Soares C, et al., J Forensic Leg Investig Sci 2022, 8: 067
DOI: 10.24966/FLIS-733X/100067

HSOA Journal of Forensic, Legal & Investigative Sciences

Review Article

Digital Forensic Analysis of Ransomwares for Identification and Binary Extraction of Cryptographic Keys

Cleber Soares[1], Deivison Franco[1,2]* and Joas Santos[1]

[1]Researcher and Consultant in Digital Forensic and Information Security–Belém/PA, Brasil

[2]ACCESS Security Lab and Bank of Amazônia–Belém/PA, Brasil

Abstract

This article aims to show the use of digital forensic to recover the cryptographic key of files encrypted by ransomwares through identification, extraction and binary analysis of memory dumps. Thus, in the approached scenario, it was verified the possibility of recovering the encrypted files by verifying the characteristics and behavior of the ransomware, allowing to identify and extract its cryptographic key through the analysis of the data contained in memory, with a methodological approach that can be used analogously for other similar cases in which it is necessary to recover environments attacked by this type of malware.

Keywords: Binary extraction; Cryptographic keys; Digital forensic; Memory dump; Ransomwares

Introduction

Ransomware is a type of malware that prevents access to the infected system by blocking and encrypting files, charging a ransom to recover them by paying with cryptocurrencies, which makes it impossible to identify and track the criminal. Once a system is infected, the ransomware encrypts the user's data in the background, without the user noticing, and when ready, emits a "pop-up" informing that the machine is blocked and that the user will no longer be able to use it. it, unless you pay a fee to obtain the key that gives access to the data. (Figure 1) illustrates the typical anatomy of a ransomware attack.

***Corresponding author:** Deivison Franco, Researcher and Consultant in Digital Forensic and Information Security, ACCESS Security Lab and Bank of Amazônia–Belém/PA, Brasil, Email ID: deivison.pfranco@gmail.com

Citation: Soares C, Franco D, Santos J (2022) Digital Forensic Analysis of Ransomwares for Identification and Binary Extraction of Cryptographic Keys. Forensic Leg Investig Sci 8: 067.

Received: November 30, 2022; **Accepted:** December 12, 2022; **Published:** December 17, 2022

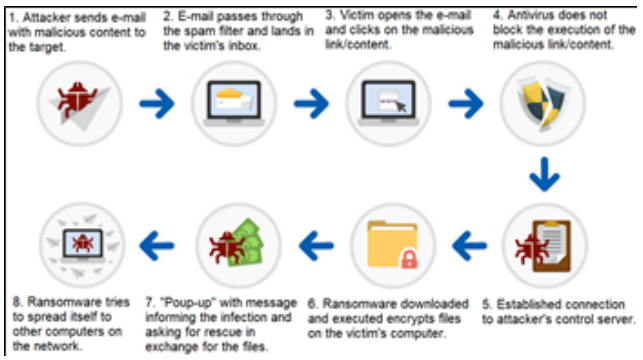


Figure 1: Typical anatomy of a ransomware attack (Adapted from STATISTA, 2016).

The first ransomware was created in 1989, called PC Cyborg, popularly known as AIDS, it was developed by Joseph Popp and simulated the collection of a ransom in the amount of US$ 189.

Ransomware attacks have been increasing considerably, and one of the best known in the world occurred on May 12, 2017-WannaCry, infecting thousands of users around the world.

Digital Forensic Analysis Process

The expert work is based on technical-scientific doctrines and procedures, which aim at the preservation and integrity of the evidence. In the specific case of computation, the manipulation of data contained in computational storage media must be carried out with all possible attention, as the proof cannot have its initial state altered, that is, no bit can be modified. This ensures the validity of the evidence in court. Thus, the investigator should always use forensic equipment and software. To get an idea of the sensitivity of digital evidence, just by turning on a computer and waiting for its operating system to boot, data contained on the hard drive is already altered.

The cybercrime investigation process, that is, the digital forensic process, consists of four phases that deal with everything from receiving the material to preparing the report, namely: Identification; Preparation; Forensic Imaging; Forensic Analysis and Forensic Report. This entire procedure is illustrated in (Figure 2) and explained below.

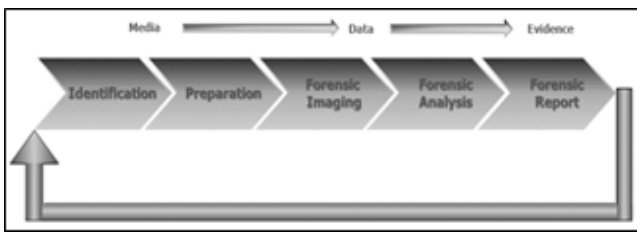


Figure 2: Digital Forensic Analysis Process.

Identification

In this first step, digital evidence seized on a crime scene need to be identified. Responsible for the seizure must write a report, to specify everything captured, with type of evidence, trademark, serial number, memory capacity, exact place where it was, and people to whom it belongs. Based on that report, forensic examiners write these evidence characteristics on the forensic report.

Preparation

In the second step, all forensic examination is performed based on a document, called "forensic request". This request is analyzed, to verify if there is sufficient information to start the examinations. Forensic examiners can coordinate the investigation and examination with requesters to determine additional steps. They also setup and validate forensic hardware and software. Afterwards, based on the forensic request and on the data to be analyzed, forensic tools are selected, for instance: tools for evidence analysis, data recovery, decryption and password cracking, steganography analysis and mobile forensics examination.

Forensic imaging

In this step, forensic examiners must make a forensic imaging of the evidence data since they are not allowed to work directly on the original evidence due to the risk to modify and/or to damage evidence. Hence, after this step, the forensic examiners work just based on the copies of the evidence.

Forensic analysis

This step is the process to discover evidentiary information in the computer evidence based on the forensic request. In some cases, this information is not apparent to the investigators or may be protected by passwords or encryption. Forensic examiners may use specific software's, such as FTK [1], EnCase [2], SleuthKit [3]and others, to locate, undelete, and put available all user's files, for instance, .pdf, Microsoft Office files and email. Note that the exemplified files are usually the most important for the investigation.

Forensic report

In this last step, a forensic report may be issued based on the forensic request, and on the forensic data analysis. All forensic procedures done during the examination may be written in this report, as well as all important evidence discovered. The questions of the forensic request need to be answered in this report.

Isolation of Cybernetic Traces

Isolation, although described as a subsequent phase to identification and registration, in practice can occur concurrently, as as items are identified at the crime scene, some measures can be taken to ensure their isolation.

The main idea of isolation is to prevent attacks on the integrity of the evidence (alterations, deletions, insertions, destructions). Due to the special nature of the cybernetic trace, we will divide isolation into two categories: the physical and the logical.

Physical isolation

Understanding the physical perimeter and delimiting it in order to isolate it seems simple, but it is a difficult task to perform.

What is the size of the area to be isolated in order to cover all traces? The rule is to isolate the largest possible area within the context of the crime, since isolation done too little can contaminate the region not covered by the isolation and lose important traces.

It is worth remembering that human beings are not the only agent that modifies the environment, there are other factors to be considered, such as bad weather (cold, rain, humidity, heat, sunlight, wind, magnetic radiation, etc.). Depending on the region, some additional measures must be taken in order to quickly identify and isolate existing traces. Therefore, some classifications of the places are necessary.

Regarding the region

a. Immediate: region with the highest concentration of traces of the occurrence of the fact. More careful examinations will be carried out there, since due to the principle of locality of spatial reference, most of the evidence will probably be found there.

b. Mediate: region comprised by the periphery of the immediate region. In the same way that occurred in the immediate region, we have the possibility of the existence of more than one mediate region.

Regarding the preservation

a. Suitable: place where the traces have remained unchanged since the occurrence of the fact until its registration.

b. Inappropriate: place where the vestiges were compromised, either by removal, insertion or a combination of both.

Regarding the area

a. Internal: one that has at least superior protection against rain, sun and other more aggressive natural elements. The absence of walls in the confinement of the room does not deprive it of this classification. An open shed or a building entrance are examples of this type of classification.

b. External: that which is located outside the premises and is directly subject to the influence of the most aggressive natural elements. It is possible to find in these environments network cables, signal transmitting/receiving antennas, biometric authentication devices, etc.

c. Virtual: one where there is no direct link between the physical context and the logical one. An action performed in a given physical environment can produce physical and logical evidence in another completely different location.

Regarding the nature

Place classified according to the type of event associated with it, such as: pedophilia, insertion of data into information systems, invasion of computer networks, etc.

Logical isolation

The nature of the device to be isolated for subsequent seizure is who will dictate the appropriate procedures. The most common device categories at digital crime scenes are highlighted below.

Notebooks and desktops

Most of the time, the most relevant information to be isolated is found on some secondary storage media: HD, Pendrive, external HD, etc. This means that only these storage devices need to be isolated for later collection.

In some cases the entire machine will have to be identified and isolated for this purpose, this is the case with those that use RAID [4] disk arrangements where from a physical point of view we find several HDs and from a logical point of view we have a single disk. In this sense, another aspect that must be taken into account is the state these devices are in: On or Off.

- On: if it is on and the operating system is properly initialized, first check the feasibility of registering evidence in flagrant situations. Collecting the contents of primary memory, which is often volatile, should be considered. Shared files, running programs, open windows, browsing sessions in progress, conversations in communication software and, mainly, information decrypted when reading (but which is encrypted when stored on secondary media). In any case, the main idea in this state is to ensure that during the shutdown process, the normal operating system shutdown steps are not followed, since they may be associated with unwanted events or compromising the integrity of the evidence.
- Off: generally, it should be kept in these conditions, and should not be turned on, since the operating system initialization process causes changes in certain data regions of the secondary storage media, some user programs may still carry out unwanted activities, which can compromise the integrity of the trace. If there is a need to analyze this type of media in loco, care must be taken with regard to protection against writing, for this purpose, a widely adopted solution is to boot using another operating system stored on another media that, in this way, will not produce changes. in the media questioned.

Input/Output devices

Generally, they should not be collected, but in specific cases, their identification and isolation are essential to elucidate the case. As hypothetical examples, a case of anonymous defamatory emails typed from a computer whose keyboard is defective on certain keys, or a printer responsible for printing fraudulent certificates; in a scanner used to capture images used in counterfeit paper money, etc.

Due to the plurality of connection formats and standards, cables, accessories and chargers must be identified as part of the equipment for collection purposes.

Single media

This category includes basically all external secondary storage media on computers (optical media, pendrives, external HDs, memory cards, floppy disks, zip-drives, etc.).

These media can be found both connected and disconnected from computers. Sometimes they are found inside their original equipment, such as camcorders or cameras. In these cases, it is important to remember that despite being a camcorder or camera, the memory contained therein behaves like any other memory, being capable of storing other types of files in addition to photos and videos.

On-site data copies

If in the identification phase any device is identified as important, but the logical evidence can be extracted without the need to collect its support, that is, the physical evidence, copies can be made on site for later analysis. Such copies aim to meet the technical or legal unfeasibility of the collection or even the reduction of the scope of the materials to be collected.

The guarantee of the authenticity and integrity of data collected such as logs, operating system settings, information system files, user files and others deemed necessary, will be done by preserving the original directory structure, as well as the metadata of these files, such as date, creation time and permissions. If possible, it is recommended to take your cryptographic digests (hashes [2]).

Network connected devices

This fact must be recorded and the machine must be disconnected from the network, either by disconnecting the cable or by turning off the machine itself. It may be necessary to identify and isolate the network element itself as evidence of the crime (switch/router). Many times the data of these equipments and their internal configurations will serve as evidence [5].

Special attention must be given to wireless networks, since the absence of metallic or optical cabling does not mean the absence of computer networks. It is necessary to identify access points to wireless networks or even the configuration of ad-hoc networks [6].

Digital Forensic Analysis of Ransomware for Identification and Binary Cryptographic Key Extraction

Analyzed scenario

A scenario was analyzed in which a user executed a malicious artifact that encrypted all his files, which was replicated in a virtualized laboratory, where a Command and Control environment was developed (C2) containing encoded ransomware that, when executed, encrypts the host's data and forwards its cryptographic key to C2, as per the scheme in (Figure 3) and execution shown in (Figure 4).

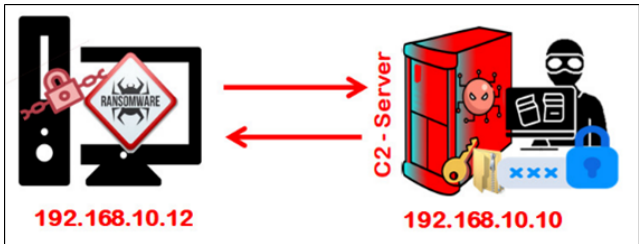


Figure 3: Outline of the analyzed scenario.

Figure 4: Ransomware execution.

Initial procedures

After the incident, the incident response and forensic teams must act quickly following their own or market methodologies to prevent and/or minimize damage. So, avoiding decision-making can hinder creating forensic graphs, or identifying root causes, or creating a consistent knowledge base.

The compromised machine was isolated from its infrastructure, kept on and running a GNU/Linux live CD with the CAINE Forensic distribution (CAINE Live USB/DVD [3]), which has several tools.

Among the range of distribution tools, the FTK Imager was used - forensic software developed by Access Data Corp. [3] that creates binary disk copies, makes memory dumps, in addition to having an intuitive and friendly graphical interface that helps in the forensic analysis process of the dumped images. Therefore, the operational procedures for digital forensic analysis of ransomware were followed for identification and binary extraction of its cryptographic key [7-9].

Downloaded FTK Imager Lite and, after downloading, the "FTKImagerLite" folder was accessed and the "FTKImagerLite.exe" application was executed, as shown in (Figures 5 & 6).

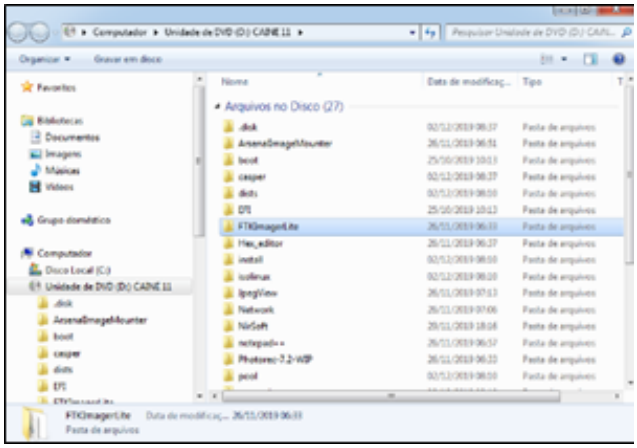


Figure 5: Application Folder "FTKImagerLite".

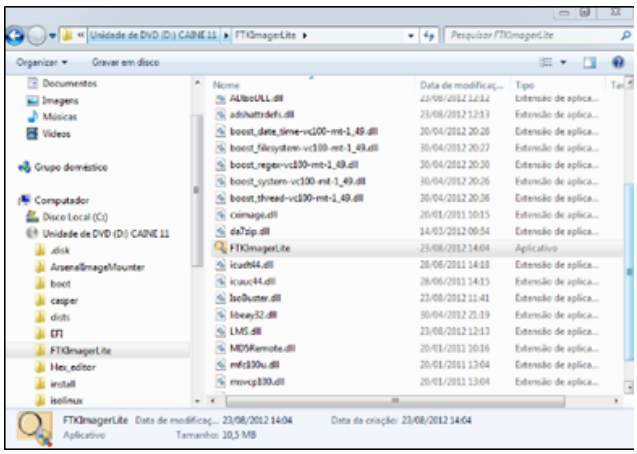


Figure 6: Application "FTKImagerLite.exe".

After running the FTK Imager, click on the "File" menu and select the "Capture Memory" option, as shown in (Figure 7).

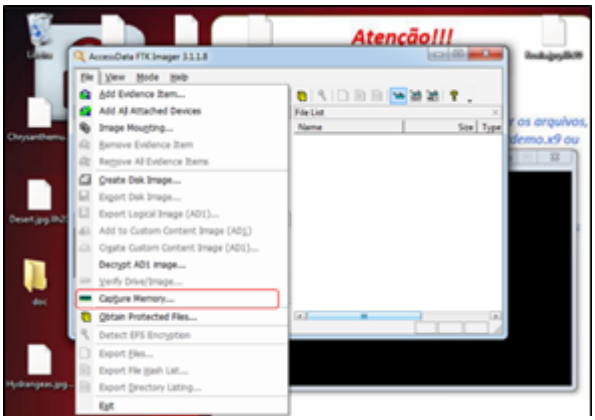


Figure 7: "Capture Memory" option.

A window opened and in it, in the "Destination path" option, where to save the memory dump was chosen and in "Destination filename", the dump file was named as "memdump.mem", and the options of include a paging file ("Include pagefile" [10]) and create an AD1 file ("Create AD1 file") not used at this stage.

Once that was done, click on "Capture Memory", as shown in (Figure 8) (a very valid observation is that if the operating system has a lot of memory, the process may take a while).

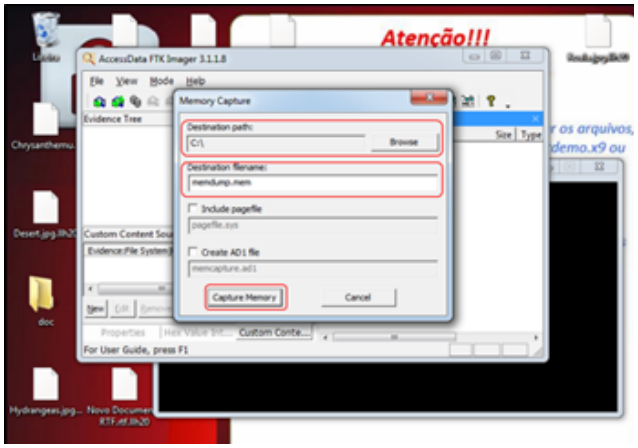


Figure 8: Setting the "Capture Memory" option.

After completing the procedure, click on the "Close" button as shown in (Figure 9).

With the output file in the selected destination folder, the media was removed for analysis of the dump on another device.

In the next step, Volatility [10] was used-command line tool developed in python and one of the most used for memory analysis, containing several plugins for Windows, Linux and Mac systems.

Identification and binary extraction of cryptographic key

There is not even a step-by-step to be followed, as the tool allows the inheritance and analysis of useful memory information, such as running processes and network connections, also allowing to discard

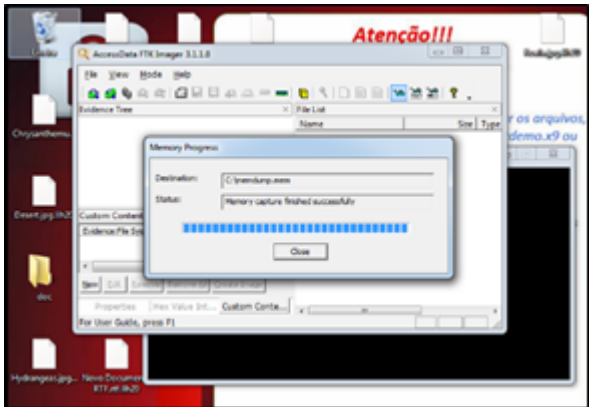


Figure 9: Running the "Capture Memory" option.

DLLs [10] and processes for later analysis, it is up to the investigator to assess what is most useful for his analysis. Next, the procedures performed and the commands executed for the scenario under analysis.

First, the tool's information was verified, showing its commands and the operating system versions that support it through the "info" option, shown in (Figure 10).

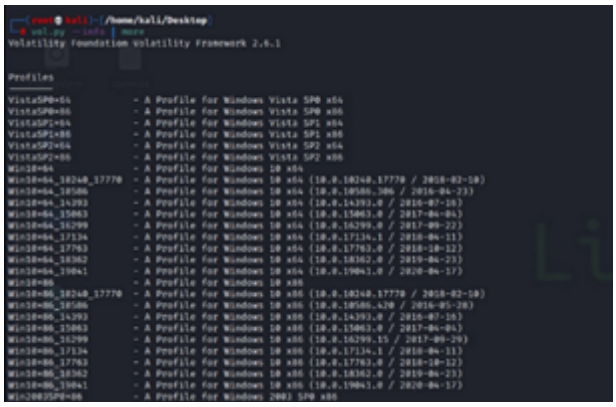


Figure 10: Running the command "volatility --info".

```
# volatility –info
```

Then, to analyze information about memory dumps, the "imageinfo" option was used, as shown in (Figure 11).

Figure 11: Running the command "volatility imageinfo -f memdump.mem".

Afterwards, to verify the processes that were running in the operating system, the "pslist" plugin was used, with the command shown in (Figure 12).

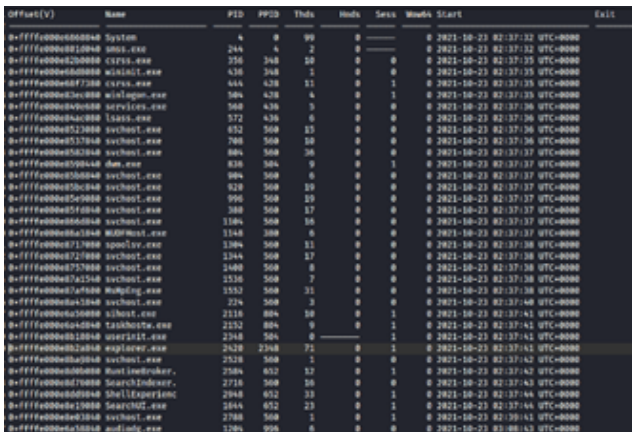


Figure 12: Running the command "volatility -f memdump.mem --profile=Win10x64_10240_17770 pslist".

```
# volatility -f memdump.mem --profile=Win10x64_10240_17770 pslist
```

One option of the "pslist" plugin, which can be used to display the parent and child processes, is the "pstree", which was employed as shown in (Figure 13).

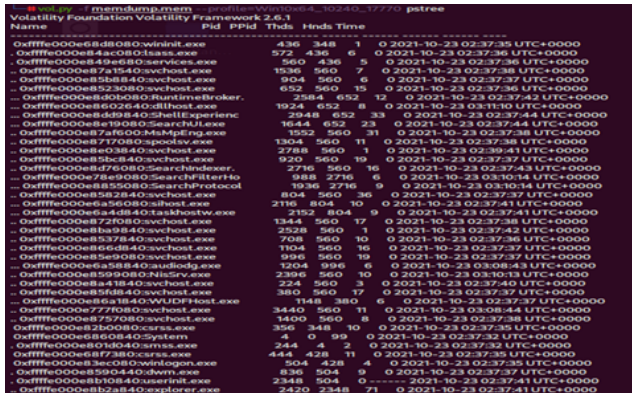


Figure 13: Running the command "volatility -f memdump.mem --profile=Win10x64_10240_17770 pstree".

```
# volatility -f memdump.mem --profile=Win10x64_10240_17770 pstree
```

Then, the "psxview" plugin was used to list the processes that are trying to hide on the computer, as shown in (Figure 14).

After checking the running processes, another fundamental point is to analyze the connections related to them. For this, the "netscan" command was executed, which showed that there was a connection between the machine 192.168.10.12, with "close" status, with the C2 of the attacker 192.168.10.10, as shown in (Figure 15), below.

Although there was evidence of a connection, apparently no suspicious processes were found. So, it was necessary to better analyze some more specific artifacts, as it is characteristic of malware to inject itself into legitimate processes.

Given the above, to validate the Security Identifiers (SIDs), the "getsids" command was used to identify the processes associated with a given user and that may have privileges that can be maliciously

Figure 14: Running the command "volatility -f memdump.mem --profile=Win10x64_10240_17770 psxview".

volatility -f memdump.mem --profile=Win10x64_10240_17770 psxview

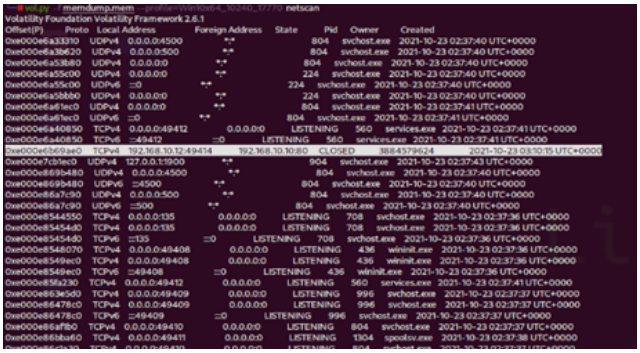


Figure 15: Running the command "volatility -f memdump.mem --profile=Win10x64_10240_17770 netscan".

volatility -f memdump.mem --profile=Win10x64_10240_17770 netscan

escalated, and among the various processes, it was observed that that process 2420 was being executed by several users, in particular by the user "srvmaster" as shown in (Figure 16).

Figure 16: Running the command **"volatility -f memdump.mem --profile=Win10x64_10240_17770 getsids -p 2420"**.

Therefore, based on the results of the "pstree" and "pslist" commands, the "memdump" command was used in process 2420 to extract all its information and dump it in a specific file with the "-p 2420" command followed by the "-dump-dir" option (directory where you want to extract the dump), as shown in Figure 17.

Figure 17: Running the command **"volatility -f memdump.mem --profile=Win10x64_10240_17770 memdump -p 2420 –dump-dir /home/kali/Desktop/dump"**.

 # volatility -f memdump.mem --profile=Win10x64_10240_17770 memdump -p 2420 –dump-dir/home/kali/Desktop/dump

That done, with the "strings" command, the content of the dump was redirected to a file with the ">" parameter, as shown in Figure 18.

Figure 18: Running the command "strings 2420.dmp > 2420.txt".

 # strings 2420.dmp > 2420.txt

After a thorough analysis of the identified and extracted binary, it was possible to identify the computer's communication with the attacker's Command and Control, including some machine information, such as a password that is the key to decrypt the files, as shown in Figure 19.

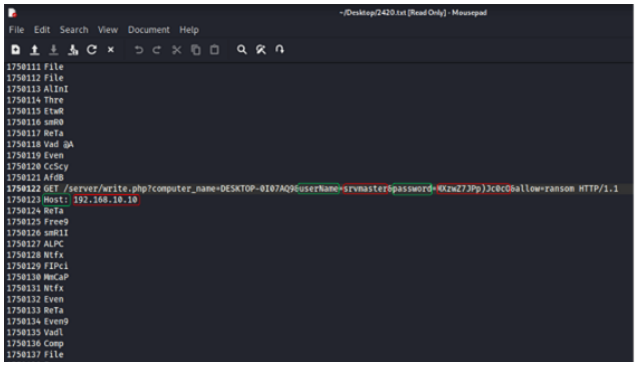
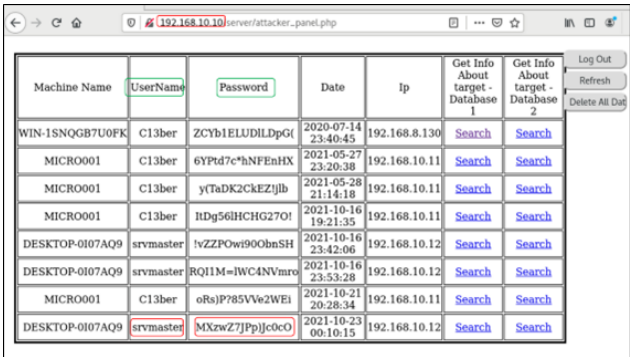


Figure 19: Connection information to the attacker's Command and Control environment including the ransomware's cryptographic key.

Therefore, in the environment that was replicated, it was possible to identify all the information of the equipment present in the attacker's C2, including the rescue password, as can be seen in Figure 20.

Conclusion

Due to the increase in the number of connected computing devices, the distribution of malicious programs associated with criminal practice grows daily. Consequently, the presence of malware in forensic examinations is increasingly frequent. In addition, the high diversity of classes and distinct methods of malware performance make the expert examinations performed in these types of programs create challenges for digital forensic specialists. The purpose of this article was to present ransomware-specific analysis to professionals in the field, along with tools and techniques that will assist in identifying and extracting its cryptographic key.



Machine Name	UserName	Password	Date	Ip	Get Info About target - Database 1	Get Info About target - Database 2
WIN-1SNQGB7U0FK	C13ber	ZCYb1ELUDlLDpG(	2020-07-14 23:40:45	192.168.8.130	Search	Search
MICRO001	C13ber	6YPtd7c*hNFEnHX	2021-05-27 23:20:38	192.168.10.11	Search	Search
MICRO001	C13ber	y(TaDK2ckEZ!jlb	2021-05-28 21:14:18	192.168.10.11	Search	Search
MICRO001	C13ber	RDg56lHCHG27O!	2021-10-16 19:21:35	192.168.10.11	Search	Search
DESKTOP-0I07AQ9	srvmaster	!vZZPOwi90ObnSH	2021-10-16 23:42:06	192.168.10.12	Search	Search
DESKTOP-0I07AQ9	srvmaster	RQI1M=lWC4NVmro	2021-10-16 23:53:28	192.168.10.12	Search	Search
MICRO001	C13ber	oRs)P?85VVe2WEi	2021-10-21 20:28:34	192.168.10.11	Search	Search
DESKTOP-0I07AQ9	srvmaster	MXzwZ7JPp)Jc0cO	2021-10-23 00:10:15	192.168.10.12	Search	Search

Figure 20: Information from the attacker's Command and Control environment with the ransomware cryptographic key.

In view of the above, this article addressed the digital forensic analysis of ransomware for the binary extraction of its cryptographic key, given the preservation of the cybernetic trace along with its respective identification, isolation and collection, since the manipulation of data contained in computational storage media must be carried out with all possible care, as the test cannot have its initial state changed, that is, no bit can be modified.

In the approached scenario, it was verified the possibility of recovering the encrypted files by verifying the characteristics and behavior of the ransomware, allowing to identify and extract its cryptographic key through the analysis of the data contained in memory, with a methodological approach that can be used analogously for other similar cases in which it is necessary to recover environments attacked by this type of malware, since the analysis of malware, in particular ransomware, becomes an increasingly frequent reality in forensic examinations. Understanding the concepts on the subject, knowing methods to understand its operation in order to identify and extract its cryptographic key(s) are tasks that must be present in the daily life of any criminal expert who works in Forensic Computer.

References

1. https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia https://www.academia.edu/34105040/Forensic_Toolkit_FTK_User_Guide
2. ACCESSDATA CORP. FTK User Guide. Lindon, Utah, EUA: AccessData, 2010.
3. Aquilina J, Casey E, Malin C (2008) Malware Forensics: Investigating and Analyzing Malicious Code. EUA: Syngress.
4. Departamento de segurança da informação e comunicações do gabinete de segurança institucional da presidência da república. Diretrizes para o registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes. Brasília, 2014.
5. https://es.statista.com/grafico/9376/como-funciona-un-ransomware/
6. http://ldemetrio.com.br/Livros/Livros_TI/segunda_unid/Sistemas%20Operacionais%20Modernos%20-%20Tanenbaum%20-%204%20Edi%C3%A7%C3%A3o.pdf
7. Velho JA (2016) Tratado de Computação Forense. Campinas: Milennium.
8. Velho JA, Costa KA, Damasceno CTM (2013) Locais de Crimes - dos Vestígios à Dinâmica Criminosa. Campinas: Millennium.
9. Velho JA, Geiser GC (2021) Espíndula A Ciências Forenses-Uma introdução às principais áreas da Criminalística Moderna. 4ª. ed. Campinas: Millennium.
10. Velho JA, Vilar GP, Gusmão E, Franco DP, Grochocki LR, (2020) Polícia Científica-Transformando Vestígios em Evidências. Curitiba: Intersaberes.

HERALD

Advances In Industrial Biotechnology | ISSN: 2639-5665

Advances In Microbiology Research | ISSN: 2689-694X

Archives Of Surgery And Surgical Education | ISSN: 2689-3126

Archives Of Urology

Archives Of Zoological Studies | ISSN: 2640-7779

Current Trends Medical And Biological Engineering

International Journal Of Case Reports And Therapeutic Studies | ISSN: 2689-310X

Journal Of Addiction & Addictive Disorders | ISSN: 2578-7276

Journal Of Agronomy & Agricultural Science | ISSN: 2689-8292

Journal Of AIDS Clinical Research & STDs | ISSN: 2572-7370

Journal Of Alcoholism Drug Abuse & Substance Dependence | ISSN: 2572-9594

Journal Of Allergy Disorders & Therapy | ISSN: 2470-749X

Journal Of Alternative Complementary & Integrative Medicine | ISSN: 2470-7562

Journal Of Alzheimers & Neurodegenerative Diseases | ISSN: 2572-9608

Journal Of Anesthesia & Clinical Care | ISSN: 2378-8879

Journal Of Angiology & Vascular Surgery | ISSN: 2572-7397

Journal Of Animal Research & Veterinary Science | ISSN: 2639-3751

Journal Of Aquaculture & Fisheries | ISSN: 2576-5523

Journal Of Atmospheric & Earth Sciences | ISSN: 2689-8780

Journal Of Biotech Research & Biochemistry

Journal Of Brain & Neuroscience Research

Journal Of Cancer Biology & Treatment | ISSN: 2470-7546

Journal Of Cardiology Study & Research | ISSN: 2640-768X

Journal Of Cell Biology & Cell Metabolism | ISSN: 2381-1943

Journal Of Clinical Dermatology & Therapy | ISSN: 2378-8771

Journal Of Clinical Immunology & Immunotherapy | ISSN: 2378-8844

Journal Of Clinical Studies & Medical Case Reports | ISSN: 2378-8801

Journal Of Community Medicine & Public Health Care | ISSN: 2381-1978

Journal Of Cytology & Tissue Biology | ISSN: 2378-9107

Journal Of Dairy Research & Technology | ISSN: 2688-9315

Journal Of Dentistry Oral Health & Cosmesis | ISSN: 2473-6783

Journal Of Diabetes & Metabolic Disorders | ISSN: 2381-201X

Journal Of Emergency Medicine Trauma & Surgical Care | ISSN: 2378-8798

Journal Of Environmental Science Current Research | ISSN: 2643-5020

Journal Of Food Science & Nutrition | ISSN: 2470-1076

Journal Of Forensic Legal & Investigative Sciences | ISSN: 2473-733X

Journal Of Gastroenterology & Hepatology Research | ISSN: 2574-2566

Journal Of Genetics & Genomic Sciences | ISSN: 2574-2485

Journal Of Gerontology & Geriatric Medicine | ISSN: 2381-8662

Journal Of Hematology Blood Transfusion & Disorders | ISSN: 2572-2999

Journal Of Hospice & Palliative Medical Care

Journal Of Human Endocrinology | ISSN: 2572-9640

Journal Of Infectious & Non Infectious Diseases | ISSN: 2381-8654

Journal Of Internal Medicine & Primary Healthcare | ISSN: 2574-2493

Journal Of Light & Laser Current Trends

Journal Of Medicine Study & Research | ISSN: 2639-5657

Journal Of Modern Chemical Sciences

Journal Of Nanotechnology Nanomedicine & Nanobiotechnology | ISSN: 2381-2044

Journal Of Neonatology & Clinical Pediatrics | ISSN: 2378-878X

Journal Of Nephrology & Renal Therapy | ISSN: 2473-7313

Journal Of Non Invasive Vascular Investigation | ISSN: 2572-7400

Journal Of Nuclear Medicine Radiology & Radiation Therapy | ISSN: 2572-7419

Journal Of Obesity & Weight Loss | ISSN: 2473-7372

Journal Of Ophthalmology & Clinical Research | ISSN: 2378-8887

Journal Of Orthopedic Research & Physiotherapy | ISSN: 2381-2052

Journal Of Otolaryngology Head & Neck Surgery | ISSN: 2573-010X

Journal Of Pathology Clinical & Medical Research

Journal Of Pharmacology Pharmaceutics & Pharmacovigilance | ISSN: 2639-5649

Journal Of Physical Medicine Rehabilitation & Disabilities | ISSN: 2381-8670

Journal Of Plant Science Current Research | ISSN: 2639-3743

Journal Of Practical & Professional Nursing | ISSN: 2639-5681

Journal Of Protein Research & Bioinformatics

Journal Of Psychiatry Depression & Anxiety | ISSN: 2573-0150

Journal Of Pulmonary Medicine & Respiratory Research | ISSN: 2573-0177

Journal Of Reproductive Medicine Gynaecology & Obstetrics | ISSN: 2574-2574

Journal Of Stem Cells Research Development & Therapy | ISSN: 2381-2060

Journal Of Surgery Current Trends & Innovations | ISSN: 2578-7284

Journal Of Toxicology Current Research | ISSN: 2639-3735

Journal Of Translational Science And Research

Journal Of Vaccines Research & Vaccination | ISSN: 2573-0193

Journal Of Virology & Antivirals

Sports Medicine And Injury Care Journal | ISSN: 2689-8829

Trends In Anatomy & Physiology | ISSN: 2640-7752