v. 13, n. 1, p. 143-155, 2024
ISSN 2237-9223

REVISTA BRASILEIRA DE CRIMINALÍSTICA

DOI: http://dx.doi.org/10.15260/rbc.v13i1.793

Análise de Ransomwares para identificação e extração binária de chaves criptográficas

C. Soares [a], D. Franco [a,b,*], J. Santos [a]

[a] *Pesquisador e Consultor Independente em Computação Forense e Segurança da Informação, Belém (PA), Brasil*
[b] *aCCESS Security Lab e Banco da Amazônia, Belém (PA), Brasil*

**Endereço de e-mail para correspondência: deivison.pfranco@gmail.com. Tel.: +55-91-991671922.*

Recebido em 20/10/2023; Revisado em 27/12/2023; Aceito em 03/01/2024

Resumo

Este artigo tem como objetivo mostrar o emprego da Computação Forense para recuperação da chave criptográfica de arquivos criptografados por ransomwares através da identificação, extração e análise binária de dump de memória. Dessa forma, no cenário abordado, constatou-se a possibilidade de recuperação dos arquivos criptografados através da verificação das características e do comportamento do ransomware, permitindo identificar e extrair sua chave criptográfica por meio da análise dos dados contidos em memória, com uma abordagem metodológica que pode ser empregada analogamente para outros casos semelhantes em que seja necessário recuperar ambientes atacados por esse tipo de malware.

Palavras-Chave: Forense Computacional; Ransomwares; Chaves Criptográficas; Extração Binária; Dump de Memória.

Abstract

This article aims to show the use of Computer Forensics 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: Computer Forensics; Ransomwares; Cryptographic Keys; Binary Extraction; Memory Dump.

1. INTRODUÇÃO

Ransomware é um tipo de malware que impede o acesso ao sistema infectado através do bloqueio e criptografia[1] de arquivos, cobrando resgate para reavê-los mediante pagamento com criptomoedas, o que inviabiliza a identificação e o rastreamento do criminoso. Uma vez que um sistema é infectado, o ransomware criptografa os dados do usuário em segundo plano, sem que ele perceba, e quando pronto, emite um "pop-up" informando que a máquina está bloqueada e que o usuário não poderá mais usá-la, a menos que se pague um valor para obter a chave que dá acesso aos dados.

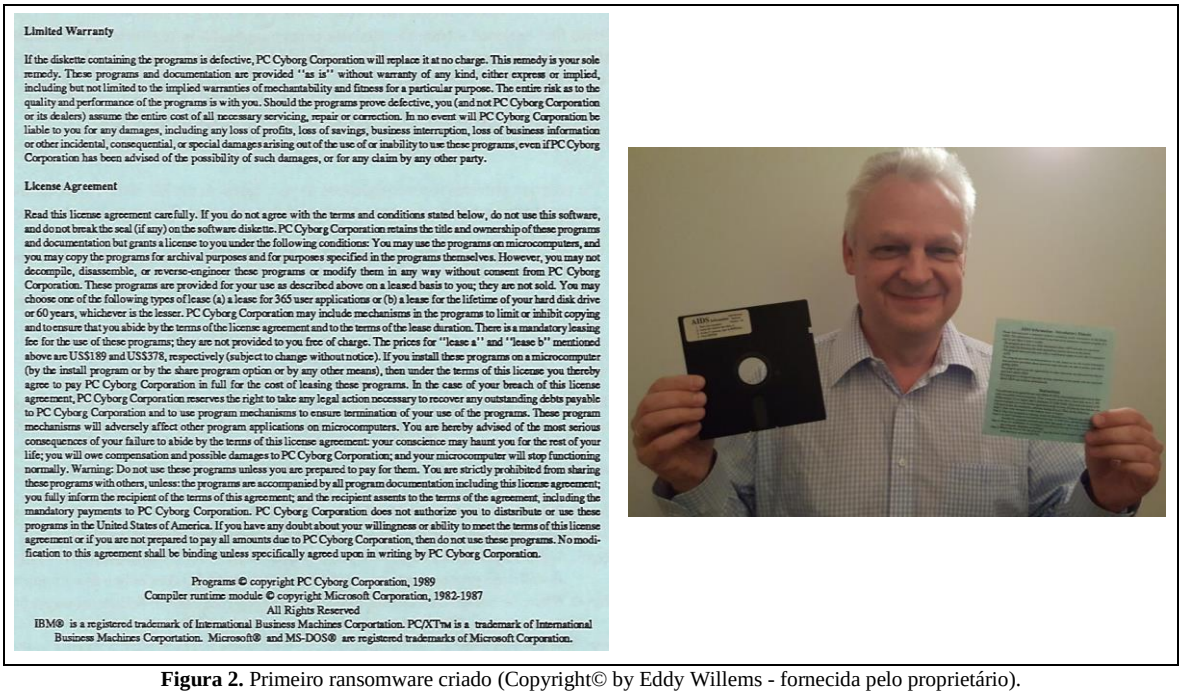
No contexto de ransomwares, a criptografia simétrica AES é geralmente usada para criptografar os arquivos da vítima, tornando-os inacessíveis sem a chave correta. Essa chave é mantida em posse dos atacantes. Alguns ransomwares também utilizam a criptografia assimétrica RSA para proteger essa chave simétrica. Nesse caso, a chave simétrica é criptografada usando a chave pública RSA do atacante e só pode ser descriptografada com a correspondente chave privada do atacante. Isso dificulta ainda mais a recuperação dos dados sem pagar o resgate exigido pelos criminosos. A Figura 1 ilustra a anatomia típica de um ataque de ransomware.

O primeiro ransomware foi criado em 1989, denominado de PC Cyborg e popularmente conhecido

[1] Na criptografia simétrica, a mesma chave é usada tanto para criptografar quanto para descriptografar os dados. Isso significa que a chave precisa ser compartilhada entre o remetente e o destinatário de forma segura. Já na criptografia assimétrica, são usadas duas chaves diferentes - uma chave pública para criptografar os dados e uma chave privada correspondente, que é mantida em segredo pelo destinatário, para descriptografá-los. Isso permite que qualquer pessoa possa enviar dados criptografados usando a chave pública, mas apenas o destinatário com a chave privada correspondente pode descriptografá-los.

como AIDS, em alusão à doença causada pelo HIV, foi desenvolvido por Joseph Popp e cobrava um resgate no valor de US$ 189. A Figura 2 mostra o primeiro ransomware.

Figura 1. Anatomia de um ataque de ransomware (Adaptado de [5]).


Limited Warranty

If the diskette containing the programs is defective, PC Cyborg Corporation will replace it at no charge. This remedy is your sole remedy. These programs and documentation are provided "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of mechantability and fitness for a particular purpose. The entire risk as to the quality and performance of the programs is with you. Should the programs prove defective, you (and not PC Cyborg Corporation or its dealers) assume the entire cost of all necessary servicing, repair or correction. In no event will PC Cyborg Corporation be liable to you for any damages, including any loss of profits, loss of savings, business interruption, loss of business information or other incidental, consequential, or special damages arising out of the use of or inability to use these programs, even if PC Cyborg Corporation has been advised of the possibility of such damages, or for any claim by any other party.

License Agreement

Read this license agreement carefully. If you do not agree with the terms and conditions stated below, do not use this software, and do not break the seal (if any) on the software diskette. PC Cyborg Corporation retains the title and ownership of these programs and documentation but grants a license to you under the following conditions: You may use the programs on microcomputers, and you may copy the programs for archival purposes and for purposes specified in the programs themselves. However, you may not decompile, disassemble, or reverse-engineer these programs or modify them in any way without consent from PC Cyborg Corporation. These programs are provided for your use as described above on a leased basis to you; they are not sold. You may choose one of the following types of lease (a) a lease for 365 user applications or (b) a lease for the lifetime of your hard disk drive or 60 years, whichever is the lesser. PC Cyborg Corporation may include mechanisms in the programs to limit or inhibit copying and to ensure that you abide by the terms of the license agreement and to the terms of the lease duration. There is a mandatory leasing fee for the use of these programs; they are not provided to you free of charge. The prices for "lease a" and "lease b" mentioned above are US$189 and US$378, respectively (subject to change without notice). If you install these programs on a microcomputer (by the install program or by the share program option or by any other means), then under the terms of this license you thereby agree to pay PC Cyborg Corporation in full for the cost of leasing these programs. In the case of your breach of this license agreement, PC Cyborg Corporation reserves the right to take any legal action necessary to recover any outstanding debts payable to PC Cyborg Corporation and to use program mechanisms to ensure termination of your use of the programs. These program mechanisms will adversely affect other program applications on microcomputers. You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement: your conscience may haunt you for the rest of your life; you will owe compensation and possible damages to PC Cyborg Corporation; and your microcomputer will stop functioning normally. Warning: Do not use these programs unless you are prepared to pay for them. You are strictly prohibited from sharing these programs with others, unless: the programs are accompanied by all program documentation including this license agreement; you fully inform the recipient of the terms of this agreement; and the recipient assents to the terms of the agreement, including the mandatory payments to PC Cyborg Corporation. PC Cyborg Corporation does not authorize you to distribute or use these programs in the United States of America. If you have any doubt about your willingness or ability to meet the terms of this license agreement or if you are not prepared to pay all amounts due to PC Cyborg Corporation, then do not use these programs. No modification to this agreement shall be binding unless specifically agreed upon in writing by PC Cyborg Corporation.

Programs © copyright PC Cyborg Corporation, 1989
Compiler runtime module © copyright Microsoft Corporation, 1982-1987
All Rights Reserved
IBM® is a registered trademark of International Business Machines Corportation. PC/XT™ is a trademark of International Business Machines Corportation. Microsoft® and MS-DOS® are registered trademarks of Microsoft Corporation.

Figura 2. Primeiro ransomware criado (Copyright© by Eddy Willems - fornecida pelo proprietário).

2. PROCESSO DE ANÁLISE FORENSE COMPUTACIONAL

O trabalho pericial é pautado em doutrinas e procedimentos técnico-científicos, que visam à preservação e a integridade da prova. No caso específico da computação, a manipulação dos dados contidos em mídias de armazenamento computacional deve ser realizada com toda atenção possível, pois a prova não pode ter seu estado inicial alterado, ou seja, nenhum bit pode ser modificado. Isso garante a validade da prova em juízo. Assim, o investigador deve sempre utilizar equipamentos e softwares forenses. Para se ter uma ideia da sensibilidade das evidências digitais, apenas ao ligar um computador e aguardar seu sistema operacional ser inicializado, dados contidos no disco rígido já são alterados.

O processo de investigação de crimes cibernéticos, isto é, o processo de perícia digital consiste em quatro fases que tratam desde o recebimento do material à elaboração do laudo, quais sejam: Coleta/Preservação; Extração/Exame; Análises Periciais e Formalização/Resultados. Todo esse procedimental é ilustrado na Figura 3 e explicado a seguir.

Figura 3. Processo da Análise Forense Computacional.

2.1. Coleta / Preservação

Esta fase é considerada vital para o processo, pois é nela que toda a massa crítica de dados será coletada, sendo necessário cuidado especial para manter a integridade das informações. Por isso, os exames devem, sempre que possível, ser realizados em cópias fiéis obtidas a partir do material original, utilizando técnicas de espelhamento ou de imagem, nas quais é recomendável a aplicação de funções hash[2] sobre partes e/ou todo o conteúdo do dispositivo de armazenamento, a fim de registrar o conteúdo presente no material examinado. Tal procedimento visa garantir a integridade das evidências.

2.2. Extração / Exame

Nesta fase o objetivo principal é separar dados e informações relevantes ao caso. Antes de iniciar esse processo é preciso definir quais as ferramentas que serão utilizadas para o exame dos dados. Essa escolha está relacionada a cada tipo de investigação e informações que estão sendo procuradas.

Nessa etapa, deve ser realizada a recuperação dos arquivos eventualmente apagados, uma vez que o sistema operacional tem apenas um controle de quais partes do disco rígido estão livres e quais estão ocupadas. Assim, técnicas apropriadas devem ser aplicadas no conteúdo da mídia, fazendo com que tais arquivos sejam acessíveis para as análises periciais subsequentes.

2.3. Análises periciais

Na terceira fase, praticamente paralela à anterior, os dados e informações anteriormente separados serão analisados com o intuito de encontrar informações úteis e relevantes que auxiliem na investigação do caso. Todos os dados/informações encontradas consideradas relevantes devem ser correlacionados com informações referentes à investigação, para que assim seja possível reconstruir os eventos, estabelecer o nexo causal e realizar a conclusão – provar a materialidade do fato.

Essa é a principal fase do exame pericial e a que exige maior esforço, cuidado e capacidade técnica do investigador, pois requer especial atenção quanto a arquivos protegidos por senha, criptografia ou ocultos, além do exame de possíveis sistemas e programas existentes no dispositivo examinado.

2.4. Formalização / Resultados

Nesta última etapa, o objetivo é reunir todas as evidências coletadas, examinadas e analisadas, a fim de se apresentar um laudo que deve informar com toda a veracidade possível o que foi encontrado nos dados analisados, para que se prove o nexo causal, garantindo-se a materialidade do fato crime – prova irrefutável. Todo o processo pericial desde o início, ferramentas/técnicas e informações que comprovem a integridade das informações deve ser relatado no laudo.

3. ISOLAMENTO DE VESTÍGIOS CIBERNÉTICOS

Para [7], o isolamento, embora geralmente considerado como uma etapa a seguir à identificação e registro, na prática pode ocorrer simultaneamente. Portanto, à medida que os itens são identificados na cena do crime, medidas podem ser tomadas para garantir seu isolamento e, dessa forma, a principal finalidade do isolamento é prevenir ataques à integridade das evidências, como alterações, supressões, inserções ou destruições. Dada a natureza especial do vestígio cibernético, dividimos o isolamento em duas categorias: física e lógica.

[2] Funções matemáticas de via única que geram uma saída de tamanho fixo a partir de uma entrada de tamanho variável que visam criar uma representação resumida de arquivos ou mensagens para garantia de inforjabilidade da integridade de seu conteúdo.

3.1. Isolamento físico

Compreender o perímetro físico e estabelecer sua delimitação para realizar o isolamento pode parecer simples, mas é uma tarefa complexa. Qual seria o tamanho ideal da área a ser isolada para abarcar todos os vestígios? A diretriz é isolar a maior extensão possível dentro do contexto do crime, uma vez que um isolamento feito em uma área menor pode contaminar a região não abrangida e ocasionar a perda de vestígios cruciais.

É importante ressaltar que o ser humano não é o único agente que modifica o ambiente; há outros fatores a serem considerados, como condições climáticas adversas (frio, chuva, umidade, calor, luz solar, vento, radiação magnética etc.). Dependendo da localidade, medidas adicionais podem ser necessárias para identificar e isolar os vestígios prontamente. Portanto, de acordo com [7], algumas classificações dos locais se tornam imprescindíveis, as quais serão tratadas a seguir.

3.1.1. Quanto à Região

a) Imediato: área onde há uma elevada concentração de vestígios relacionados ao incidente em questão. Nesse local, serão realizadas investigações mais minuciosas, visto que, segundo o princípio da localização espacial de referência, é provável que a maioria das evidências esteja presente ali.

b) Mediato: área delimitada pelos arredores da zona imediata. Assim como na área imediata, há a chance de haver mais de uma área adjacente.

3.1.2. Quanto à Preservação

a) Idôneo: local onde as evidências permaneceram sem alterações desde que o incidente ocorreu até serem oficialmente registradas.

b) Inidôneo: local onde os vestígios foram afetados devido à remoção, inserção ou a uma combinação de ambas as ações.

3.1.3. Quanto à Área

a) Interno: apresenta ao menos uma forma de proteção contra chuva, sol e outros elementos naturais mais severos. Mesmo sem paredes, mas delimitando o espaço, não o exclui dessa categoria, como um galpão sem paredes ou a entrada de um prédio, por exemplo.

b) Externo: localizado fora das estruturas convencionais e está diretamente exposto aos elementos naturais mais adversos. Esses espaços podem incluir cabos de rede, antenas transmissoras/receptoras de sinais, dispositivos de autenticação biométrica, entre outros.

c) Virtual: não possui uma conexão direta entre o contexto físico e o lógico. Uma atividade realizada em um ambiente físico específico pode gerar evidências físicas e lógicas em outro local totalmente diferente.

3.1.4. Quanto à Natureza

Espaço categorizado com base no tipo de evento relacionado a ele, como por exemplo: casos de pedofilia, inserção de informações em sistemas de computador, invasões de redes, entre outros.

3.2. Isolamento Lógico

Os procedimentos adequados serão determinados pela natureza do dispositivo que precisa ser isolado para posterior apreensão. A seguir, são ressaltadas as categorias mais frequentes de dispositivos encontrados em cenas de crimes digitais.

3.2.1. Notebooks e Desktops

Na maioria das situações, as informações mais cruciais para serem isoladas geralmente residem em dispositivos de armazenamento secundários, como HDs, pendrives, HDs externos, entre outros. Isso significa que somente esses dispositivos de armazenamento precisam ser isolados para posterior coleta.

Em certos casos, a máquina como um todo deve ser identificada e isolada para esse propósito, como ocorre em sistemas que usam arranjos de disco RAID[3]. Nesses arranjos, fisicamente encontramos vários HDs, mas logicamente eles funcionam como um único disco.

Ainda para [7], outro fator a ser considerado é o estado em que esses dispositivos se encontram: se estão ligados ou desligados.

a) Ligado: se o dispositivo estiver ligado e o sistema operacional estiver ativo, é crucial verificar se é possível registrar a evidência em situações de flagrância. A coleta de dados da memória principal, que geralmente é volátil, deve ser considerada. Isso inclui arquivos compartilhados, programas em execução, janelas abertas, atividades de navegação, conversas em aplicativos de comunicação e informações descriptografadas durante a leitura (mas criptografadas quando armazenadas em dispositivos de armazenamento secundários). No entanto, é importante notar que ao desligar o sistema nesse estado, é recomendado não seguir os procedimentos normais de encerramento do sistema operacional, pois eles podem comprometer a integridade das evidências ao associarem-se a eventos indesejados.

b) Desligado: normalmente, é recomendado manter o dispositivo nessas condições sem ligá-lo, pois a inicialização do sistema operacional pode alterar partes específicas dos dados armazenados na mídia secundária, e alguns programas em execução podem realizar ações indesejadas, comprometendo assim a integridade das evidências. Se for necessário realizar análises nesse tipo

[3] Forma de se criar um subsistema de armazenamento composto por vários discos individuais, com a finalidade de ganhar segurança e desempenho através da redundância de dados.

de mídia no local, é crucial tomar medidas de proteção contra escrita. Uma solução comum é inicializar o sistema por meio de outro sistema operacional armazenado em outra mídia, o que evita realizar alterações na mídia original em questão.

3.2.2. Dispositivos de Entrada/Saída

De acordo com [7], certos itens não são coletados como evidências, mas em casos específicos, sua identificação e isolamento são vitais para resolver o caso. Por exemplo, um cenário hipotético inclui a identificação de um teclado com defeito em teclas específicas, usado para digitar e-mails difamatórios anônimos, ou uma impressora responsável pela produção de certidões fraudulentas. Além disso, dispositivos como scanners utilizados na criação de imagens para falsificações de moeda também devem ser considerados.

Devido aos seus formatos de conexão e padrões, os cabos, acessórios e carregadores devem ser identificados como parte integrante do equipamento para fins de coleta de evidências.

3.2.3. Mídias Avulsas

Essa categoria engloba principalmente todos os tipos de dispositivos de armazenamento externo de computadores, como CDs, pendrives, HDs externos, cartões de memória, disquetes, zip-drives, entre outros. Esses dispositivos podem ser encontrados conectados ou desconectados dos computadores. Às vezes, são localizados dentro de seus dispositivos originais, como câmeras de vídeo ou máquinas fotográficas (Vilar e Gusmão, 2016).

É importante lembrar que, apesar de estarem em uma filmadora ou câmera, a memória presente nesses dispositivos age como qualquer outro tipo de armazenamento, podendo conter diversos tipos de arquivos além de fotos e vídeos.

3.2.4. Cópias de Dados in Loco

Ainda nas considerações de [7], se durante a identificação for percebido que um dispositivo é importante, mas a evidência digital pode ser extraída sem coletar o suporte físico, cópias podem ser feitas no local para futura análise. Essas cópias são feitas para lidar com problemas técnicos ou legais que impedem a coleta, ou para reduzir a quantidade de materiais a serem coletados.

A autenticidade e a integridade dos dados coletados, como logs, configurações do sistema operacional, arquivos de sistema e de usuário, serão asseguradas preservando a estrutura de diretórios original e os metadados[4] dos arquivos, como data, hora de criação e permissões. Se possível, recomenda-se gerar resumos criptográficos (hashes).

3.2.5 Equipamentos Conectados em Rede

Seguindo nos apontamentos de [7], estes equipamentos precisam ser registrados e devem ser desconectados da rede, seja através da remoção do cabo ou desligamento do dispositivo. Em certos casos, pode ser necessário isolar os elementos de rede, como switches ou roteadores, como evidência do crime. As informações e configurações armazenadas nesses dispositivos frequentemente servem como provas.

É fundamental prestar atenção especial às redes sem fio, já que a ausência de cabos não indica a inexistência de redes de computadores. É necessário identificar os pontos de acesso às redes sem fio ou até mesmo a configuração de redes ad-hoc[5].

4. ANÁLISE FORENSE COMPUTACIONAL DE RANSOMWARE PARA IDENTIFICAÇÃO E EXTRAÇÃO BINÁRIA DE CHAVE CRIPTOGRÁFICA

4.1. Cenário Analisado

Analisou-se o cenário no qual um usuário executou um artefato malicioso[6] que criptografou todos os seus arquivos, o qual foi replicado em laboratório virtualizado, onde foi desenvolvido um ambiente de Comando e Controle[7] (C2) contendo o ransomware codificado que, ao ser executado, criptografa os dados do hospedeiro e encaminha sua chave criptográfica para o C2, conforme esquema da Figura 4 e execução mostrada na Figura 5.

4.2 Procedimentos Iniciais

Após o ocorrido, os times de resposta a incidente e perícia forense devem atuar rapidamente seguindo metodologias próprias ou de mercado para impedir e/ou minimizar danos. Portanto, evitar a tomada de decisões pode prejudicar a criação de gráficos forenses, ou a identificação das causas raiz, ou a criação de uma base de conhecimento consistente.

A máquina comprometida foi isolada de sua infraestrutura, mantida ligada e nela executado um live CD GNU/Linux com a distribuição Forense CAINE (CAINE Live USB/DVD[8]), que possui várias ferramentas.

[4] São dados sobre outros dados, elementos que podem dizer do que se trata aquele dado. Geralmente uma informação inteligível por um computador que facilitam o entendimento dos relacionamentos e a utilidade das informações dos dados.

[5] Redes que não utilizam dispositivos concentradores sem fio para intercomunicação dos dispositivos e que realizam a comunicação diretamente entre si através das próprias interfaces de rede.

[6] Nota dos Autores: foi utilizado o ransomware "Hidden Tear", cujo sample está disponível em https://github.com/carlosbsdev/hiddentear.

[7] C2 é um centro de controle, isto é, um ambiente computacional controlado por um cibercriminoso, utilizado de forma maliciosa para controlar sistemas comprometidos, sendo também empregados no recebimento de dados do atacante e das máquinas comprometidas.

[8] https://www.caine-live.net/

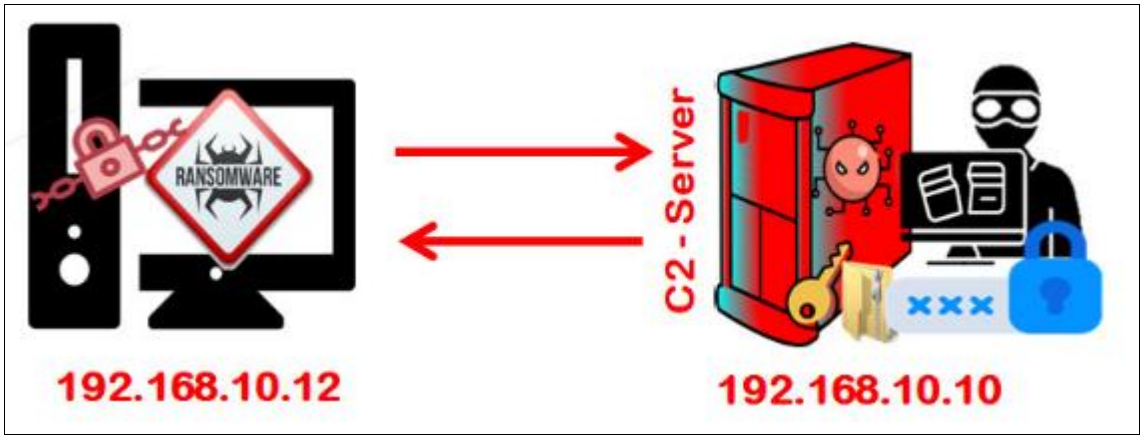


Figura 4. Esquema do cenário analisado.

Figura 5. Execução do ransomware.

Dentre o ferramental da distribuição, utilizou-se o FTK Imager[9] - software forense desenvolvido pela empresa Access Data[10] que cria cópias binárias de disco, faz dump de memória, além de possuir uma interface gráfica que auxilia no processo de análise forense das imagens dumpadas. Sendo assim, seguiu-se os procedimentos operacionais para análise forense computacional do ransomware para identificação e extração binária de sua chave criptográfica.

Baixou-se o FTK Imager Lite[11] e, após o download, acessou-se a pasta "FTKImagerLite" e executou-se o aplicativo "FTKImagerLite.exe", conforme mostrado nas Figuras 6 e 7.

Após a execução do FTK Imager, clicou-se no menu "File" e selecionou-se a opção "Capture Memory", conforme mostrado na Figura 8.

Abriu-se uma janela e nela, na opção "Destination path", escolheu-se onde salvar o dump de memória e em "Destination filename", nomeou-se o arquivo do dump como "memdump.mem", sendo que as opções de incluir um arquivo de paginação ("Include pagefile"[12]) e de criar um arquivo AD1 ("Create AD1 file"[13]) não foram utilizadas nesta etapa.

[9] https://accessdata.com/product-download/ftk-imager-version-4-5
[10] https://accessdata.com/
[11] https://accessdata.com/product-download/how-to-run-ftk-imager-from-a-flash-drive-imager-lite

[12] Arquivo de memória virtual para auxiliar o processo de dump de memória.
[13] Extensão dos arquivos de imagem criados pelo FTK Imager.

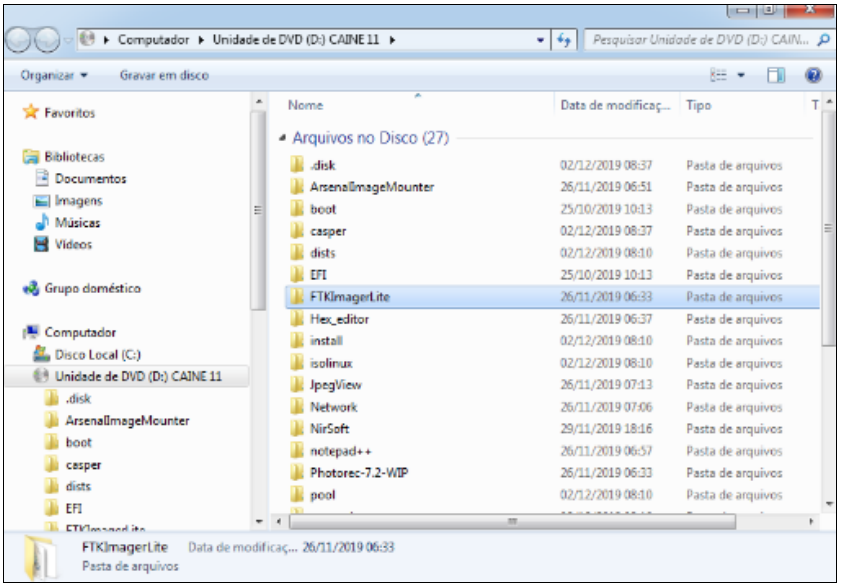


Figura 6. Pasta do aplicativo “FTKImagerLite”.

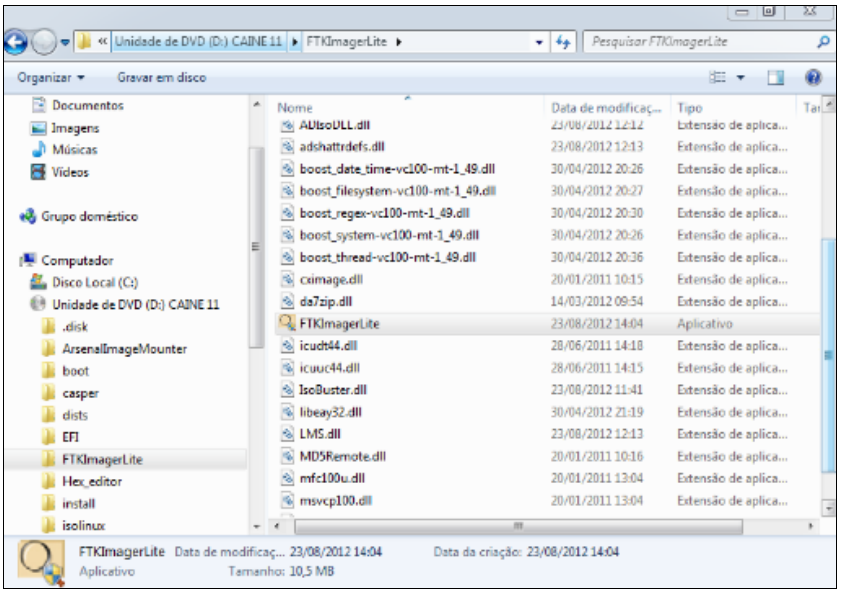


Figura 7. Aplicativo “FTKImagerLite.exe”.

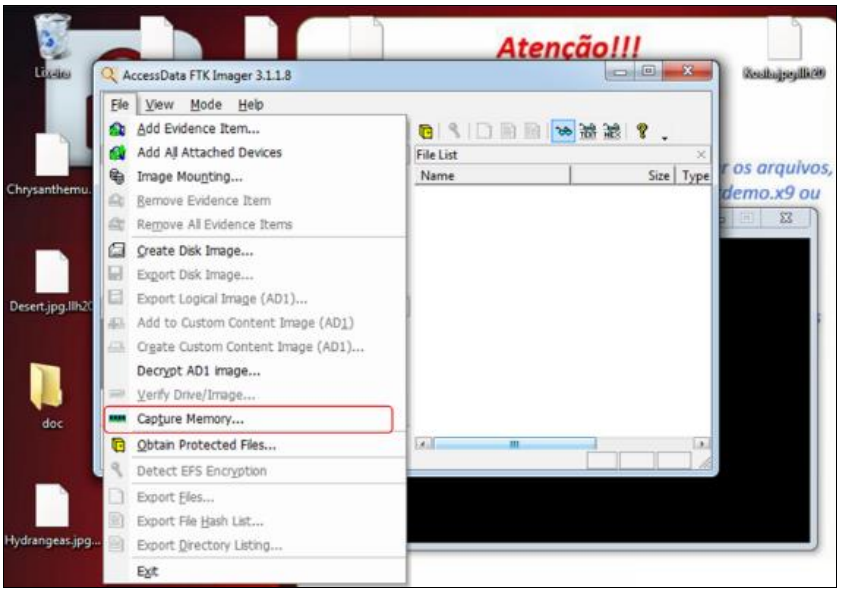


Figura 8. Opção “Capture Memory”.

Feito isso, clicou-se em “Capture Memory”, conforme mostrado na Figura 9 (uma observação muito válida é que se o sistema operacional tiver muita memória, o processo pode demorar um pouco).

Após a finalização do procedimento, clicou-se no botão "Close” como mostrado na Figura 10.

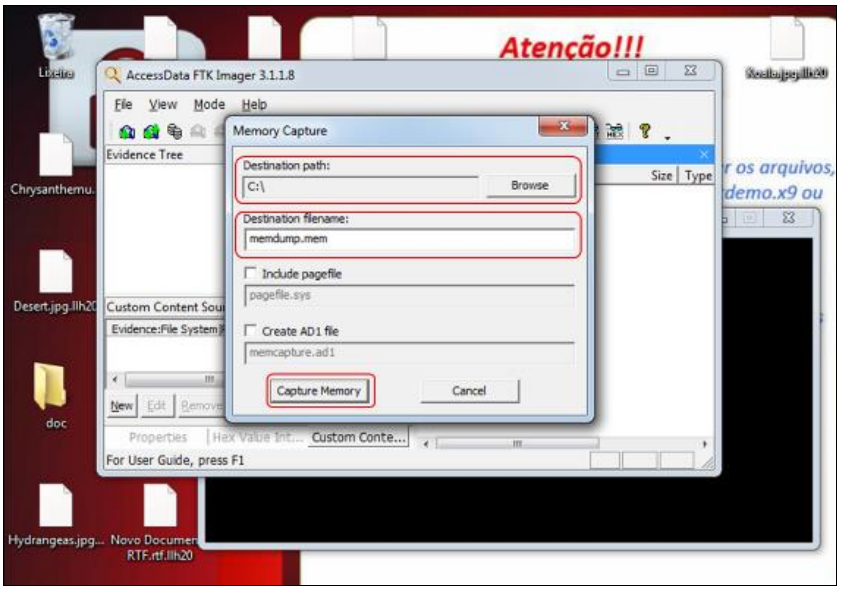


Figura 9. Configuração da opção “Capture Memory”.

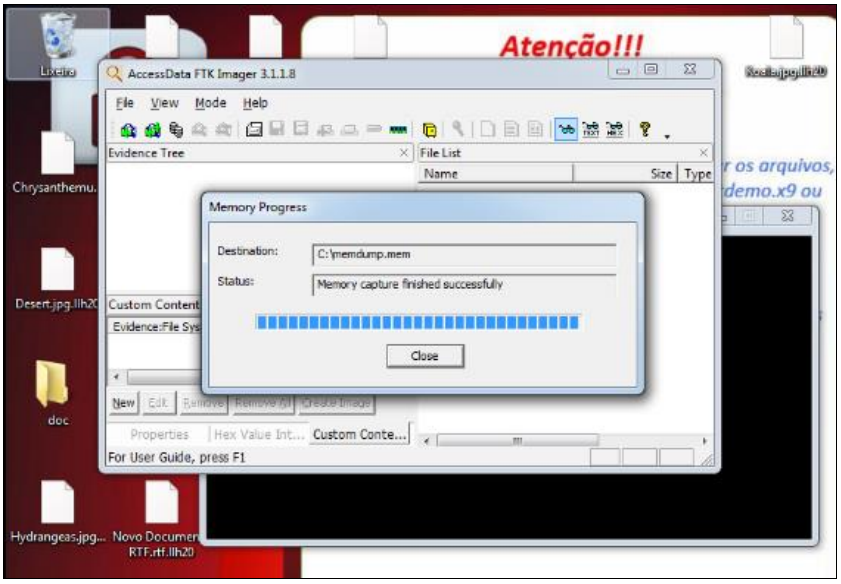


Figura 10. Execução da opção “Capture Memory”.

Com o arquivo de saída na pasta de destino selecionada, removeu-se a mídia para análise do dump em outro equipamento.

Na próxima etapa utilizou-se o Volatility[14] - ferramenta de linha de comando desenvolvida em python e uma das mais utilizadas para análise de memória, contendo diversos plugins para sistemas Windows, Linux e Mac.

4.3. Identificação e Extração Binária de Chave Criptográfica

Não existe nem um passo a passo a ser seguido, pois a ferramenta permite a extração e análise de informações úteis da memória, como processos em execução e conexões de rede, possibilitando, ainda, descartar DLLs[15] e processos para análise posterior, cabendo ao investigador avaliar o que é mais útil para sua análise. A seguir, os procedimentos realizados e os comandos executados para o cenário em análise.

Primeiramente, verificou-se as informações da ferramenta que mostram seus comandos e as versões de sistema operacional que a suportam através da opção

[14] https://github.com/volatilityfoundation/volatility

[15] Dynamic-Link Library, ou Biblioteca de Link Dinâmico, são implementações feitas pela Microsoft para bibliotecas compartilhadas nos sistemas operacionais Windows.

"info", mostrada na Figura 11.

Em seguida, para análise de informações sobre despejos de memória, utilizou-se a opção "imageinfo", como mostra a Figura 12.

Após, para verificar os processos que estavam sendo executados no sistema operacional, utilizou-se o plugin "pslist", com o comando apresentado na Figura 13.

 # volatility --info

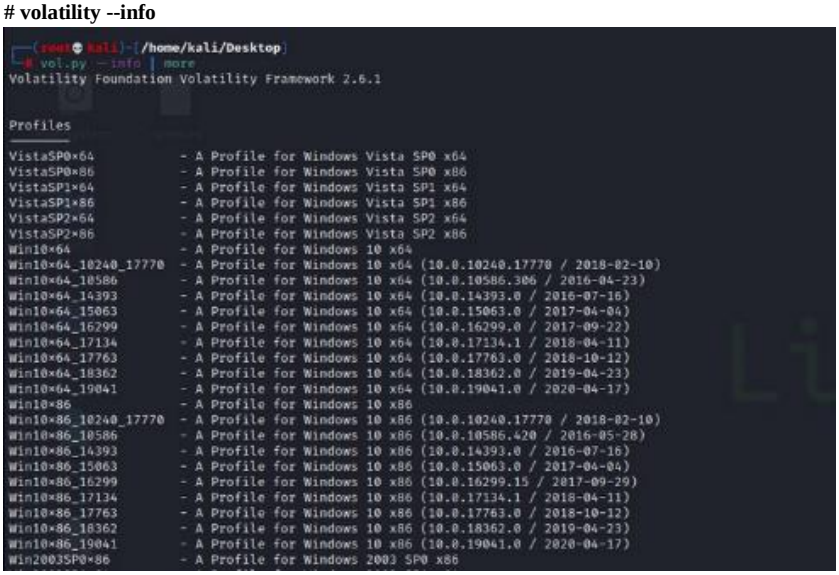


Figura 11. Execução do comando "**volatility --info**".

 # volatility imageinfo -f memdump.mem

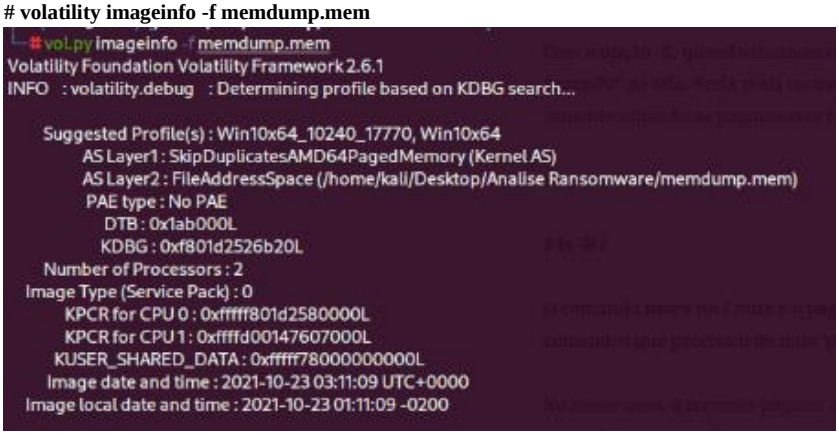


Figura 12. Execução do comando "**volatility imageinfo -f memdump.mem**".

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

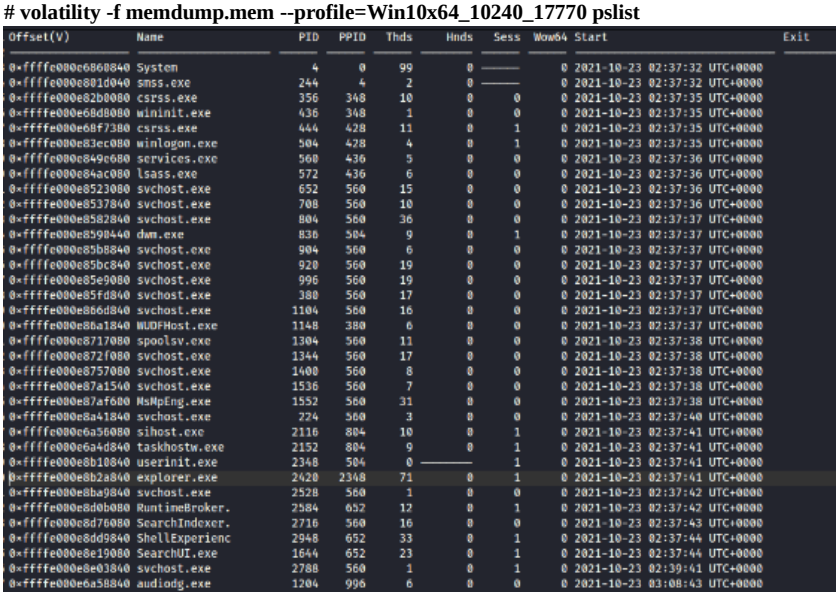


Figura 13. Execução do comando "**volatility -f memdump.mem --profile=Win10x64_10240_17770 pslist**".

Uma opção do plugin “pslist”, que pode ser usada para exibir os processos pais e filhos, é o “pstree”, que foi empregada conforme mostrado na Figura 14.

Em seguida, utilizou-se o plugin “psxview” para listar os processos que estão tentando se ocultar no computador, como mostra a Figura 15.

Após verificar os processos em execução, outro ponto fundamental é analisar as conexões relacionadas a eles. Para isso, executou-se o comando “netscan” que mostrou que houve uma conexão entre a máquina 192.168.10.12, com status “close”, com o C2 do atacante 192.168.10.10, como mostrado na Figura 16, a seguir.

Apesar de haver evidências de conexão, aparentemente não foi encontrado nenhum processo suspeito. Então, foi preciso analisar melhor alguns artefatos mais específicos, pois é característico de malwares se injetarem em processos legítimos.

Dado o exposto, para validar os Identificadores de Segurança (SIDs), utilizou-se o comando “getsids” para identificar os processos associados a um determinado usuário e que possam ter privilégios que podem ser maliciosamente escalados e, dentre os vários processos, observou-se que o processo 2420 estava sendo executado por vários usuários, em particular pelo usuário “srvmaster” conforme é trazido na Figura 17.

Sendo assim, com base nos resultados dos comandos “pstree” e “pslist”, utilizou-se o comando “memdump” no processo 2420 para extrair todas as suas informações e despejá-las em um arquivo específico com o comando “-p 2420” seguido da opção “-dump-dir” (diretório onde se quer extrair o despejo), tal como é mostrado na Figura 18.

Feito isso, com o comando “strings”, redirecionou-se o conteúdo do despejo para um arquivo com o parâmetro “>”, como mostra a Figura 19.

Após análise minuciosa do binário identificado e extraído, foi possível identificar a comunicação do computador com o Comando e Controle do atacante, incluindo algumas informações da máquina, como um password que é a chave para descriptografar os arquivos, como apresentado na Figura 20.

Sendo assim, no ambiente que foi replicado, foi possível identificar todas as informações do equipamento presente no C2 do atacante, incluindo a senha de resgate, conforme pode ser constatado na Figura 21.

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

```
# vol.py -f memdump.mem --profile=Win10x64_10240_17770 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
0xffffe000e68d8080:wininit.exe                        436    348      1      0 2021-10-23 02:37:35 UTC+0000
. 0xffffe000e84ac080:lsass.exe                        572    436      6      0 2021-10-23 02:37:36 UTC+0000
. 0xffffe000e849e680:services.exe                     560    436      5      0 2021-10-23 02:37:36 UTC+0000
.. 0xffffe000e87a1540:svchost.exe                    1536    560      7      0 2021-10-23 02:37:38 UTC+0000
.. 0xffffe000e85b8840:svchost.exe                     904    560      6      0 2021-10-23 02:37:37 UTC+0000
.. 0xffffe000e8523080:svchost.exe                     652    560     15      0 2021-10-23 02:37:36 UTC+0000
... 0xffffe000e8d0b080:RuntimeBroker.                2584    652     12      0 2021-10-23 02:37:42 UTC+0000
... 0xffffe000e8602640:dllhost.exe                   1924    652      8      0 2021-10-23 03:11:10 UTC+0000
... 0xffffe000e8dd9840:ShellExperienc                2948    652     33      0 2021-10-23 02:37:44 UTC+0000
... 0xffffe000e8e19080:SearchUI.exe                  1644    652     23      0 2021-10-23 02:37:44 UTC+0000
.. 0xffffe000e87af600:MsMpEng.exe                    1552    560     31      0 2021-10-23 02:37:38 UTC+0000
.. 0xffffe000e8717080:spoolsv.exe                    1304    560     11      0 2021-10-23 02:37:38 UTC+0000
.. 0xffffe000e8e03840:svchost.exe                    2788    560      1      0 2021-10-23 02:39:41 UTC+0000
.. 0xffffe000e85bc840:svchost.exe                     920    560     19      0 2021-10-23 02:37:37 UTC+0000
.. 0xffffe000e8d76080:SearchIndexer.                 2716    560     16      0 2021-10-23 02:37:43 UTC+0000
... 0xffffe000e78e9080:SearchFilterHo                 988   2716      6      0 2021-10-23 03:10:14 UTC+0000
... 0xffffe000e8855080:SearchProtocol                1936   2716      9      0 2021-10-23 03:10:14 UTC+0000
.. 0xffffe000e8582840:svchost.exe                     804    560     36      0 2021-10-23 02:37:37 UTC+0000
... 0xffffe000e6a56080:sihost.exe                    2116    804     10      0 2021-10-23 02:37:41 UTC+0000
... 0xffffe000e6a4d840:taskhostw.exe                 2152    804      9      0 2021-10-23 02:37:41 UTC+0000
.. 0xffffe000e872f080:svchost.exe                    1344    560     17      0 2021-10-23 02:37:38 UTC+0000
.. 0xffffe000e8ba9840:svchost.exe                    2528    560      1      0 2021-10-23 02:37:42 UTC+0000
.. 0xffffe000e8537840:svchost.exe                     708    560     10      0 2021-10-23 02:37:36 UTC+0000
.. 0xffffe000e866d840:svchost.exe                    1104    560     16      0 2021-10-23 02:37:37 UTC+0000
.. 0xffffe000e85e9080:svchost.exe                     996    560     19      0 2021-10-23 02:37:37 UTC+0000
... 0xffffe000e6a58840:audiodg.exe                   1204    996      6      0 2021-10-23 03:08:43 UTC+0000
.. 0xffffe000e8599080:NisSrv.exe                     2396    560     10      0 2021-10-23 03:10:13 UTC+0000
.. 0xffffe000e8a41840:svchost.exe                     224    560      3      0 2021-10-23 02:37:40 UTC+0000
.. 0xffffe000e85fd840:svchost.exe                     380    560     17      0 2021-10-23 02:37:37 UTC+0000
... 0xffffe000e86a1840:WUDFHost.exe                  1148    380      6      0 2021-10-23 02:37:37 UTC+0000
.. 0xffffe000e777f080:svchost.exe                    3440    560     11      0 2021-10-23 03:08:44 UTC+0000
.. 0xffffe000e8757080:svchost.exe                    1400    560      8      0 2021-10-23 02:37:38 UTC+0000
0xffffe000e82b0080:csrss.exe                          356    348     10      0 2021-10-23 02:37:35 UTC+0000
0xffffe000e6860840:System                               4      0     99      0 2021-10-23 02:37:32 UTC+0000
. 0xffffe000e801d040:smss.exe                         244      4      2      0 2021-10-23 02:37:32 UTC+0000
0xffffe000e68f7380:csrss.exe                          444    428     11      0 2021-10-23 02:37:35 UTC+0000
0xffffe000e83ec080:winlogon.exe                       504    428      4      0 2021-10-23 02:37:35 UTC+0000
. 0xffffe000e8590440:dwm.exe                          836    504      9      0 2021-10-23 02:37:37 UTC+0000
. 0xffffe000e8b10840:userinit.exe                    2348    504      0 ------ 2021-10-23 02:37:41 UTC+0000
.. 0xffffe000e8b2a840:explorer.exe                   2420   2348     71      0 2021-10-23 02:37:41 UTC+0000
```

Figura 14. Execução do comando “**volatility -f memdump.mem --profile=Win10x64_10240_17770 pstree**”.

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

```
Offset(P)          Name                PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
------------------ -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------

0x000000007e2d8080 wininit.exe          436 True  True  True   True  True  True  False
0x0000000009f9f680 services.exe         560 True  True  True   True  True  True  False
0x00000000119b4080 NisSrv.exe          2396 True  True  True   True  True  True  False
0x000000001cd87840 svchost.exe          224 True  True  True   True  True  True  False
0x0000000010964080 svchost.exe          652 True  True  True   True  True  True  False
0x000000007ca56080 sihost.exe          2116 True  True  True   True  True  True  False
0x0000000010ba9840 svchost.exe          708 True  True  True   True  True  True  False
0x0000000007d38080 svchost.exe         3440 True  True  True   True  True  True  False
0x000000001bd6b840 ShellExperienc      2948 True  True  True   True  True  True  False
0x000000000197a080 spoolsv.exe         1304 True  True  True   True  True  True  False
0x0000000008f3b080 winlogon.exe         504 True  True  True   True  True  True  False
0x000000002837c080 SearchUI.exe        1644 True  True  True   True  True  True  False
0x000000001289d080 svchost.exe          996 True  True  True   True  True  True  False
0x0000000011a16440 dwm.exe              836 True  True  True   True  True  True  False
0x0000000275524c0 conhost.exe          1636 True  True  True   True  True  True  False
0x0000000022887840 svchost.exe         2528 True  True  True   True  True  True  False
0x0000000016055540 svchost.exe         1536 True  True  True   True  True  True  False
0x000000001795a080 SearchProtocol      1936 True  True  True   True  True  True  False
0x0000000012c41840 svchost.exe          380 True  True  True   True  True  True  False
0x000000000c14600 MsMpEng.exe          1552 True  True  True   True  True  True  False
0x0000000012dc6640 dllhost.exe         1924 True  True  True   False True  True  False
0x0000000011e7f840 svchost.exe          920 True  True  True   True  True  True  False
0x000000007ca58840 audiodg.exe         1204 True  True  True   True  True  True  False
0x0000000001aa5080 svchost.exe         1400 True  True  True   True  True  True  False
0x000000000114b2840 svchost.exe         804 True  True  True   True  True  True  False
0x0000000027026080 SearchIndexer.      2716 True  True  True   True  True  True  False
0x0000000022e87080 RuntimeBroker.      2584 True  True  True   True  True  True  False
0x0000000033f1b840 svchost.exe         2788 True  True  True   True  True  True  False
0x0000000021f18840 explorer.exe        2420 True  True  True   True  True  True  False
0x0000000014266840 svchost.exe         1104 True  True  True   True  True  True  False
```

Figura 15. Execução do comando "**volatility -f memdump.mem --profile=Win10x64_10240_17770 psxview**".

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

```
# vol.py -f memdump.mem --profile=Win10x64_10240_17770 netscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0xe000e6a33310     UDPv4    0.0.0.0:4500                   *:*                                   804      svchost.exe    2021-10-23 02:37:40 UTC+0000
0xe000e6a3b620     UDPv4    0.0.0.0:500                    *:*                                   804      svchost.exe    2021-10-23 02:37:40 UTC+0000
0xe000e6a53b80     UDPv4    0.0.0.0:0                      *:*                                   804      svchost.exe    2021-10-23 02:37:40 UTC+0000
0xe000e6a55c00     UDPv4    0.0.0.0:0                      *:*                                   224      svchost.exe    2021-10-23 02:37:40 UTC+0000
0xe000e6a55c00     UDPv6    ::0                            *:*                                   224      svchost.exe    2021-10-23 02:37:40 UTC+0000
0xe000e6a5bbb0     UDPv4    0.0.0.0:0                      *:*                                   224      svchost.exe    2021-10-23 02:37:40 UTC+0000
0xe000e6a61ec0     UDPv4    0.0.0.0:0                      *:*                                   804      svchost.exe    2021-10-23 02:37:41 UTC+0000
0xe000e6a61ec0     UDPv6    ::0                            *:*                                   804      svchost.exe    2021-10-23 02:37:41 UTC+0000
0xe000e6a40850     TCPv4    0.0.0.0:49412                  0.0.0.0:0            LISTENING        560      services.exe   2021-10-23 02:37:41 UTC+0000
0xe000e6a40850     TCPv6    ::49412                        ::0                  LISTENING        560      services.exe   2021-10-23 02:37:41 UTC+0000
0xe000e6b69ae0     TCPv4    192.168.10.12:49414            192.168.10.10:80     CLOSED           3884579624               2021-10-23 03:10:15 UTC+0000
0xe000e7cb1ec0     UDPv4    127.0.0.1:1900                 *:*                                   904      svchost.exe    2021-10-23 02:37:43 UTC+0000
0xe000e869b480     UDPv4    0.0.0.0:4500                   *:*                                   804      svchost.exe    2021-10-23 02:37:40 UTC+0000
0xe000e869b480     UDPv6    ::4500                         *:*                                   804      svchost.exe    2021-10-23 02:37:40 UTC+0000
0xe000e86a7c90     UDPv4    0.0.0.0:500                    *:*                                   804      svchost.exe    2021-10-23 02:37:40 UTC+0000
0xe000e86a7c90     UDPv6    ::500                          *:*                                   804      svchost.exe    2021-10-23 02:37:40 UTC+0000
0xe000e8544550     TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        708      svchost.exe    2021-10-23 02:37:36 UTC+0000
0xe000e85454d0     TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        708      svchost.exe    2021-10-23 02:37:36 UTC+0000
0xe000e85454d0     TCPv6    :::135                         :::0                 LISTENING        708      svchost.exe    2021-10-23 02:37:36 UTC+0000
0xe000e8548070     TCPv4    0.0.0.0:49408                  0.0.0.0:0            LISTENING        436      wininit.exe    2021-10-23 02:37:36 UTC+0000
0xe000e8549ec0     TCPv4    0.0.0.0:49408                  0.0.0.0:0            LISTENING        436      wininit.exe    2021-10-23 02:37:36 UTC+0000
0xe000e8549ec0     TCPv6    :::49408                       :::0                 LISTENING        436      wininit.exe    2021-10-23 02:37:36 UTC+0000
0xe000e85fa230     TCPv4    0.0.0.0:49412                  0.0.0.0:0            LISTENING        560      services.exe   2021-10-23 02:37:41 UTC+0000
0xe000e863e5d0     TCPv4    0.0.0.0:49409                  0.0.0.0:0            LISTENING        996      svchost.exe    2021-10-23 02:37:37 UTC+0000
0xe000e86478c0     TCPv4    0.0.0.0:49409                  0.0.0.0:0            LISTENING        996      svchost.exe    2021-10-23 02:37:37 UTC+0000
0xe000e86478c0     TCPv6    :::49409                       :::0                 LISTENING        996      svchost.exe    2021-10-23 02:37:37 UTC+0000
0xe000e86af1b0     TCPv4    0.0.0.0:49410                  0.0.0.0:0            LISTENING        804      svchost.exe    2021-10-23 02:37:37 UTC+0000
0xe000e86bba60     TCPv4    0.0.0.0:49411                  0.0.0.0:0            LISTENING        1304     spoolsv.exe    2021-10-23 02:37:38 UTC+0000
0xe000e86c1a30     TCPv4    0.0.0.0:49410                  0.0.0.0:0            LISTENING        804      svchost.exe    2021-10-23 02:37:37 UTC+0000
```

Figura 16. Execução do comando "**volatility -f memdump.mem --profile=Win10x64_10240_17770 netscan**".

 # volatility -f memdump.mem --profile=Win10x64_10240_17770 getsids -p 2420

```
# vol.py -f memdump.mem --profile=Win10x64_10240_17770 getsids -p 2420
Volatility Foundation Volatility Framework 2.6.1
explorer.exe (2420): S-1-5-21-47146295-3313382980-111859884-1001 (srvmaster)
explorer.exe (2420): S-1-5-21-47146295-3313382980-111859884-513 (Domain Users)
explorer.exe (2420): S-1-1-0 (Everyone)
explorer.exe (2420): S-1-5-114 (Local Account (Member of Administrators))
explorer.exe (2420): S-1-5-32-544 (Administrators)
explorer.exe (2420): S-1-5-32-545 (Users)
explorer.exe (2420): S-1-5-4 (Interactive)
explorer.exe (2420): S-1-2-1 (Console Logon (Users who are logged onto the physical console))
explorer.exe (2420): S-1-5-11 (Authenticated Users)
explorer.exe (2420): S-1-5-15 (This Organization)
explorer.exe (2420): S-1-5-113 (Local Account)
explorer.exe (2420): S-1-5-5-0-127438 (Logon Session)
explorer.exe (2420): S-1-2-0 (Local (Users with the ability to log in locally))
explorer.exe (2420): S-1-5-64-10 (NTLM Authentication)
explorer.exe (2420): S-1-16-8192 (Medium Mandatory Level)
```

Figura 17. Execução do comando "**volatility -f memdump.mem --profile=Win10x64_10240_17770 getsids -p 2420**".

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

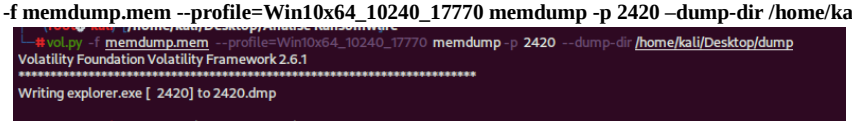


Figura 18. Execução do comando "**volatility -f memdump.mem --profile=Win10x64_10240_17770 memdump -p 2420 –dump-dir /home/kali/Desktop/dump**".

 # strings 2420.dmp > 2420.txt

Figura 19. Execução do comando "**strings 2420.dmp > 2420.txt**".

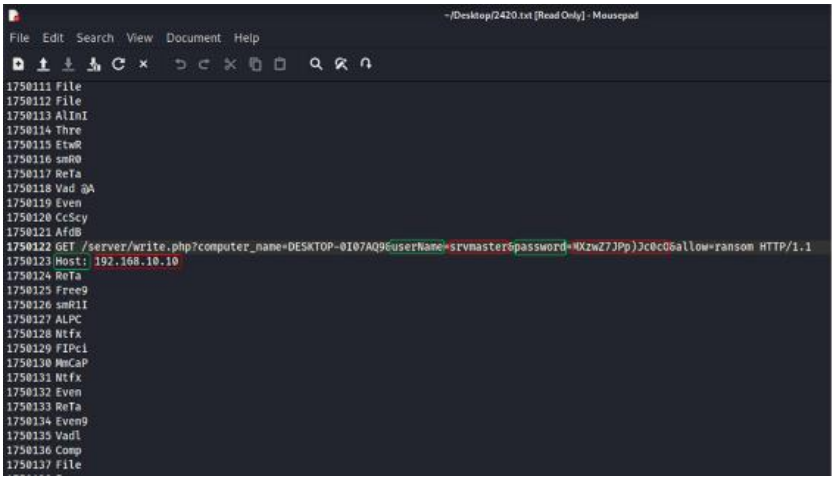
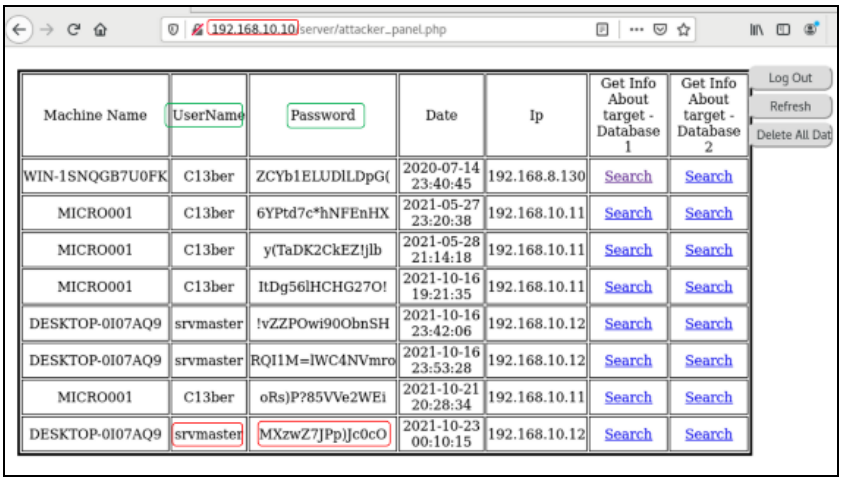


Figura 20. Informações de conexão com o ambiente de Comando e Controle do atacante incluindo a chave criptográfica do ransomware.



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	ItDg56lHCHG27O!	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

Figura 21. Informações do ambiente de Comando e Controle do atacante com a chave criptográfica do ransomware.

5. CONCLUSÃO

Devido ao aumento na quantidade de dispositivos computacionais conectados, a distribuição de programas maliciosos associados à prática criminosa cresce diariamente. Consequentemente, a presença de malwares em exames periciais é cada vez mais frequente. Além disso, a alta diversidade de classes e métodos distintos de atuação dos malwares fazem com que os exames periciais realizados nesses tipos de programas criem desafios aos especialistas em informática forense. O propósito deste artigo foi apresentar a análise específica de ransomwares para os profissionais da área, juntamente com ferramentas e técnicas que irão auxiliar na identificação e extração de sua(s) chave(s) criptográfica(s).

Ante o exposto, este artigo abordou a análise forense computacional de ransomwares para extração binária de sua chave criptográfica, dada a preservação do vestígio cibernético junto à sua respectiva identificação, isolamento e coleta, uma vez que a manipulação dos dados contidos em mídias de armazenamento computacional deve ser realizada com toda atenção

possível, pois a prova não pode ter seu estado inicial alterado, ou seja, nenhum bit pode ser modificado.

No cenário abordado, constatou-se a possibilidade de recuperação dos arquivos criptografados através da verificação das características e do comportamento do ransomware, permitindo identificar e extrair sua chave criptográfica por meio da análise dos dados contidos em memória, com uma abordagem metodológica que pode ser empregada analogamente para outros casos semelhantes em que seja necessário recuperar ambientes atacados por esse tipo de malware, visto que a análise de malwares, em particular dos ransomwares, passa a ser uma realidade cada vez mais frequente nos exames periciais. Entender os conceitos sobre o assunto, conhecer métodos para compreender seu funcionamento visando à identificação e extração de sua(s) chave(s) criptográfica(s) são tarefas que devem estar presentes no dia a dia de qualquer perito criminal que atue na Computação Forense.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ABNT. NBR 27037: Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro, 2011.

[2] ACCESSDATA CORP. FTK User Guide. Lindon, Utah, EUA: AccessData, 2010.

[3] AQUILINA, J.; CASEY, E.; MALIN, C. Malware Forensics: Investigating and Analyzing Malicious Code. EUA: Syngress, 2008.

[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] STATISTA. Como funciona um ransomware. Disponível em: <https://es.statista.com/grafico/9376/como-funciona-un-ransomware/>. Acesso em: 28 de novembro de 2022.

[6] TANENBAUM, Andrew. S. Sistemas Operacionais Modernos. 4a. ed., São Paulo: Prentice-Hall, 2015.

[7] VILAR, Gustavo Pinto; GUSMÃO, Luiz Eduardo. Identificação, isolamento, coleta e preservação do vestígio cibernético. In: VELHO, Jesus Antonio (org.). Tratado de Computação Forense. 1ª. ed. Campinas: Millennium, 2016. p. 25-32.

[8] VELHO, J. A.; COSTA, K. A.; DAMASCENO, C. T.M. Locais de Crimes - dos Vestígios à Dinâmica Criminosa. Campinas: Millennium, 2013.

[9] VELHO, J. A.; GEISER, G. C.; ESPÍNDULA, A. Ciências Forenses – Uma introdução às principais áreas da Criminalística Moderna. 4a. ed. Campinas: Millennium, 2021.

[10] VELHO, J.A.; VILAR, G.P.; GUSMÃO, E.; FRANCO, D.P.; GROCHOCKI, L.R. Polícia Científica – Transformando Vestígios em Evidências. Curitiba: Intersaberes, 2020.