

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 malware 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 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

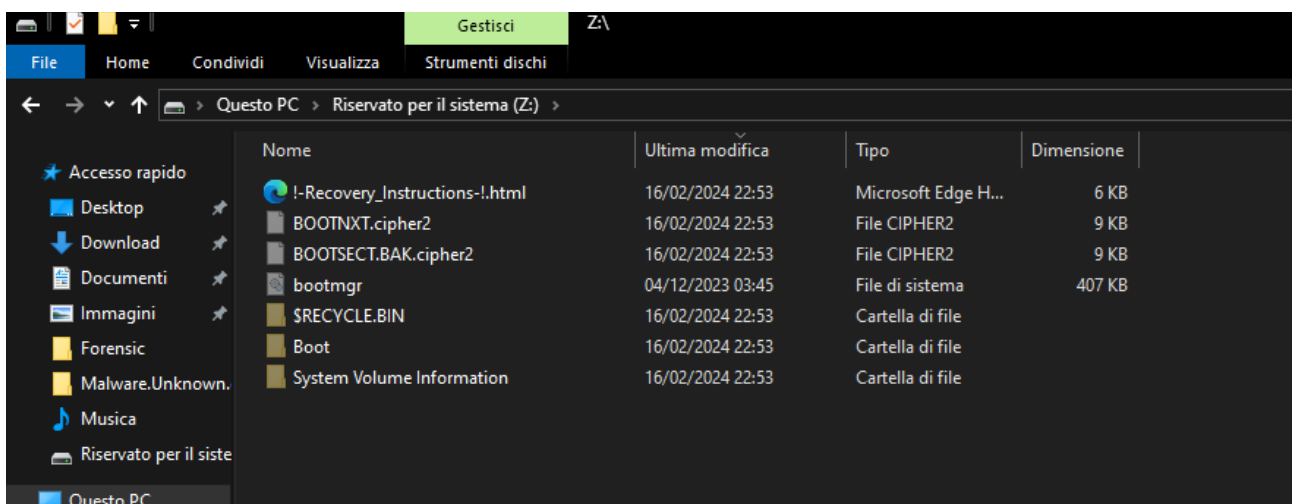
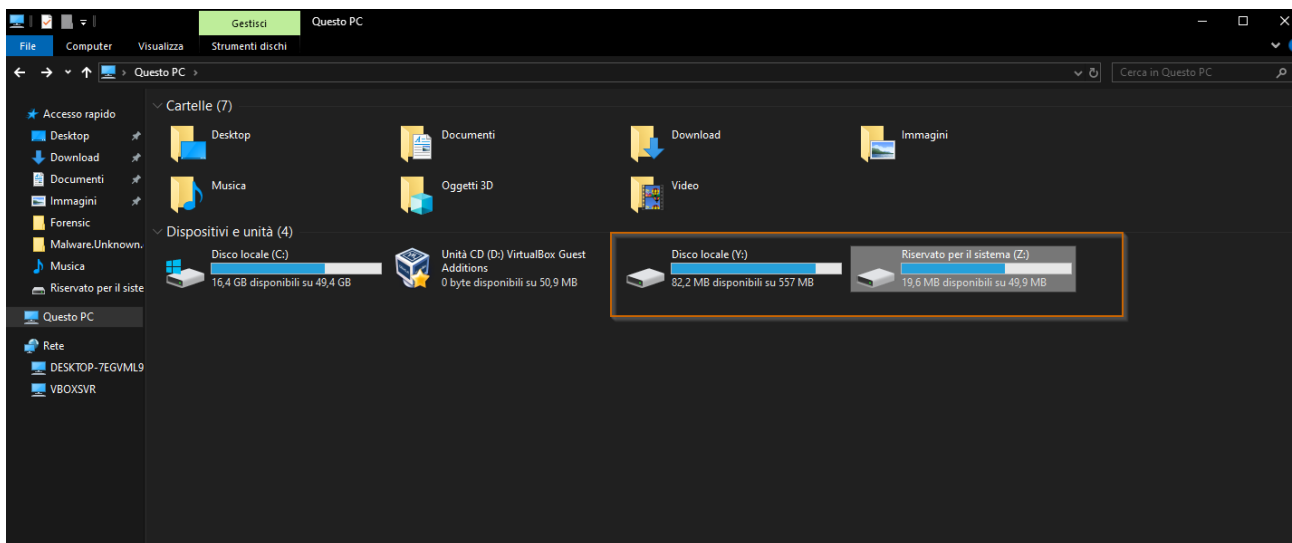
Il campione analizzato è un eseguibile Windows a 32 bit come indicano i primi bytes dello stesso (MZ).

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 :

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 bcdedit. 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 **bcdedit**. In the case reported below, it disables the ability to perform a reboot in recovery mode:

```
disable automatic Windows recovery features
namespace impact/inhibit-system-recovery
author michael.hunhoff@mandiant.com
scope basic block
att&ck Impact::Inhibit System Recovery [T1490]
basic block @ 0x40605D in function 0x405BC0
and:
  os: windows
  or:
    regex: /bcdedit(\.exe)?\s+/set\s+{default}\s+bootstatuspolicy\s+ignoreallfailures/i
    - "bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures" @ 0x4060F1
    regex: /bcdedit(\.exe)?\s+/set\s+{default}\s+recoveryenabled\s+no/i
    - "bcdedit.exe /set {default} recoveryenabled No" @ 0x4060C7
```

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
-

```

0x00406077  push    ecx
0x00406078  push    str.LOCKER_Remove_backups ; 0x4819ac
0x0040607d  lea     ecx, [var_7h]
0x00406083  call    fcn.00401100 ; fcn.00401100
0x00406088  mov     ecx, eax
0x0040608a  call    flint.4__QAEAAU0_ABU0_Z ; flint.4IUnknown__QAEAAU0_ABU0_Z
0x0040608f  mov     ecx, eax
0x00406091  call    flint.4__QAEAAU0_ABU0_Z ; flint.4IUnknown__QAEAAU0_ABU0_Z
0x00406096  mov     ecx, eax
0x00406098  call    flint.4__QAEAAU0_ABU0_Z ; flint.4IUnknown__QAEAAU0_ABU0_Z
0x0040609d  push    str.vssadmin.exe_Delete_Shadows__All__Quiet ; 0x481a10 ; int32_t arg_4h
0x004060a2  lea     ecx, [var_224h]
0x004060a8  call    fcn.00407b50 ; fcn.00407b50
0x004060ad  lea     edx, [var_224h]
0x004060b3  push    edx ; int32_t arg_4h
0x004060b4  lea     ecx, [var_9h]
0x004060b7  call    fcn.0041e2d0 ; fcn.0041e2d0
0x004060bc  lea     ecx, [var_224h]
0x004060c2  call    flint.1CA_ATL__QAE_XZ_1 ; flint.1CAIWinModule_ATL__QAE_XZ_1
0x004060c7  push    str.bcdedit.exe__set_default__recoverynabled_No ; 0x481a60 ; int32_t ar...
0x004060cc  lea     ecx, [var_1ach]
0x004060d2  call    fcn.00407b50 ; fcn.00407b50
0x004060d7  lea     eax, [var_1ach]
0x004060dd  push    eax ; int32_t arg_4h
0x004060de  lea     ecx, [var_9h]
0x004060e1  call    fcn.0041e2d0 ; fcn.0041e2d0
0x004060e6  lea     ecx, [var_1ach]
0x004060ec  call    flint.1CA_ATL__QAE_XZ_1 ; flint.1CAIWinModule_ATL__QAE_XZ_1
0x004060f1  push    str.bcdedit.exe__set_default__bootstatuspolicy_ignoreallfailures ; 0x481ac0
0x004060f6  lea     ecx, [var_1ach]
0x004060fc  call    fcn.00407b50 ; fcn.00407b50
0x00406101  lea     ecx, [var_1c4h]
0x00406107  push    ecx ; int32_t arg_4h
0x00406108  lea     ecx, [var_9h]
0x0040610b  call    fcn.0041e2d0 ; fcn.0041e2d0
0x00406110  lea     ecx, [var_1c4h]
0x00406116  call    flint.1CA_ATL__QAE_XZ_1 ; flint.1CAIWinModule_ATL__QAE_XZ_1
0x0040611b  push    str.wbadmin_DELETE_SYSTEMSTATEBACKUP ; 0x481b60 ; int32_t arg_4h
0x00406120  lea     ecx, [var_1dch]
0x00406126  call    fcn.00407b50 ; fcn.00407b50
0x0040612b  lea     edx, [var_1dch]
0x00406131  push    edx ; int32_t arg_4h
0x00406132  lea     ecx, [var_9h]
0x00406135  call    fcn.0041e2d0 ; fcn.0041e2d0
0x0040613a  lea     ecx, [var_1dch]
0x00406140  call    flint.1CA_ATL__QAE_XZ_1 ; flint.1CAIWinModule_ATL__QAE_XZ_1
0x00406145  push    str.wbadmin_DELETE_SYSTEMSTATEBACKUP__deleteOldest ; 0x481ba8 ; int32_t a...
0x0040614a  lea     ecx, [var_1f4h]
0x00406150  call    fcn.00407b50 ; fcn.00407b50
0x00406155  lea     eax, [var_1f4h]
0x0040615b  push    eax ; int32_t arg_4h
0x0040615c  lea     ecx, [var_9h]
0x0040615f  call    fcn.0041e2d0 ; fcn.0041e2d0
0x00406164  lea     ecx, [var_1f4h]
0x0040616a  call    flint.1CA_ATL__QAE_XZ_1 ; flint.1CAIWinModule_ATL__QAE_XZ_1
0x0040616f  push    str.wmic.exe_SHADOWCOPY__nointeractive ; 0x481c08 ; int32_t arg_4h
0x00406174  lea     ecx, [var_20ch]
0x0040617a  call    fcn.00407b50 ; fcn.00407b50

```

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:

Process Tree

☐ Only show processes still running at end of current trace

☒ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner	Comr ^
msedge.exe (5216)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	DESKTOP-7EGV...	"C:\P
msedge.exe (5300)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	DESKTOP-7EGV...	"C:\P
msedge.exe (6304)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	DESKTOP-7EGV...	"C:\P
msedge.exe (6320)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	DESKTOP-7EGV...	"C:\P
msedge.exe (5676)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	DESKTOP-7EGV...	"C:\P
ZoomIt64.exe (4320)	Sysinternals Scree...	C:\Tools\sysintern...		Sysinternals - ww...	DESKTOP-7EGV...	"C:\T
Procmon.exe (2536)	Process Monitor	C:\Tools\sysintern...		Sysinternals - ww...	DESKTOP-7EGV...	"C:\T
Procmon64.exe (6080)	Process Monitor	C:\Users\valer\A...		Sysinternals - ww...	DESKTOP-7EGV...	"C:\U
medusa.exe (7220)		C:\Users\valer\D...			DESKTOP-7EGV...	"C:\U
wmic.exe (7032)	Utilità riga di coma...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-7EGV...	wmic.
Conhost.exe (6328)	Host finestra cons...	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-7EGV...	\??\C
wmic.exe (7608)	Utilità riga di coma...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-7EGV...	wmic.
Conhost.exe (7628)	Host finestra cons...	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-7EGV...	\??\C
wmic.exe (6900)	Utilità riga di coma...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-7EGV...	wmic.
Conhost.exe (5332)	Host finestra cons...	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-7EGV...	\??\C
Wireshark.exe (7840)	Wireshark	C:\Program Files\...		The Wireshark de...	DESKTOP-7EGV...	"C:\P
etwdump.exe (6864)	etwdump	C:\Program Files\...		The Wireshark de...	DESKTOP-7EGV...	"C:\P
Conhost.exe (7668)	Host finestra cons...	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-7EGV...	\??\C

Description: Utilità riga di comando WMI

Company: Microsoft Corporation

Path: C:\Windows\SysWOW64\Wbem\wmic.exe

Command: wmic.exe SHADOWCOPY /nointeractive

User: DESKTOP-7EGVML9\valer

PID: 6900 Started: 18/02/2024 00:32:33

 Exited: 18/02/2024 00:32:34

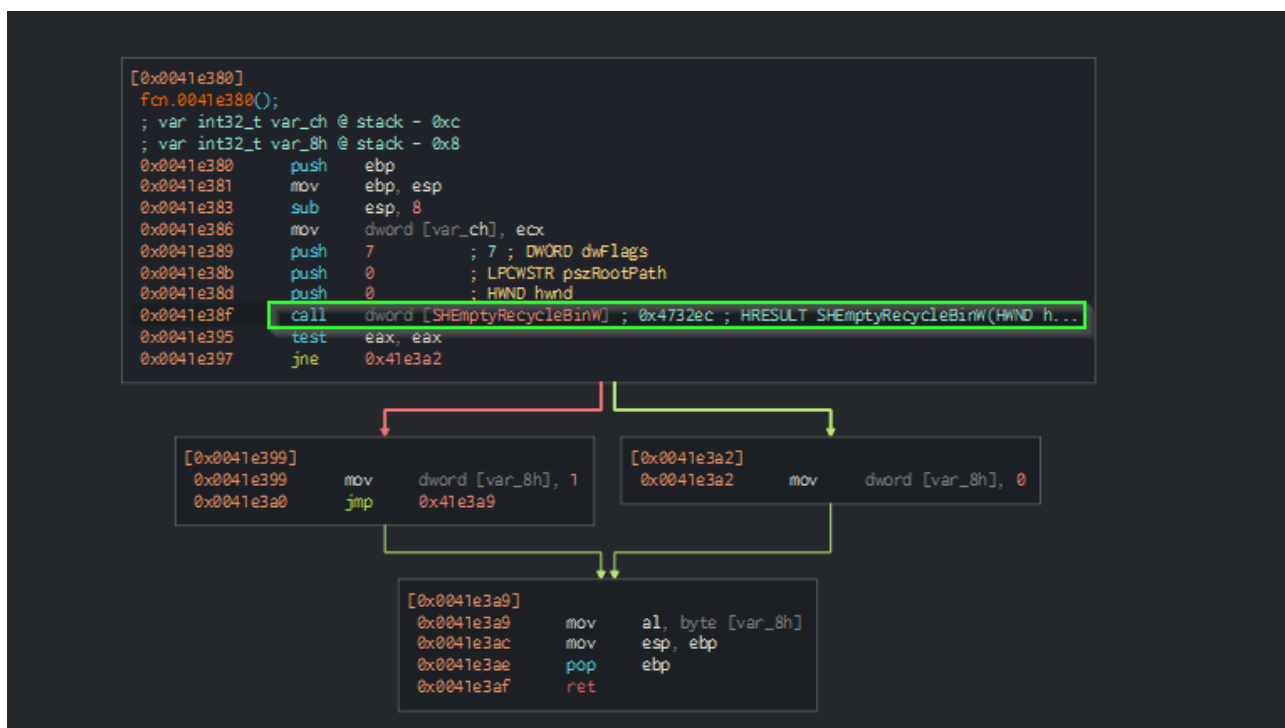
Go To Event Include Process Include Subtree Close

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 :

[illegible]

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:



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

```

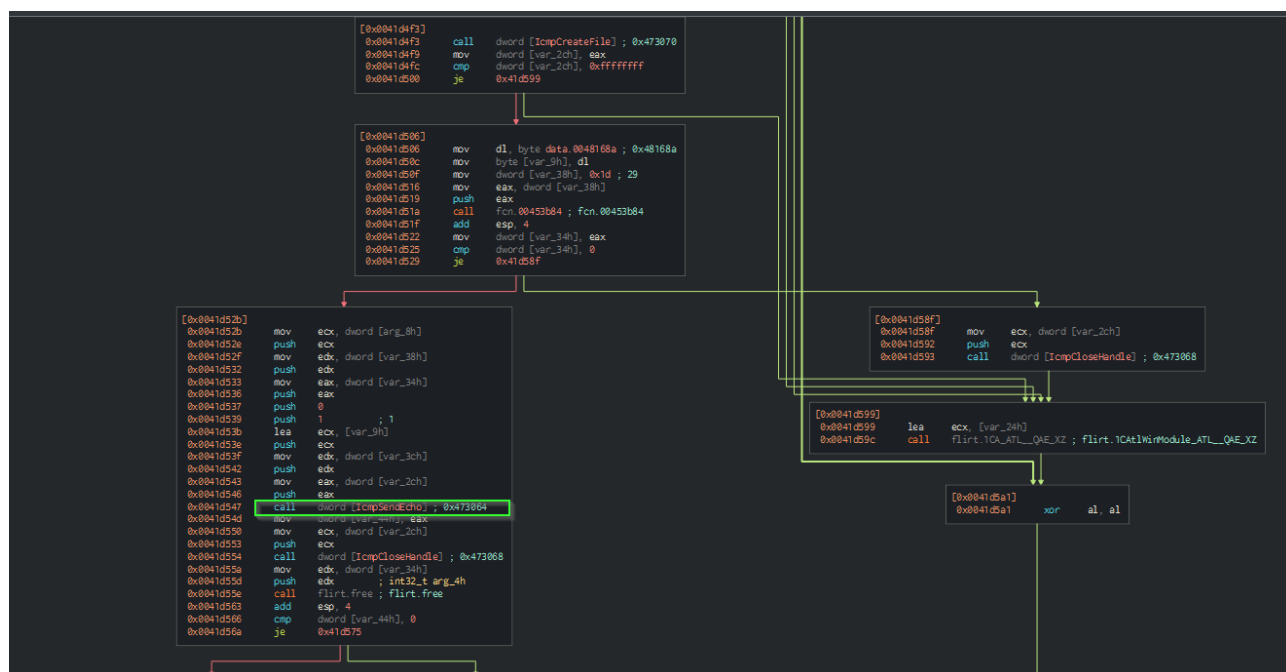
send ICMP echo request
namespace    communication/icmp
author       michael.hunhoff@mandiant.com
scope        function
mbc          Communication::ICMP Communication::Echo Request [C0014.002]
references   https://docs.microsoft.com/en-us/windows/win32/api/icmpapi/
function @ 0x41D480
and:
or:
api: IcmpSendEcho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

No.	Time	Source	Destination	Protocol	Length	Info
2137	414.071714	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.248? Tell 10.0.0.4
2138	414.576845	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.245? Tell 10.0.0.4
2139	414.576888	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.247? Tell 10.0.0.4
2140	414.577681	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.249? Tell 10.0.0.4
2141	415.065093	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.246? Tell 10.0.0.4
2142	415.065130	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.248? Tell 10.0.0.4
2143	415.067347	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.250? Tell 10.0.0.4
2144	415.569553	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.247? Tell 10.0.0.4
2145	415.569601	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.249? Tell 10.0.0.4
2146	415.561526	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.251? Tell 10.0.0.4
2147	416.064614	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.248? Tell 10.0.0.4
2148	416.064667	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.250? Tell 10.0.0.4
2149	416.065090	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.252? Tell 10.0.0.4
2150	416.574606	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.249? Tell 10.0.0.4
2151	416.574634	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.251? Tell 10.0.0.4
2152	416.575834	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.253? Tell 10.0.0.4
2153	417.093587	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.250? Tell 10.0.0.4
2154	417.093643	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.252? Tell 10.0.0.4
2155	417.095904	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.254? Tell 10.0.0.4
2156	417.571344	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.251? Tell 10.0.0.4
2157	417.571405	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.253? Tell 10.0.0.4
2158	418.062525	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.252? Tell 10.0.0.4
2159	418.062859	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.254? Tell 10.0.0.4
2160	418.564839	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.253? Tell 10.0.0.4
2161	419.065348	PCSSystemtec_16:df:...	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.254? Tell 10.0.0.4



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 :

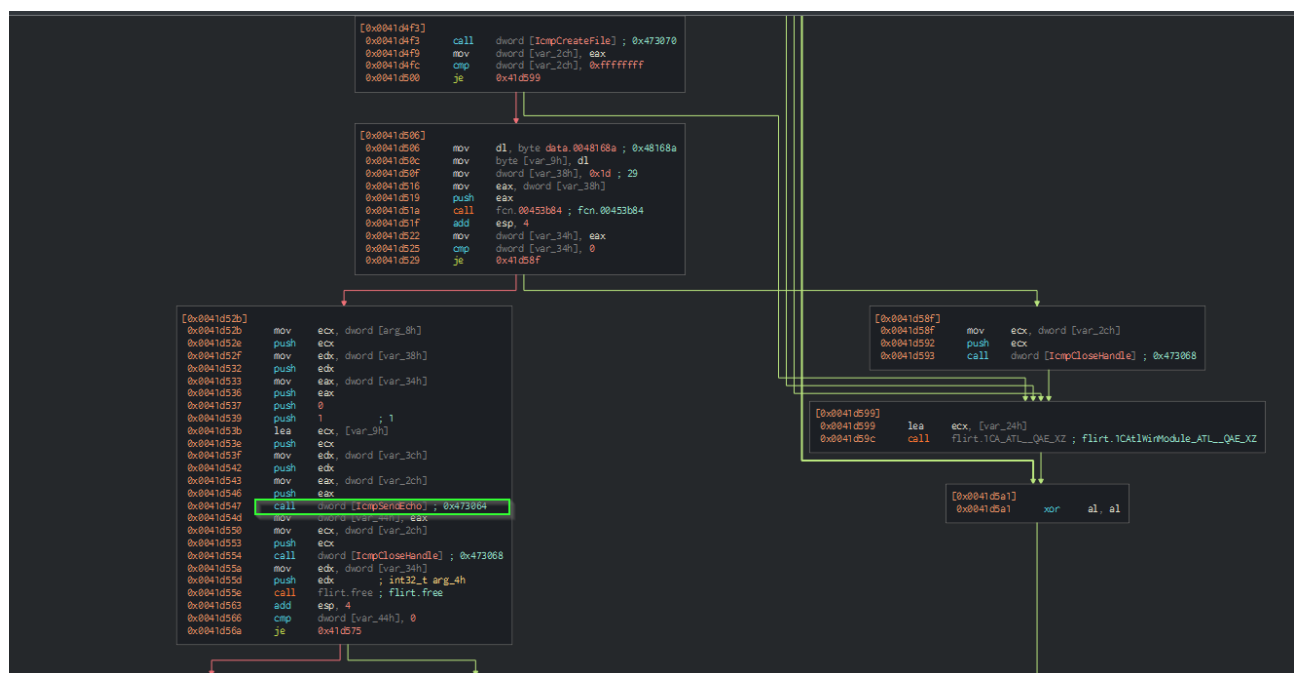
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 445 or tcp.port == 139 vb

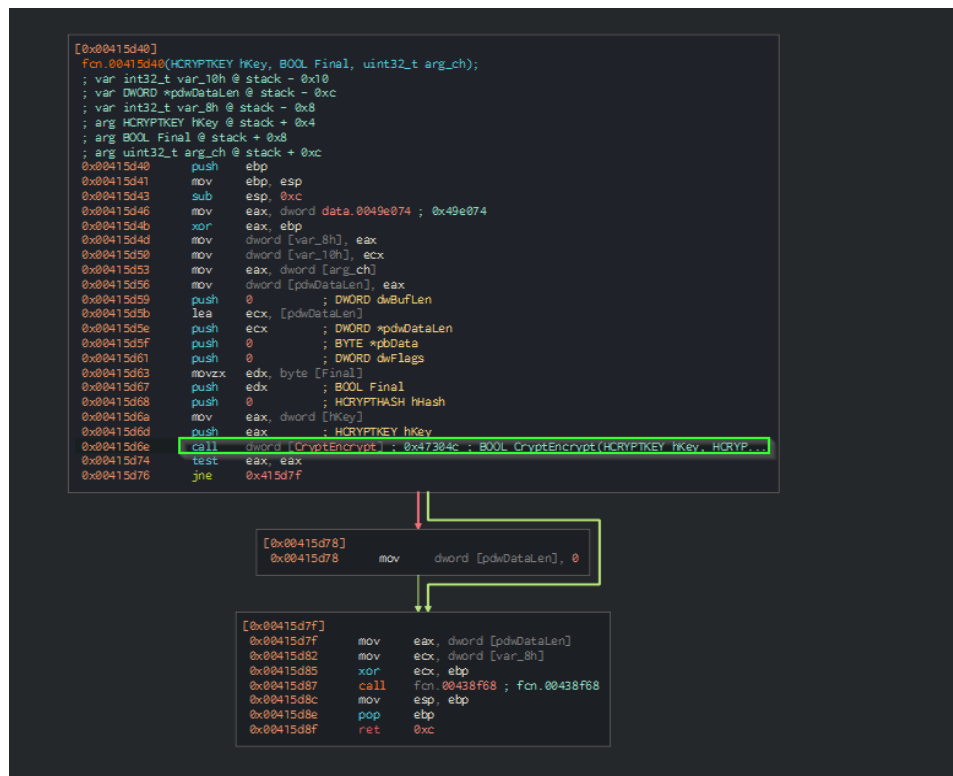
No.	Time	Source	Destination	Protocol	Length	Info
13	39.348768764	10.0.0.4	10.0.0.3	TCP	60	49787 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
14	39.348780912	10.0.0.4	10.0.0.4	TCP	54	445 → 49787 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
34	39.869557659	10.0.0.4	10.0.0.3	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 49787 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
35	39.869597313	10.0.0.4	10.0.0.3	TCP	54	445 → 49787 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1478	252.025109816	10.0.0.4	10.0.0.3	TCP	60	49829 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1479	252.025157592	10.0.0.4	10.0.0.4	TCP	54	445 → 49829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1480	252.540973325	10.0.0.4	10.0.0.3	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 49829 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1481	252.540997374	10.0.0.4	10.0.0.4	TCP	54	445 → 49829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1482	253.057809938	10.0.0.4	10.0.0.3	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 49829 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1483	253.057817429	10.0.0.4	10.0.0.4	TCP	54	445 → 49829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1484	253.186674999	10.0.0.4	10.0.0.3	TCP	60	49838 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1485	253.186712202	10.0.0.4	10.0.0.4	TCP	54	139 → 49838 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Sequence Number (raw): 1026241554
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0

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



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 :

Process Monitor - Sysinternals: www.sysinternals.com

Time	Process Name	PID	Operation	Path	Result
01:00:...	medusa.exe	7220	RegQueryKey	HKCU	SUCCESS
01:00:...	medusa.exe	7220	RegQueryKey	HKCU	SUCCESS
01:00:...	medusa.exe	7220	RegCreateKey	HKCU\Software\Microsoft\RestartManager\Session0000	SUCCESS
01:00:...	medusa.exe	7220	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS
01:00:...	medusa.exe	7220	RegSetValue	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000\Owner	SUCCESS
01:00:...	medusa.exe	7220	RegSetValue	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000\SessionHash	SUCCESS
01:00:...	medusa.exe	7220	RegCloseKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS
01:00:...	medusa.exe	7220	RegQueryKey	HKCU	SUCCESS
01:00:...	medusa.exe	7220	RegQueryKey	HKCU	SUCCESS
01:00:...	medusa.exe	7220	RegCreateKey	HKCU\Software\Microsoft\RestartManager\Session0000	SUCCESS
01:00:...	medusa.exe	7220	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS
01:00:...	medusa.exe	7220	RegSetValue	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000\Sequence	SUCCESS
01:00:...	medusa.exe	7220	RegCloseKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS
01:00:...	medusa.exe	7220	RegQueryKey	HKCU	SUCCESS
01:00:...	medusa.exe	7220	RegQueryKey	HKCU	SUCCESS
01:00:...	medusa.exe	7220	RegCreateKey	HKCU\Software\Microsoft\RestartManager\Session0000	SUCCESS
01:00:...	medusa.exe	7220	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS
01:00:...	medusa.exe	7220	RegQueryValue	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000\Sequence	SUCCESS
01:00:...	medusa.exe	7220	RegCloseKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS
01:00:...	medusa.exe	7220	RegQueryKey	HKCU	SUCCESS
01:00:...	medusa.exe	7220	RegQueryKey	HKCU	SUCCESS
01:00:...	medusa.exe	7220	RegCreateKey	HKCU\Software\Microsoft\RestartManager\Session0000	SUCCESS
01:00:...	medusa.exe	7220	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS
01:00:...	medusa.exe	7220	RegQueryValue	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000\RegFiles0000	NAME NOT FOUND
01:00:...	medusa.exe	7220	RegSetValue	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000\RegFiles0000	SUCCESS
01:00:...	medusa.exe	7220	RegSetValue	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000\RegFilesHash	SUCCESS
01:00:...	medusa.exe	7220	RegCloseKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS
01:00:...	medusa.exe	7220	RegQueryKey	HKCU	SUCCESS
01:00:...	medusa.exe	7220	RegQueryKey	HKCU	SUCCESS
01:00:...	medusa.exe	7220	RegCreateKey	HKCU\Software\Microsoft\RestartManager\Session0000	SUCCESS
01:00:...	medusa.exe	7220	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS
01:00:...	medusa.exe	7220	RegQueryValue	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000\Sequence	SUCCESS
01:00:...	medusa.exe	7220	RegCloseKey	HKCU\SOFTWARE\Microsoft\RestartManager\Session0000	SUCCESS
01:00:...	medusa.exe	7220	RegQueryKey	HKCU	SUCCESS

Showing 4,994,832 of 8,696,653 events (57%) Backed by virtual memory

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" :

