# Medusa Ransomware

**Malware Analysis**

**Dati dell'Analista**

•Nome dell'Analista: Valerio Cesaroni

•Data dell'Analisi: 26/02/2024

•Strumenti Utilizzati: Capa.exe, Cutter, Wireshark, TCPView, ProcMon, pestudio, inetsim, REMnux, FLARE VM;

**Overview**

Medusa è in circolazione dal 2021 e ha fatto parlare di sé a seguito di molteplici attacchi ed estorsioni avvenute con successo, pubblicando i dati esfiltrati in caso non si pagasse il riscatto.

Formalmente si tratta di un classico Ransomware con diverse caratteristiche degne di nota.

Prima di procedere con la crittografia, Medusa è in grado di terminare programmi che potrebbero impedirla, come database, software di backup ed antivirus.

Elimina anche le copie shadow, la possibilità di avviare in modalità provvisoria e svuota anche il cestino ed files vengono rinominati con una estensione tipica che può variare. Dispone anche della possibilità di aggirare meccanismi di difesa di Windows.
In un file che compare sul desktop vengono indicati i contatti per il riscatto.

Il malware possiede anche capacità di replicazione sulla rete che infetta utilizzando SMB ed effettuando una scansione della stessa.

Nel caso la vittima si rifiuti di pagare, i dati vengono poi pubblicati dai cybercriminali.

Medusa, which has been in circulation since 2021, has made headlines due to multiple successful attacks and extortions. In cases where the ransom is not paid, Medusa publishes the exfiltrated data. Formally, it falls into the category of a classic ransomware with several noteworthy features.

Before proceeding with encryption, Medusa is capable of terminating programs that might hinder it, such as databases, backup software, and antivirus programs. It also eliminates shadow copies, prevents booting in safe mode, and empties the recycle bin. Files are renamed with a typical extension that can vary. Additionally, Medusa can bypass Windows defense mechanisms.

Upon infection, a file appears on the desktop containing contact information for the ransom. The malare also possesses network replication capabilities, infecting systems using SMB (Server Message Block) and conducting network scans.

In cases where victims refuse to pay, the cybercriminals proceed to publicly release the data.

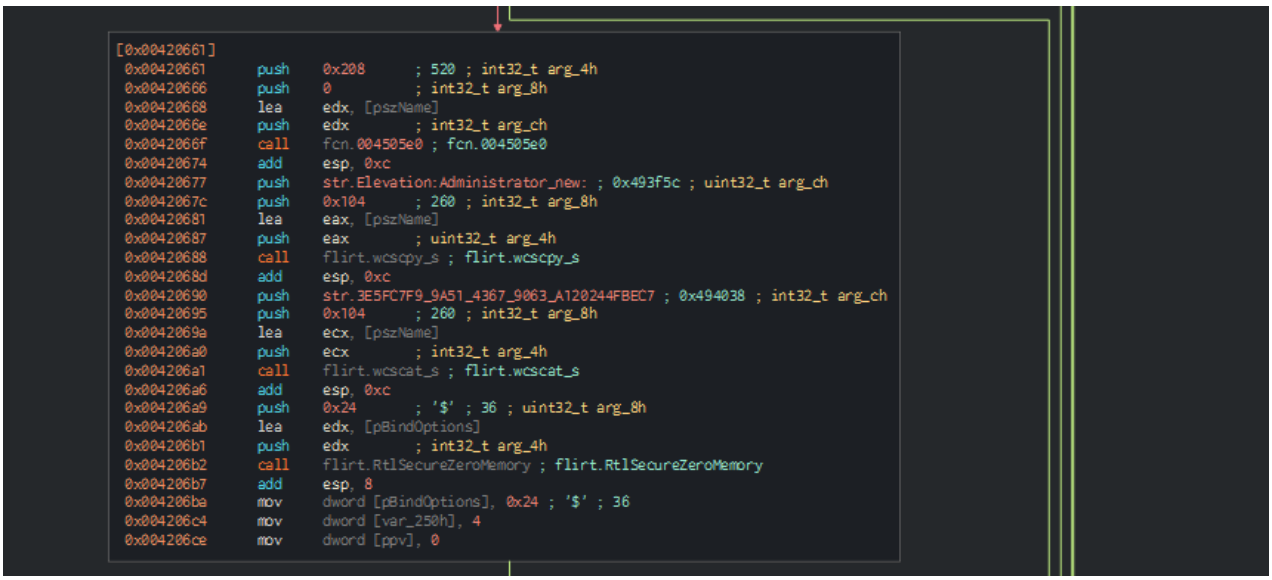
| Hashes | |
|---|---|
| MD5 | 55c4883494e8846ca0f66f20973aee0e |
| SHA256 | 8e797fff8fae9afb216b81ae341aac9f05f419061075b0f6ce4c0c7a67f458a4 |

| property | value |
|---|---|
| footprint > sha256 | 8E797FFF8FAE9AFB216B81AE341AAC9F05F419061075B0F6CE4C0C7A67F458A4 |
| first-bytes-hex | 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 |
| first-bytes-text | M Z . . . . . @ . . . . . |
| file > size | 681984 bytes |
| entropy | 6.179 |
| signature | Microsoft Visual C++ |
| tooling | Visual Studio 2015 |
| file-type | executable |
| cpu | 32-bit |
| subsystem | **GUI** |
| file-version | n/a |
| description | n/a |

Il campione analizzato è un eseguibile Windows a 32 bit come indicano i primi bytes dello stesso (MZ).

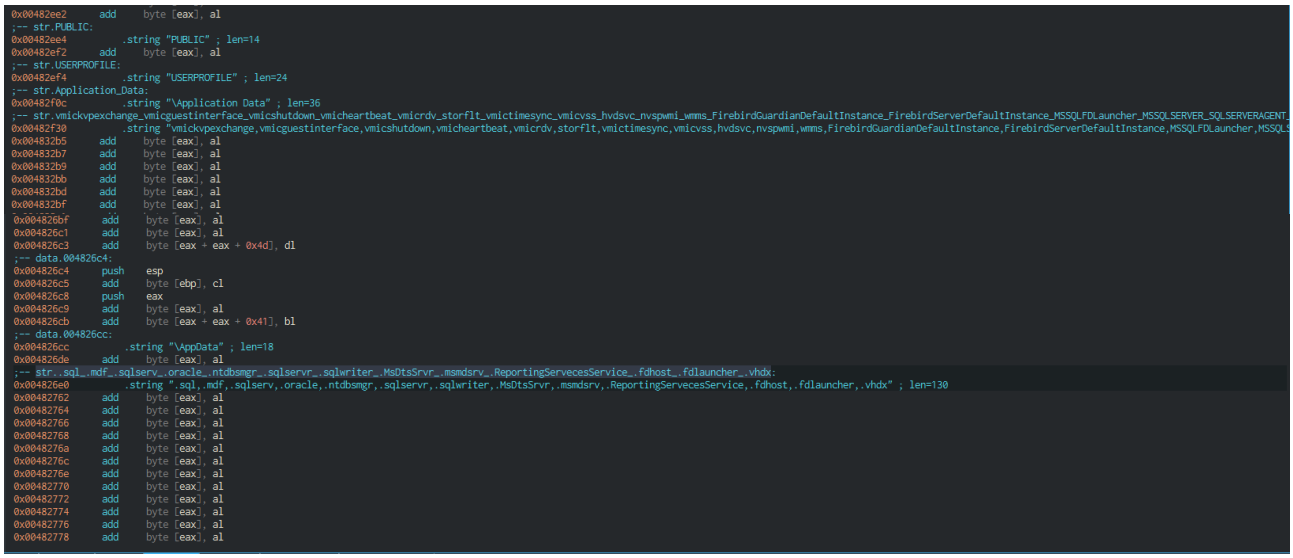
Una volta eseguito, se ha privilegi amministrativi, Medusa tenta il bypass di UAC, quel meccanismo di sicurezza che farebbe altrimenti apparire un prompt per l'approvazione dell'utente in caso si volessero eseguire istruzioni con privilegi di Amministratore:

The analyzed sample is a 32-bit Windows executable, as indicated by the initial bytes (MZ). Once executed, if it has administrative privileges, Medusa attempts to bypass User Account Control (UAC). UAC is a security mechanism that would otherwise prompt the user for approval when executing instructions with Administrator privileges :



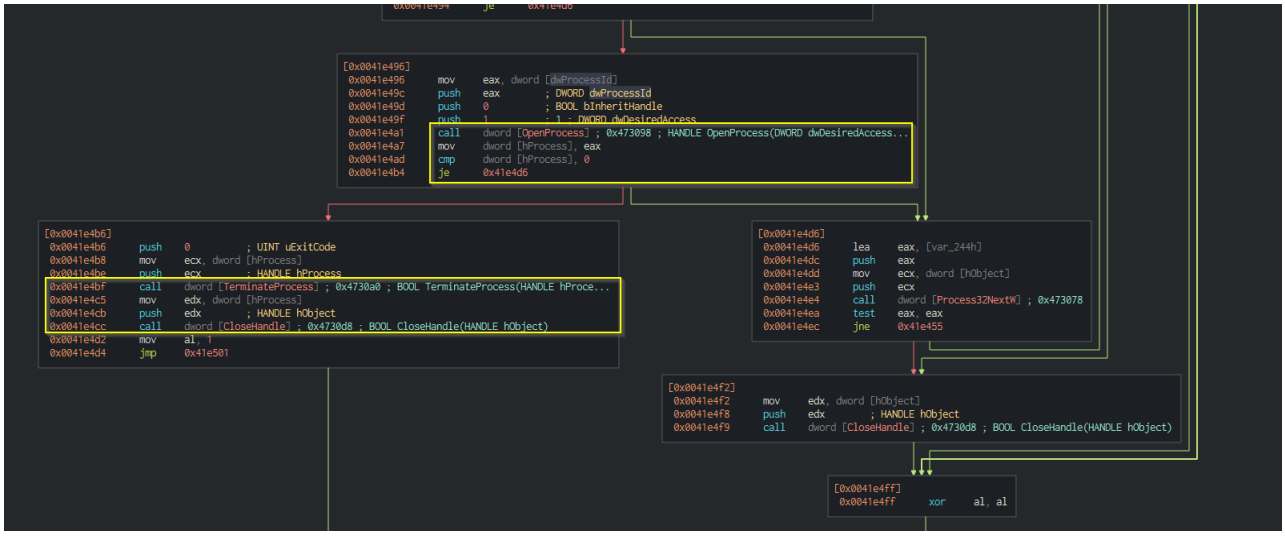

Medusa tenta la disattivazione di una serie di programmi che si trovano hardcoded nell'eseguibile:

Medusa attempts to disable a series of programs that are hardcoded within the executable:



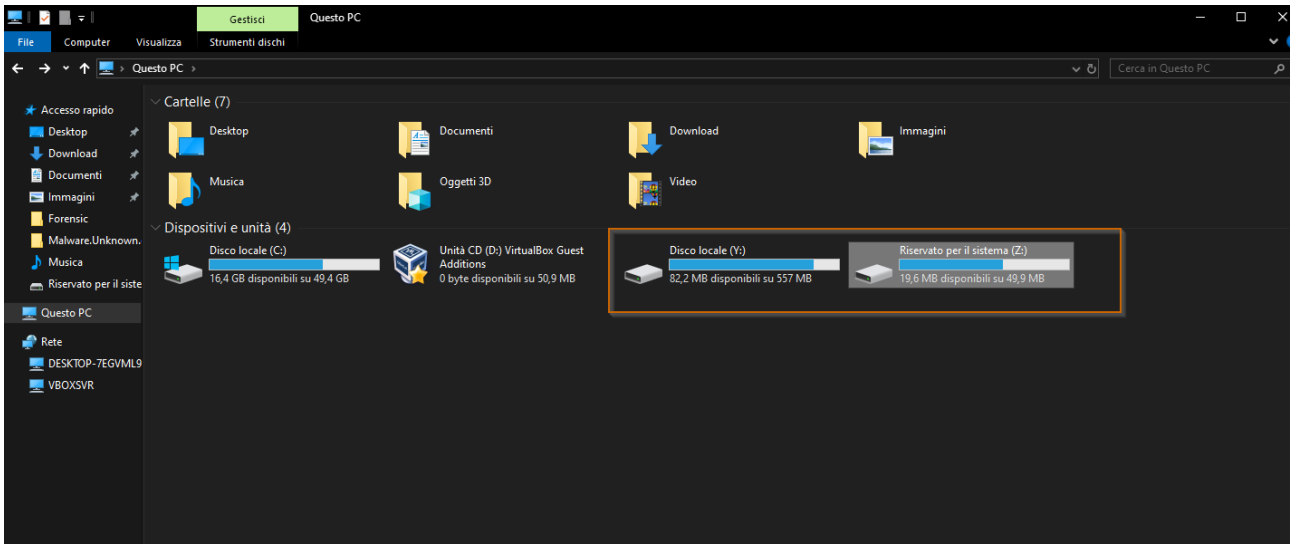

In tal senso, hardcoded nell'eseguibile, si riscontrano diverse API per la gestione dei processi

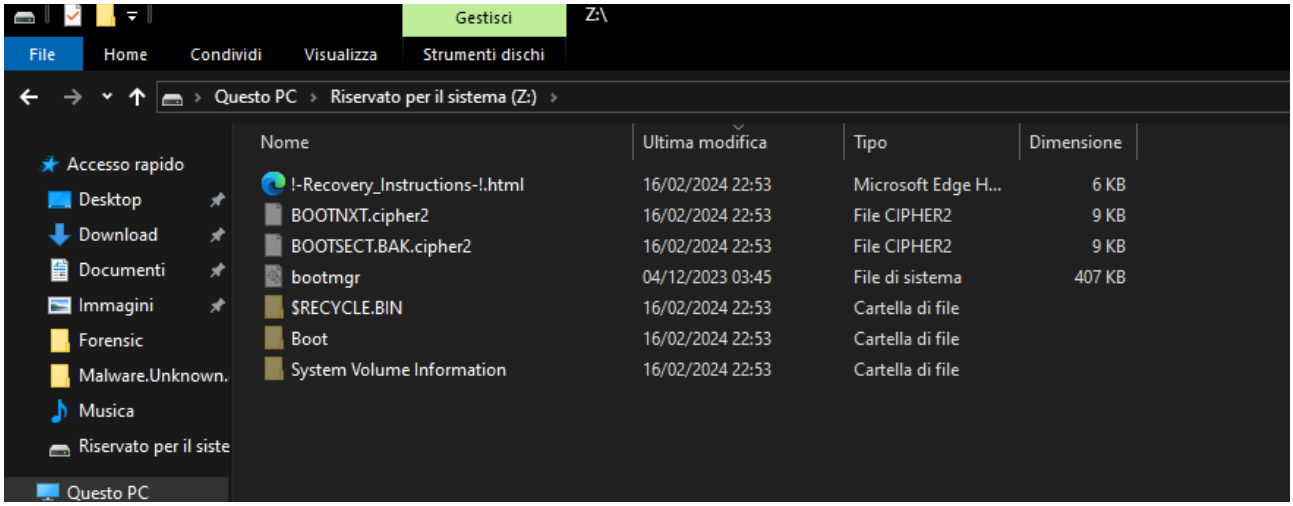
In this regard, several APIs for process management are found hardcoded within the executable



Vengono create due share di rete come appoggio per i files per l'attività del RansomWare:

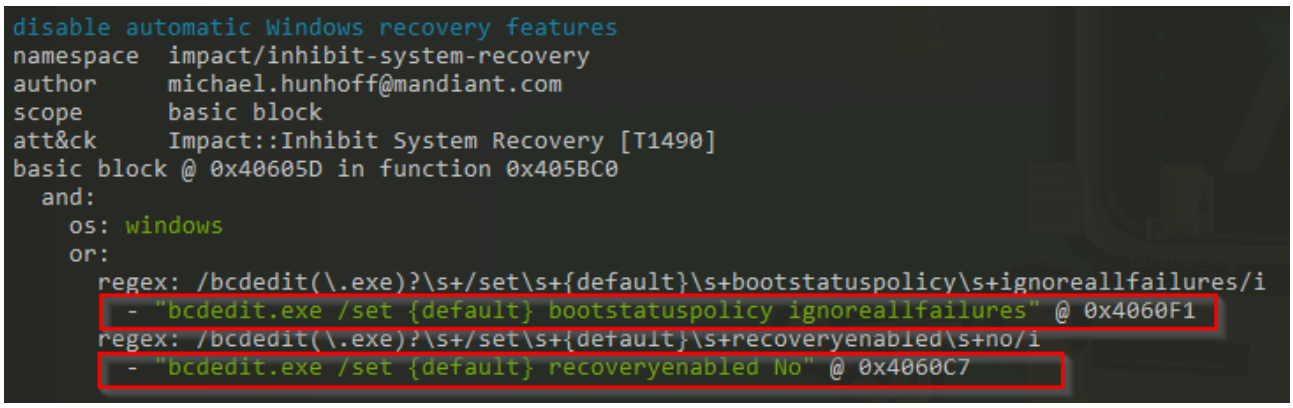
Two network shares are created as a support for the RansomWare's activity with files:




L'eseguibile dispone della capacità di inibire le features di recupero di Windows tramite bcedit. Nel caso riportato sotto si tratta di disabilitare la possibilità di effettuare il reboot in modalità di recupero:

The executable has the capability to disable Windows recovery features using **bcedit**. In the case reported below, it disables the ability to perform a reboot in recovery mode:




Disassemblando si nota la presenza di quanto riportato e anche di altre capacità. Nello specifico :

1)vssadmin.exe per la rimozione di copie shadow di un volume specificato;

2)bcdedit.exe per la rimozione della possibilità del riavvio in modalità di recupero;

3)wbadmin per la rimozione delle copie di backup;

4)wmic.exe rimozione della copie shadow.

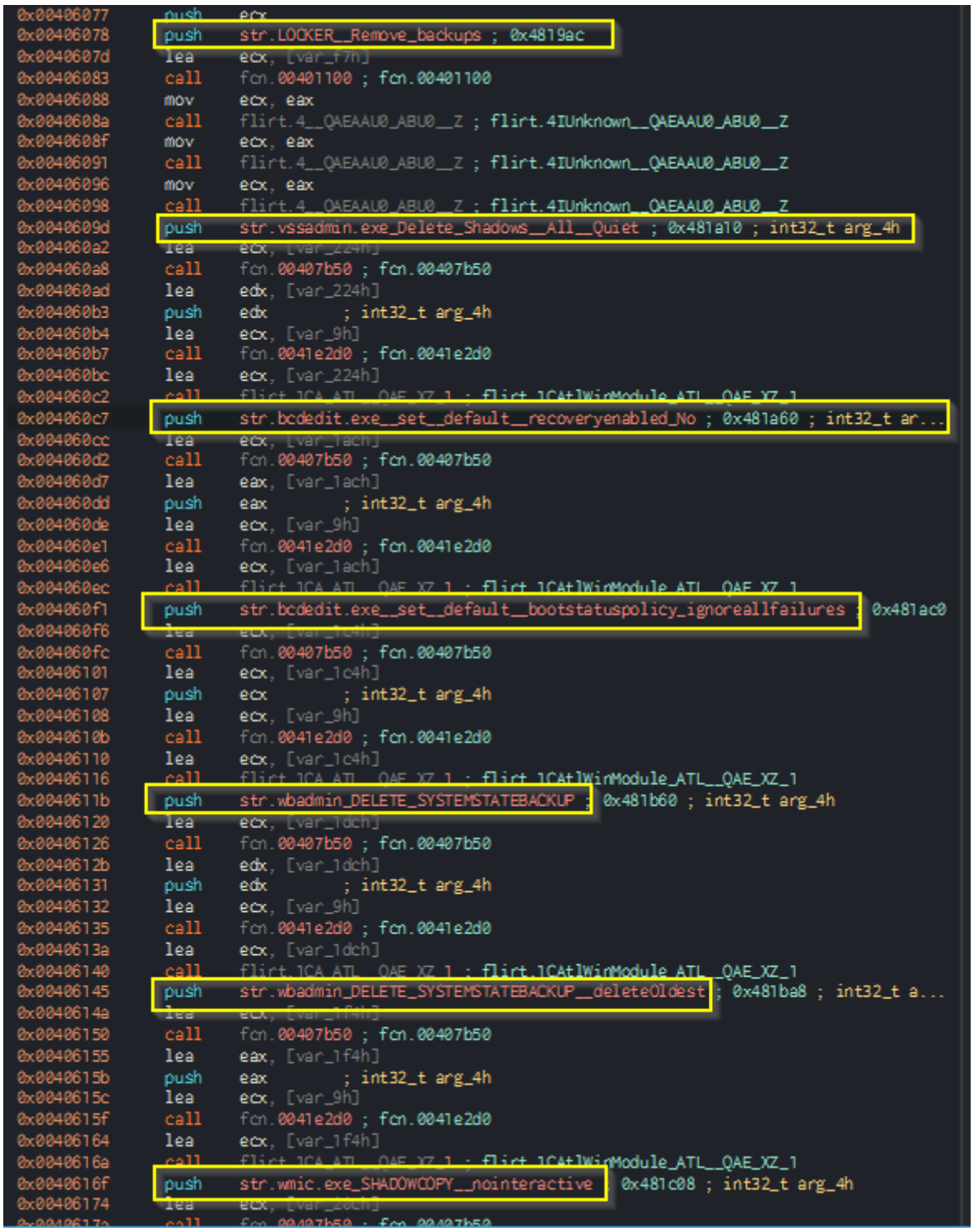
Disassembling reveals the presence of the reported capabilities and others as well. Specifically:

1.vssadmin.exe: Used for removing shadow copies of a specified volume.

2.bcdedit.exe: Used to disable the ability to reboot in recovery mode.

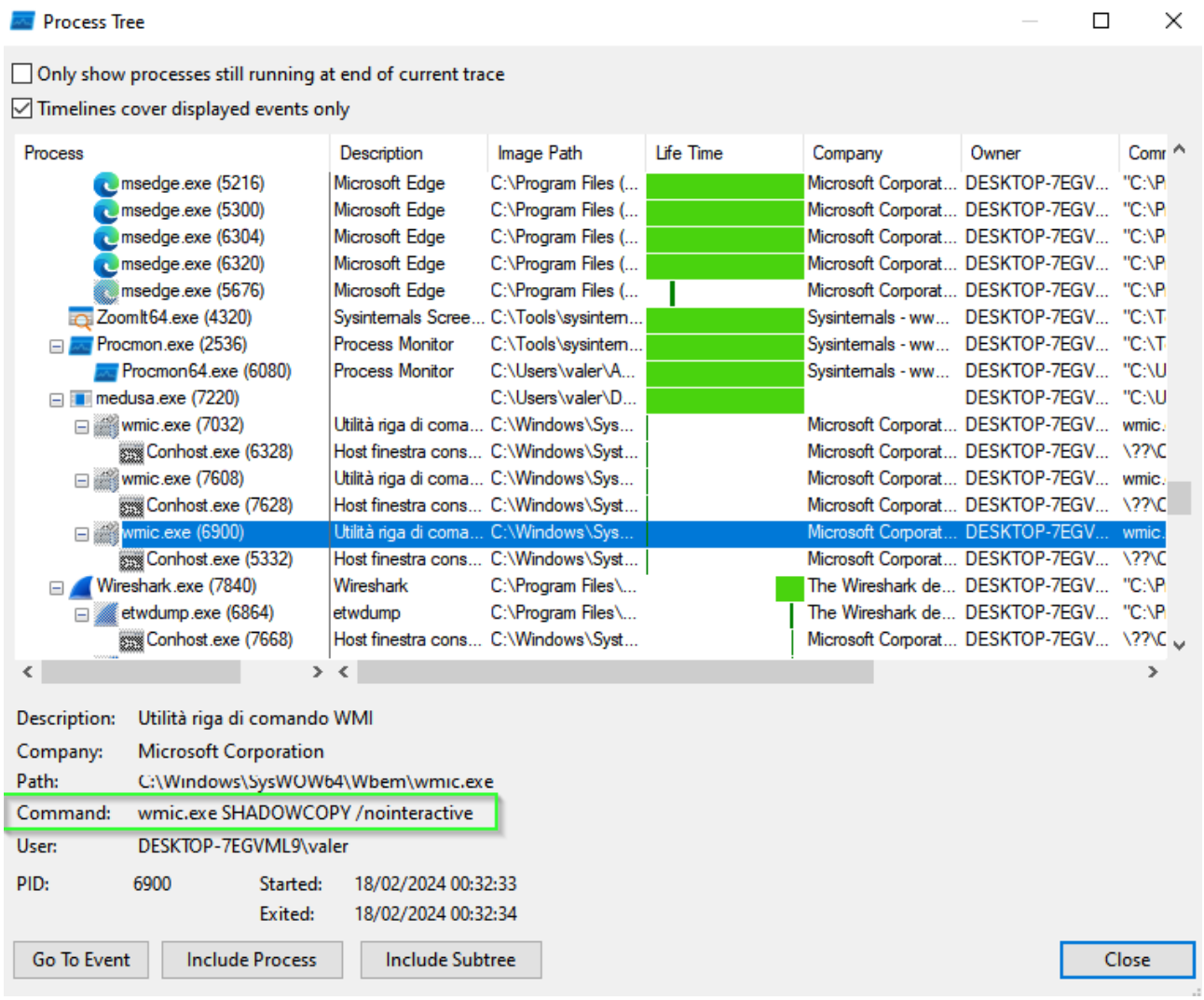
3.wbadmin: Removes backup copies.

4.wmic.exe: Removes shadow copies




Da una analisi dinamica si può notare che l'eseguibile di medusa lancia questi comandi dall'albero dei processi:

From a dynamic analysis, it can be observed that the Medusa executable launches these commands from the process tree:



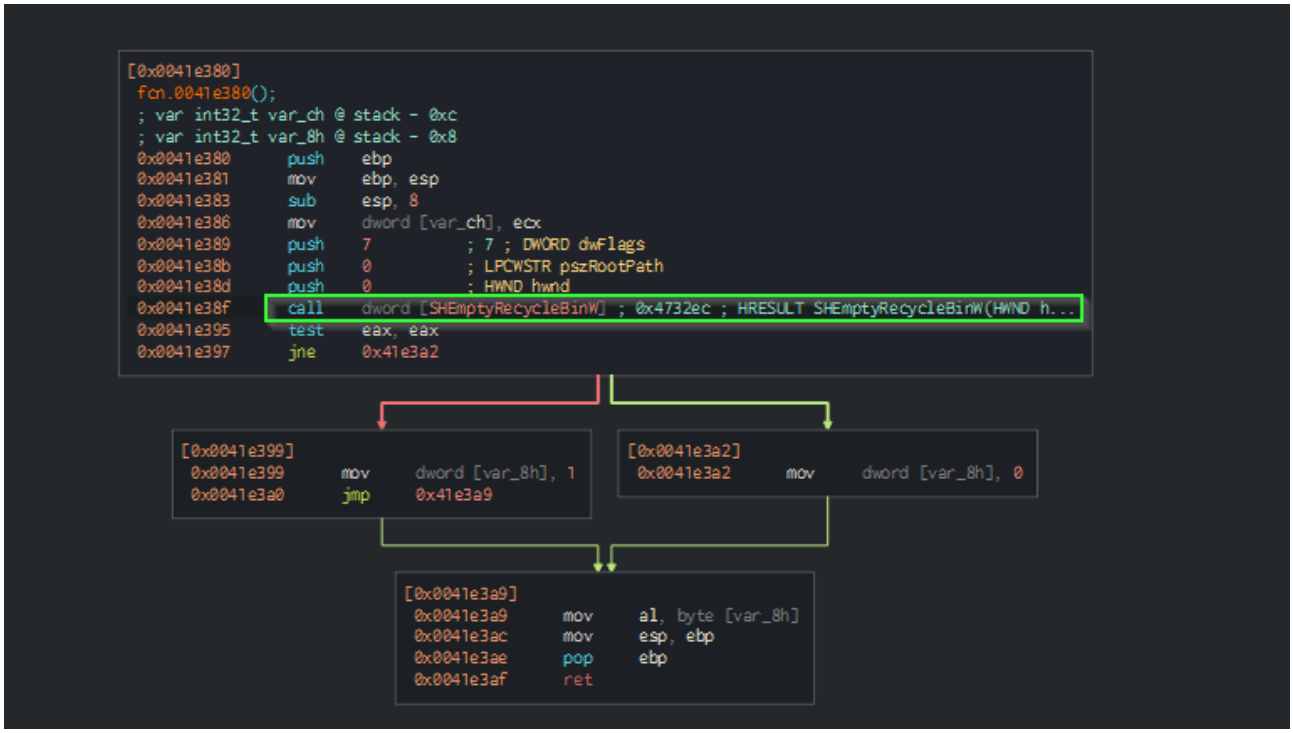

I comandi risultano anche hardcoded sotto forma di stringhe nell'eseguibile :

In this regard, several APIs for process management are found hardcoded within the executable :

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ascii | 13 | section:.rdata | - | import | dynamic-library | T1106 \| Execution through API | LoadLibraryEx |
| ascii | 11 | section:.rdata | - | import | dynamic-library | T1106 \| Execution through API | LoadLibrary |
| ascii | 12 | section:.rdata | - | import | diagnostic | - | GetLastError |
| ascii | 13 | section:.rdata | - | import | diagnostic | - | FormatMessage |
| ascii | 12 | section:.rdata | - | import | diagnostic | - | SetLastError |
| ascii | 18 | section:.rdata | - | - | diagnostic | - | RegisterTraceGuids |
| ascii | 20 | section:.rdata | - | - | diagnostic | - | UnregisterTraceGuids |
| ascii | 20 | section:.rdata | - | - | diagnostic | - | GetTraceLoggerHandle |
| ascii | 19 | section:.rdata | - | - | diagnostic | - | GetTraceEnableFlags |
| unicode | 14 | section:.rdata | - | utility | cryptography | - | Encrypt file: |
| ascii | 11 | section:.rdata | - | file | cryptography | - | CRYPT32.dll |
| ascii | 12 | section:.rdata | - | import | console | - | GetStdHandle |
| ascii | 12 | section:.rdata | - | import | console | - | SetStdHandle |
| ascii | 12 | section:.rdata | - | import | console | - | GetConsoleCP |
| ascii | 14 | section:.rdata | - | import | console | - | GetConsoleMode |
| ascii | 12 | section:.rdata | - | import | console | - | WriteConsole |
| unicode | 28 | section:.rdata | - | wmi | - | - | Elevation:Administrator!new: |
| unicode | 39 | section:.rdata | - | utility | - | - | vssadmin.exe Delete Shadows /All /Quiet |
| unicode | 45 | section:.rdata | - | utility | - | - | bcdedit.exe /set {default} recoveryenabled No |
| unicode | 61 | section:.rdata | - | utility | - | - | bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures |
| unicode | 32 | section:.rdata | - | utility | - | - | wbadmin DELETE SYSTEMSTATEBACKUP |
| unicode | 46 | section:.rdata | - | utility | - | - | wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest |
| unicode | 34 | section:.rdata | - | utility | - | - | wmic.exe SHADOWCOPY /nointeractive |
| unicode | 6 | section:.rdata | - | utility | - | - | WINDIR |
| ascii | 64 | section:.data | - | size | - | - | .?AVCancellationTokenRegistration_TaskProc@details@Concurrency@@ |
| ascii | 64 | section:.data | - | size | - | - | .?AV?$_Ref_count_obj@U?$_Task_impl@E@details@Concurrency@@@std@@ |
| ascii | 19 | section:.data | - | rtti | - | - | .?AVbad_alloc@std@@ |
| ascii | 23 | section:.data | - | rtti | - | - | .?AVbad_exception@std@@ |
| ascii | 73 | section:.data | - | rtti | - | - | .?AV?$_Ref_count_obj_alloc@V__ExceptionPtr@@U?$_StaticAllocator@H@@@std@@ |
| ascii | 44 | section:.data | - | rtti | - | - | .?AV?$_Ref_count_obj@V__ExceptionPtr@@@std@@ |
| ascii | 56 | section:.data | - | rtti | - | - | .?AVstl_critical_section_interface@details@Concurrency@@ |
| ascii | 52 | section:.data | - | rtti | - | - | .?AVstl_critical_section_vista@details@Concurrency@@ |
| ascii | 51 | section:.data | - | rtti | - | - | .?AVstl_critical_section_win7@details@Concurrency@@ |
| ascii | 53 | section:.data | - | rtti | - | - | .?AVstl_critical_section_concrt@details@Concurrency@@ |
| ascii | 58 | section:.data | - | rtti | - | - | .?AVstl_condition_variable_interface@details@Concurrency@@ |
| ascii | 54 | section:.data | - | rtti | - | - | .?AVstl_condition_variable_vista@details@Concurrency@@ |
| ascii | 53 | section:.data | - | rtti | - | - | .?AVstl_condition_variable_win7@details@Concurrency@@ |
| ascii | 55 | section:.data | - | rtti | - | - | .?AVstl_condition_variable_concrt@details@Concurrency@@ |
| ascii | 22 | section:.data | - | rtti | - | - | .?AVfuture_error@std@@ |

Medusa, oltre a rimuovere le copie di backup, si occupa anche di svuotare il cestino, come osservato da analisi dinamica e come riscontrato nella chiamata alla API apposita:

Medusa, in addition to removing backup copies, also empties the recycle bin, as observed during dynamic analysis and confirmed by the relevant API call :



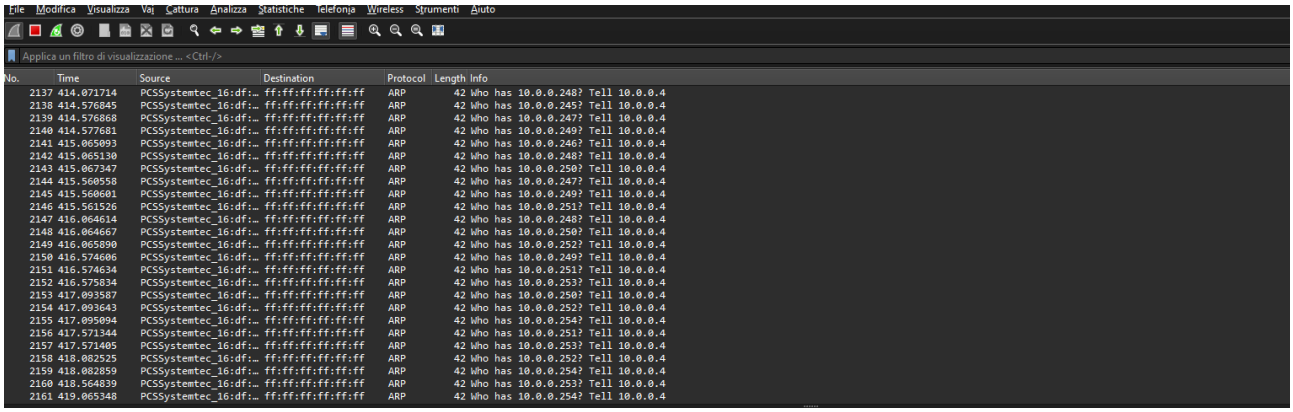

Una volta avviato, Medusa lancia una scansione nella rete per scoprire hosts raggiungibili attraverso ICMP (Internet Control Message Protocol) :

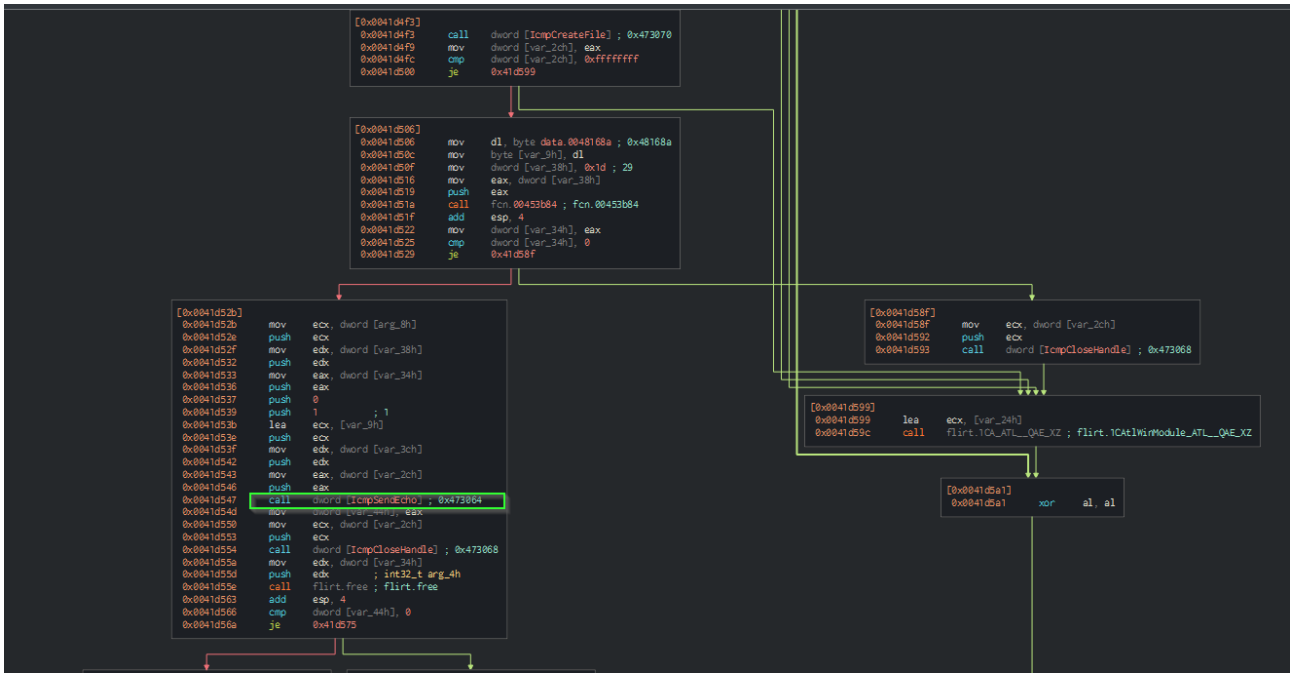
Once launched, Medusa initiates a network scan to discover reachable hosts using ICMP (Internet Control Message Protocol) :

```
send ICMP echo request
namespace   communication/icmp
author      michael.hunhoff@mandiant.com
scope       function
mbc         Communication::ICMP Communication::Echo Request [C0014.002]
references  https://docs.microsoft.com/en-us/windows/win32/api/icmpapi/
function @ 0x41D480
  and:
    or:
      api: IcmpSendEcho @ 0x41D547
    optional:
      or:
        api: IcmpCreateFile @ 0x41D4F3
      api: IcmpCloseHandle @ 0x41D554, 0x41D593
```

Questo comportamento è riscontrabile sia come capacità, disassemblando l'eseguibile, che osservando una cattura di pacchetti con Wireshark. In questo ultimo caso si osserva una sequenza di richieste ARP che coinvolge tutta la rete 10.0.0.X del laboratorio:

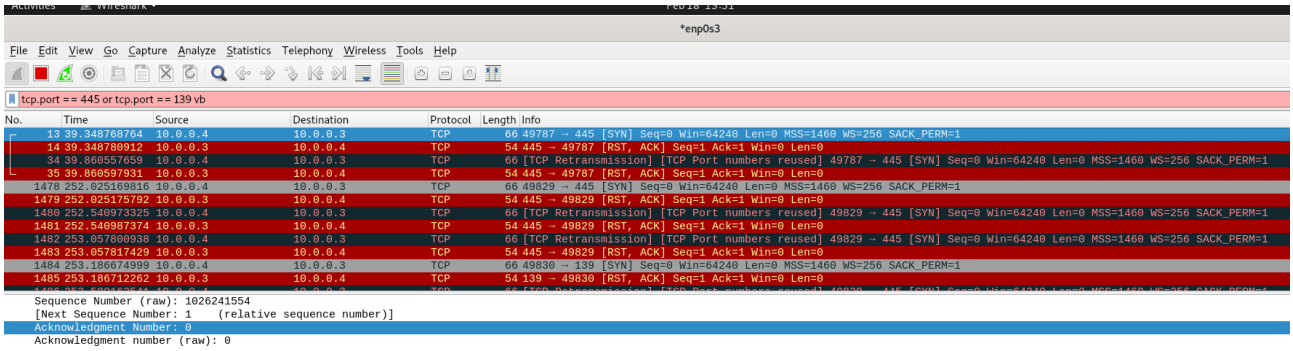
This behavior can be observed both as a capability by disassembling the executable and by observing packet captures using Wireshark. In the latter case, a sequence of ARP requests involving the entire 10.0.0.X network in the laboratory is observed:



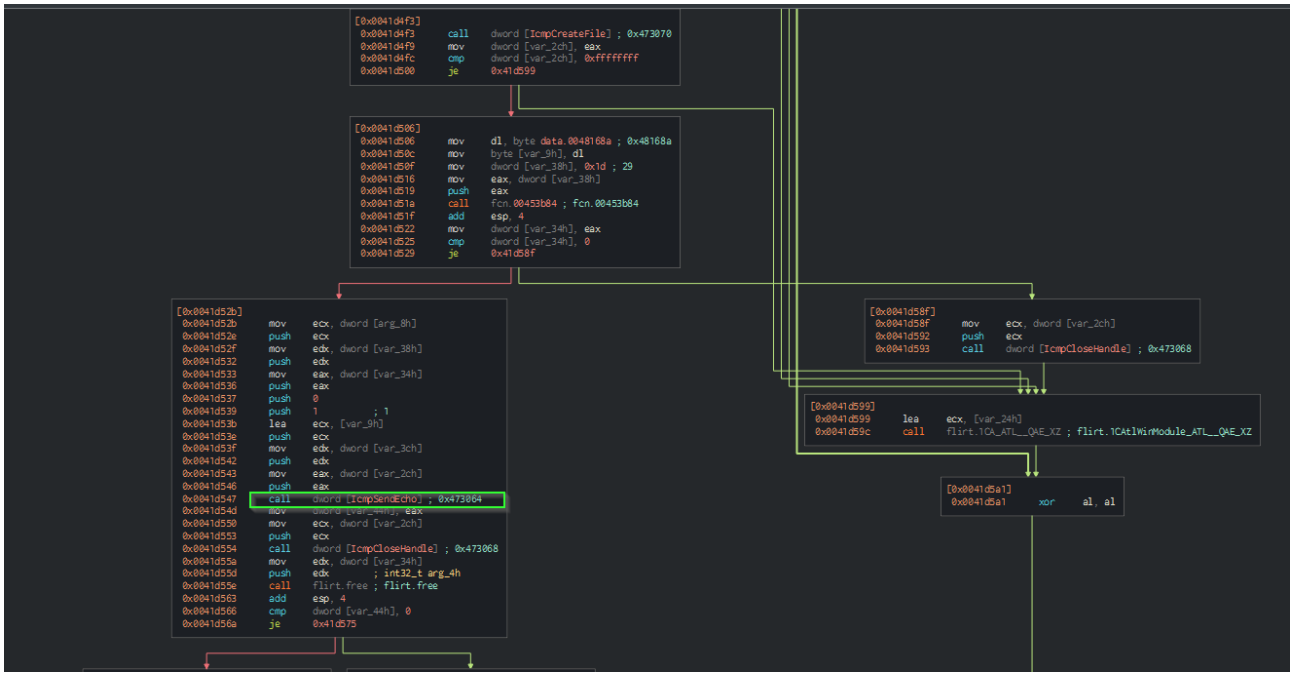
Come tecnica di movimento laterale si possono osservare chiamate agli IP rilevati nella rete su porta 445 e 139 (SMB e Netbios) comunemente usate per il movimenro laterale:

As a lateral movement technique, Medusa initiates calls to the IP addresses detected on the network via ports 445 and 139 (SMB and Netbios), which are commonly used for lateral movement :



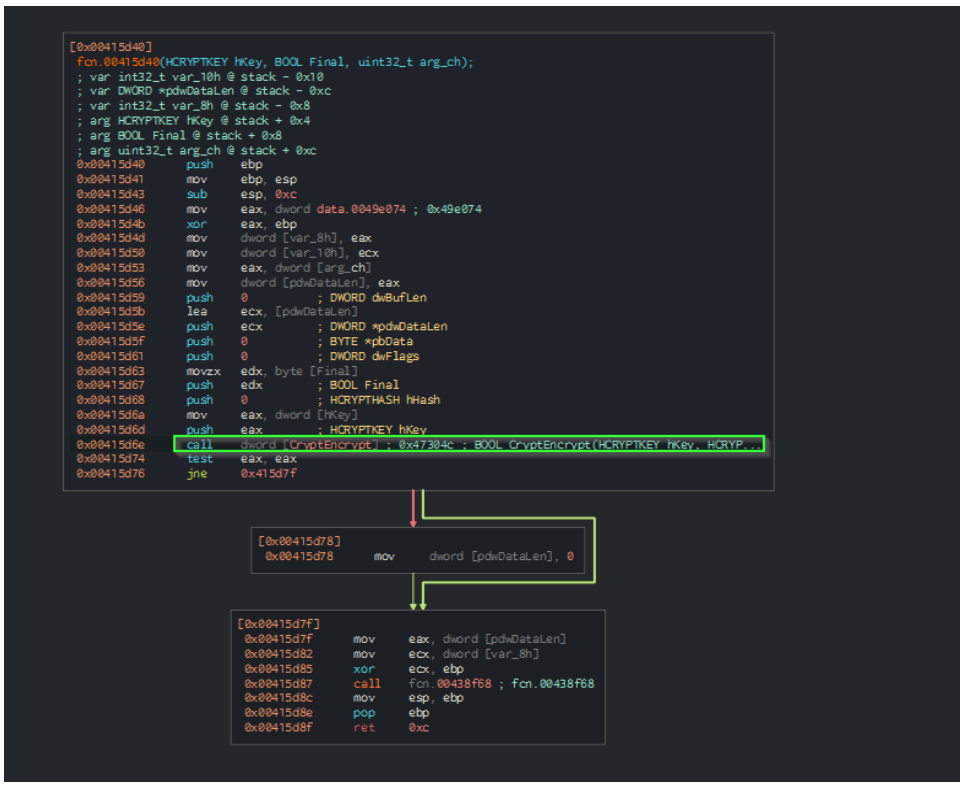

Sulla macchina bersaglio Medusa in cicli di 60 secondi cerca nuovi files da codificare:

On the target machine, Medusa periodically scans for new files to encrypt in 60-second cycles :



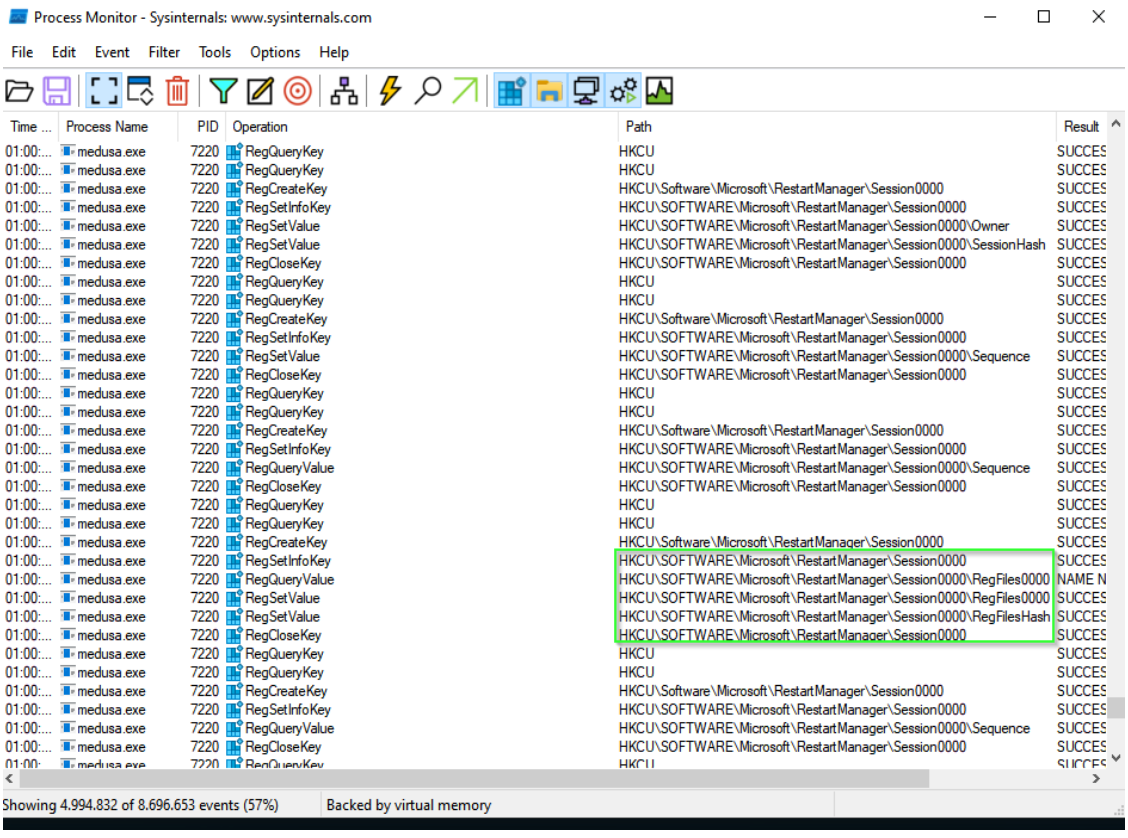
per arrivare alla fase di encrypt:

To reach the encryption phase :




si nota l'uso di RestartManager ( si occupa di far chiudere salvando i files prima del riavvio ) per fare unlocking dei files aperti e poterli crittare:

RestartManager is employed by Medusa to gracefully close and save open files before initiating a reboot. This step ensures that files are not left in an inconsistent state during the encryption process. By unlocking open files, Medusa can proceed to encrypt them without risking data corruption or loss :



Infine, sempre nel ciclo dei 60 secondi, medusa resta in attesa di nuovi files. Sul desktop compare il seguente file e i files codificati hanno estensione cipher2 :

Finally, within the 60-second cycle, Medusa patiently awaits new files. On the desktop, a file appears, and the encrypted files bear the extension ".cipher2" :