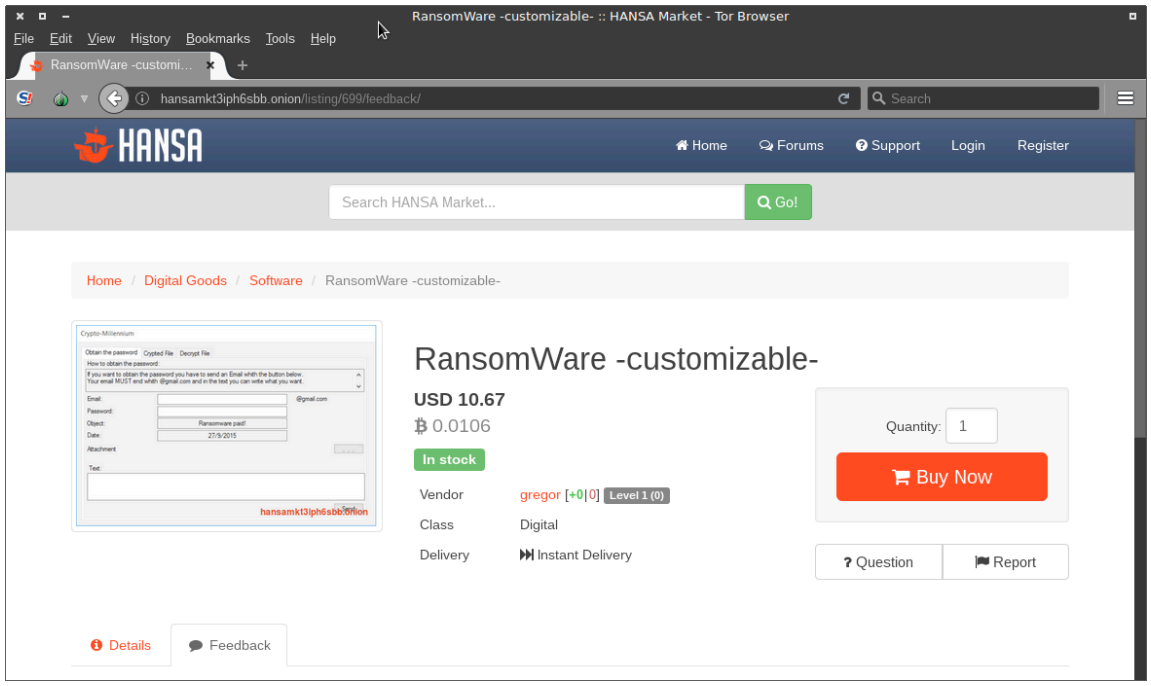

Figure 22: Ransomware's blackmarket.

In the Details tab, the visitor finds the ransomware suite specifications.

This black market behind the ransomware gives us an idea of how lucrative this segment is, although only a few people are subject to payment for the rescue of their data.

Summary

As we can see, the task of removing a ransomware is a very technical task in which the victim sometimes opt to pay for the rescue of their data due to the time line that can take until its complete restoration. Fortunately, only about three percent of the victims opt for the data rescue payment.

I made it a point to show the reader that even with the criminal features hosted in the obscure environment of deepweb they can be exploited and revealed.

Keep in mind to back up your data regularly to minimize the damages that a digital malware may bring.

For companies, consider creating specific policies for access controls, maintain security patches and not any less important, educate and train your users to maintain compliance with the information security policies.

We can make the digital criminals' life much more difficult if making use of the best practices of information security.

References

https://www.youtube.com/watch?v=2Kt2p9r_b4E. Access in February 11, 2017.

Author: Washington

Washington is an Electronic Engineer specialized in Digital Forensics and Cyber Security with more than 25 years of experience in the Information Technology and Engineering areas, working for large companies in the sectors as Engineering, Information Technology, Consulting, Chemical and Mining. Professional certified by players as Cisco and Microsoft acts as Digital Forensics with in-depth knowledge of computer hardware, network technologies, telephony, programming, data communication protocols and a vast of information security knowledge with a set of skills known by ethical hackers, where this knowledge base is fundamental to assist the Justice.

Wash Web page: www.washingtonalmeida.com.br

Washington Almeida e-mail:
wualmeida@washingtonalmeida.com.br.