REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE
DREJTORIA E ANALIZËS SË SIGURISË KIBERNETIKE

Analizë e skedarëve të sulmit nga *Grupet Iraniane*

Versioni: 1.2
Data: 16/02/2024

Adresa: Rruga "Papa Gjon Pali II" nr 3 Tiranë;
Tel./Fax: 04 2221 0

Tabela e përmbajtjes:

Raporti është hartuar për të dokumentuar dhe analizuar sulmin kibernetik ndaj një infrastrukture në Republikën e Shqipërisë. Përmbajtja e këtij raporti bazohet në informacionet e disponueshëm deri në datën e përfundimit të analizës.

Përcjellja e këtij raporti ka për qëllim informimin dhe ndërgjegjësimin e palëve të interesuara mbi incidentin kibernetik të dokumentuar. Raporti nuk duhet trajtuar si përfundimtar deri në përditësimin final të tij.

Ky raport ka kufizime dhe duhet interpretuar me kujdes!

Disa nga këto kufizime përfshijnë:

Faza e parë:
Burimet e informacionit: Raporti është bazuar në informacionet e vëna në dispozicion në momentin e përgatitjes së tij. Ndërkohë, disa aspekte mund të jenë të ndryshme nga zhvillimet aktuale.

Faza e dytë:
Detajet e analizës: Për shkak të kufizimeve burimore, disa aspekte të incidentit mund të mos jenë analizuar thellësisht. Çdo informacion shtesë i panjohur mund të reflektojë në ndryshime të raportit.

Faza e tretë:
Analiza e kufizuar: Për shkak të natyrës komplekse të sulmit kibernetik, analiza mund të jetë e kufizuar në disa aspekte. Interpretimi i ngjarjes është subjektiv dhe mund të ndikohet nga mungesa e disa të dhënave kyçe.

Faza e katërt:
Siguria e informacionit: Për të mbrojtur burimet dhe informacionet konfidenciale, disa detaje mund të jenë të zbutura ose jo të përfshira në raport. Ky vendim është marrë për të mbajtur integritetin dhe sigurinë e të dhënave të përdorura.

AKCESK rezervon të drejtën për të ndryshuar, përditësuar, ose ndryshuar çfarëdo pjesë të këtij raporti pa lajmërim paraprak.

*Ky raport nuk është një dokument përfundimtar (nxjerrja e detajeve hyr*ëse të aktorëve keqdashës do ju vihet në dispozicion në një moment të dytë*).*

Gjetjet e raportit bazohen në informacionin e disponueshëm gjatë kohës së hetimit dhe analizës. Nuk ka garanci në lidhje me ndryshime të mundshme apo përditësime të informacioneve të raportuara gjatë periudhës në vijim. Autorët e raportit nuk marrin përgjegjësi për përdorimin e gabuar ose pasojat e ndonjë vendimmarrjeje të bazuar në këtë raport.

Informacione Teknike

Referuar sulmit kibernetik të ndodhur drejt infrastrukturës është kryer një analizim paraprak, mbi sipërfaqen e sulmit dhe detaje teknike të evidentuara bazuar në materialet e vendosura në dispozicion. Aktualisht është evidentuar se teknika përfundimtare e përdorur është nëpërmjet skedarit **MEK-DDMC.exe**, ku kryhet procesi i ***Wipering*** (fshirje e rekordeve të sektorit të ***Boot***).

Nga kjo teknikë u evidentua se janë prekur pajisje që ndodhen në **Active Directory** dhe nuk janë prekur pajisje jashtë saj. U evidentua gjithashtu se pajisjet e prekura, pjesë të **Active Directory** ishin të ndezura gjatë kohës së sulmit, ndërsa pajisjet të cilat nuk ishin të ndezura , por pjesë e **AD**, nuk janë afektuar nga ky sulm.

Gjatë procesit të skanimit dhe analizimit në disa pajisje kompjuterike, skedari ***MEK-DDMC.exe*** u evidentua në të njëjtën vendndodhje tek të gjithë pajisjet e analizuara.

"***C:\Users\Public .***"

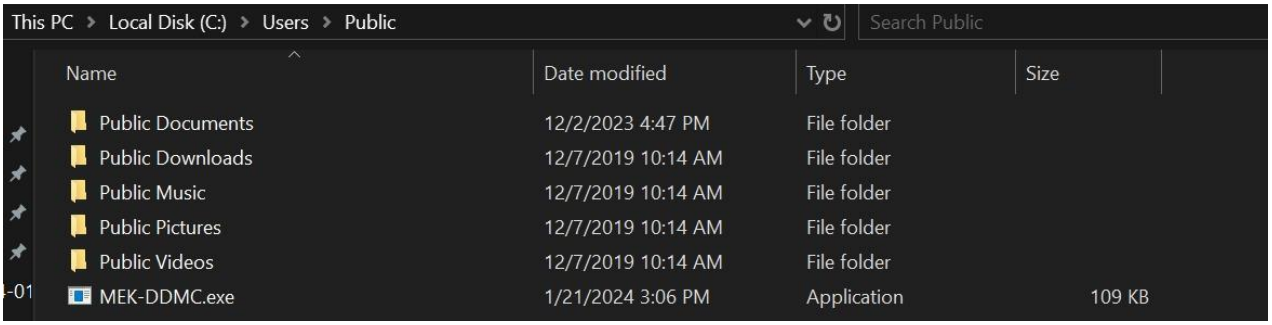


Figura 1. Vendndodhja e MEK-DDMC.exe

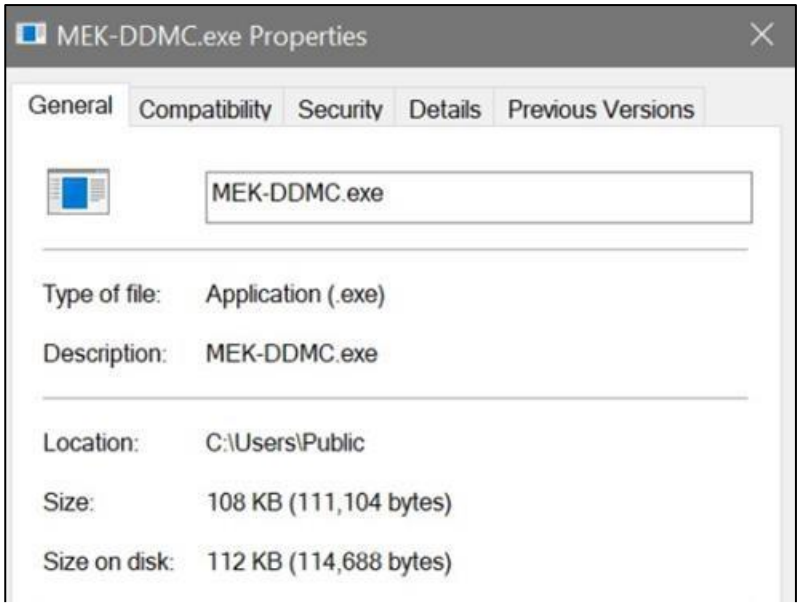


Figura 2. Të dhënat e skedarit malinj.

Prania e skedarit keqdashës u evidentua në pajisjet kompjuterike Windows, ku nuk ka qenë e mundur të kryhet ekzekutimi përfundimtar me veti shkatërruese për sistemin operativ dhe rekordet e Boot (MBR apo GPT).

Nga analiza e eventeve tek këto pajisje kompjuterike, evidentohen tentativa të shumta në rrjet në porta të ndryshme për të fituar akses mbi to.

Figura 3. Tentativa drejt portave të ndryshme në rrjet në intervale të ndryshme kohore.

Gjithashtu u evidentuan evente **Audit Failure** gjatë kësaj periudhe kohore.

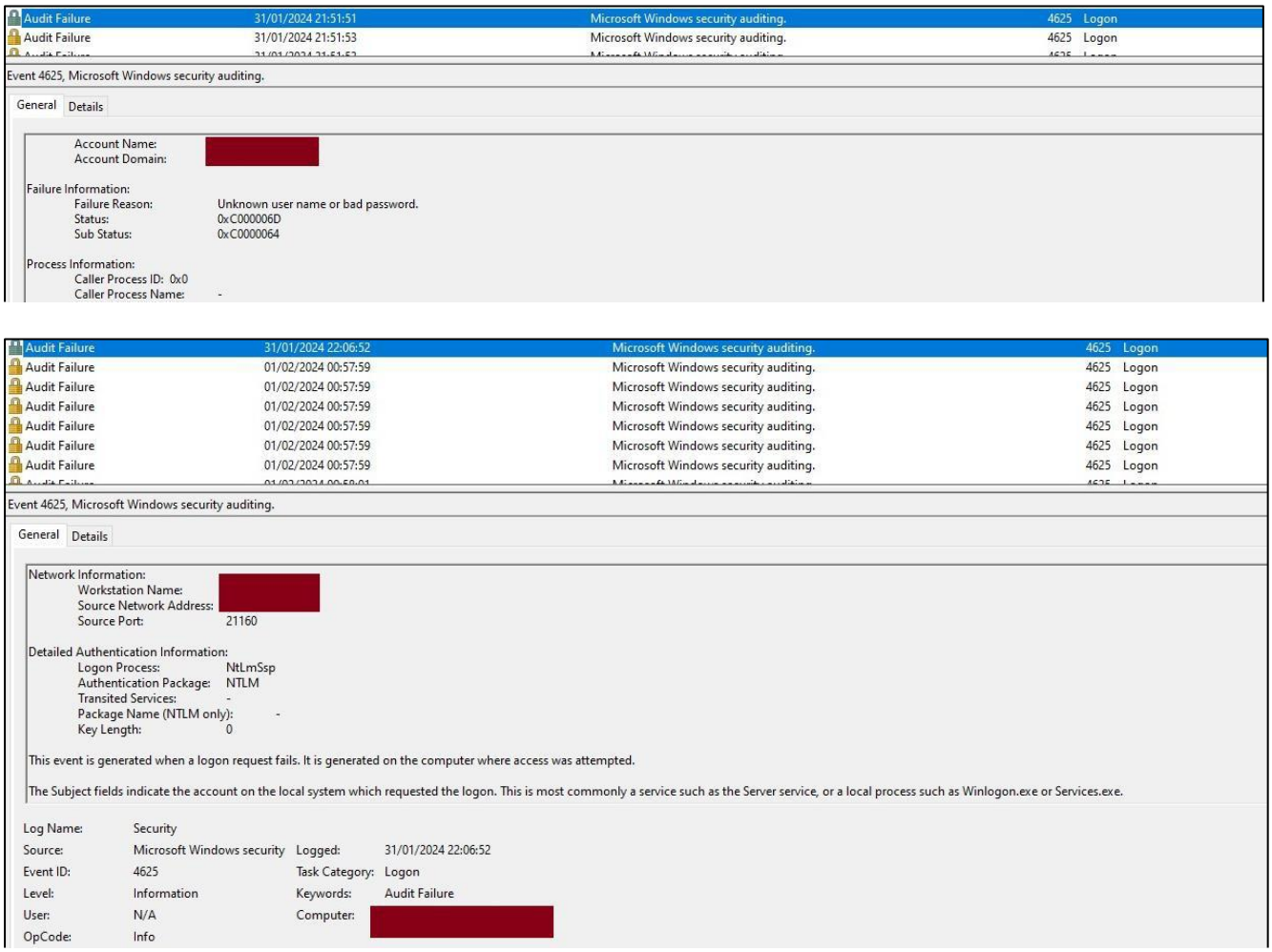


Figura 4. Audit Logs gjatë periudhës së sulmit.

Përditësim 1.1

Nga skanimet dhe analizimet e kryera në infrastrukturë si dhe gjatë procesit të rikthimit të sistemeve, u evidentua se në njërën nga makinat virtuale , gjenden disa skedarë të veçantë që janë krijuar nga aktorët keqdashës për të kryer sulmin brenda rrjetit të Institucionit.

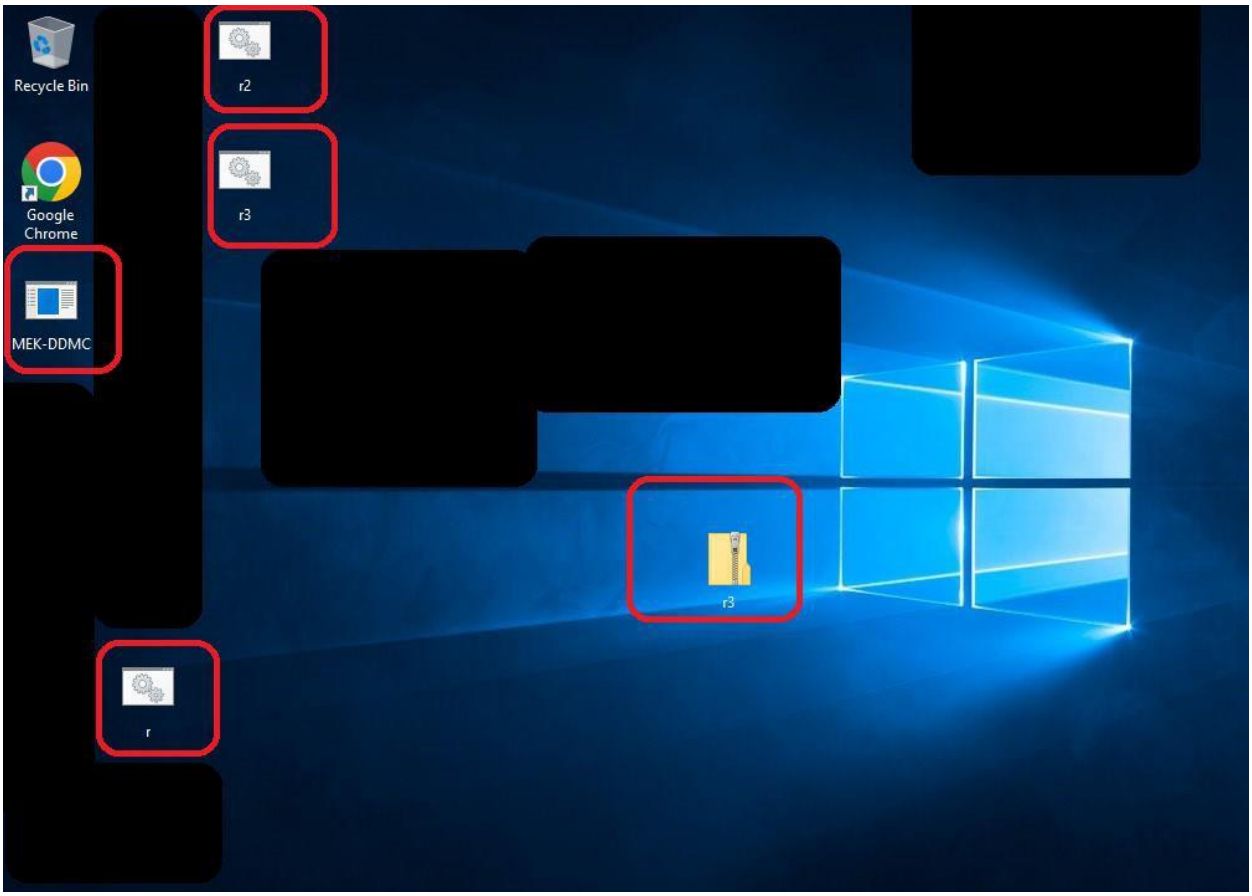


Figura 5. Skedarë të dyshimtë të gjendur në njërën nga makinat virtuale.

Skedarët e evidentuar janë:

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

Analiza e skedarit r.bat

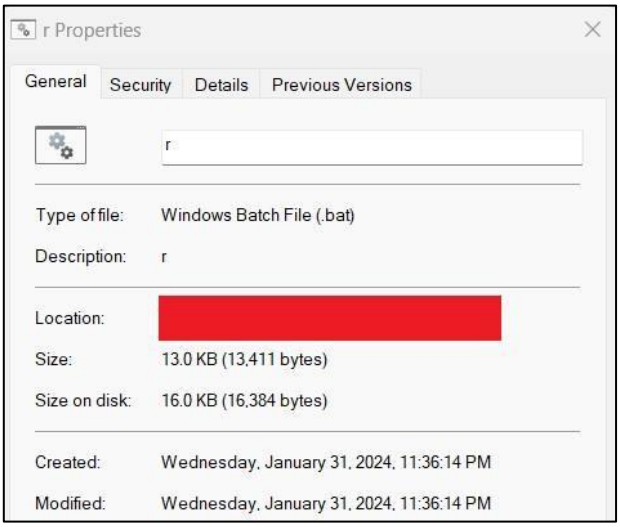


Figura 6. Detaje të skedarit r.bat

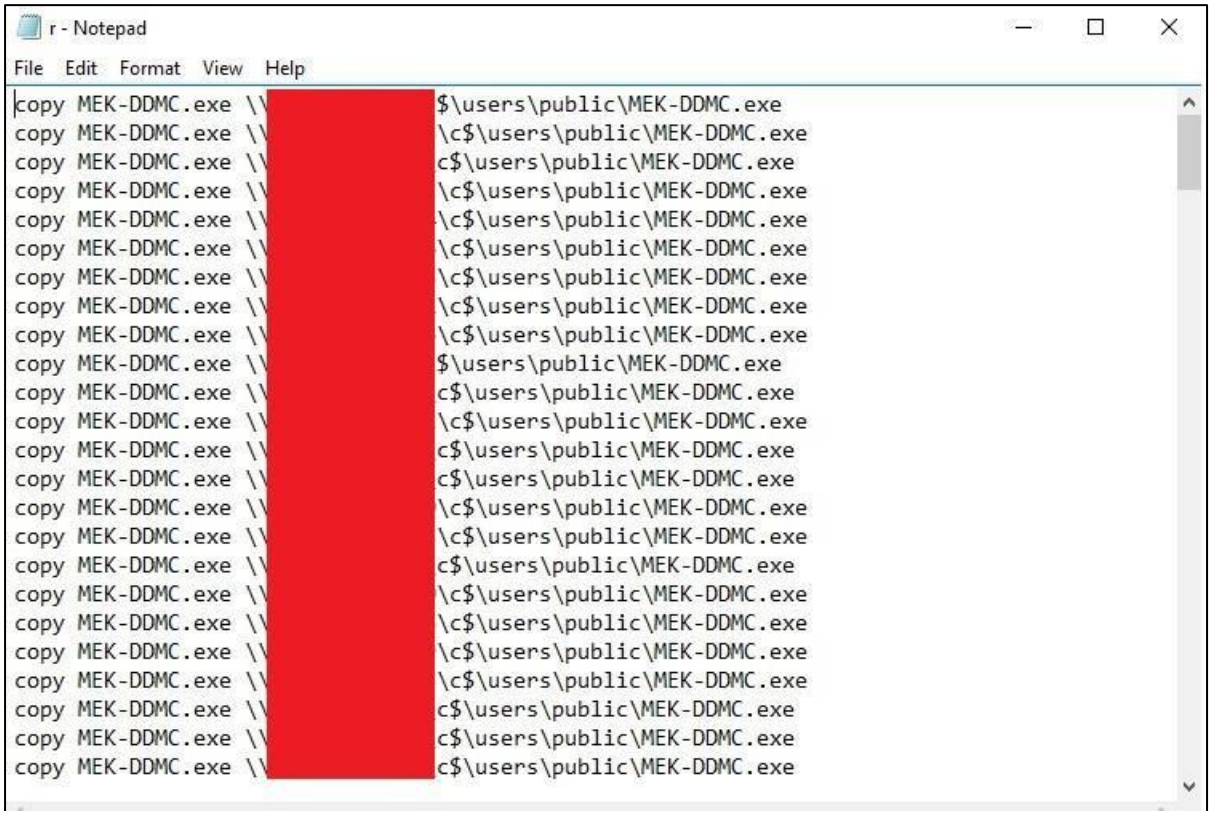


Figura 7. Përmbatja e skedarit r.bat.

Ky skedar ka kryer rolin e transportuesit të skedarit keqdashës **MEK-DDMC.exe**, ku është shpërndarë drejt kompjuterave të evidentuar në rrjetin e infrastrukturës, nëpërmjet direktorisë shared të "***C:\Users\Public.***" që ka qenë i aksesueshëm në rrjet.

Analiza e skedarit r2.bat

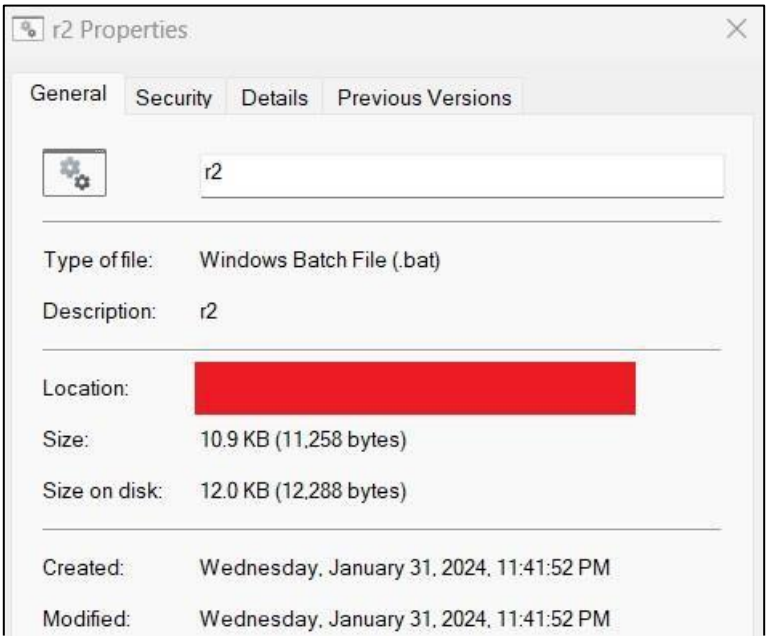
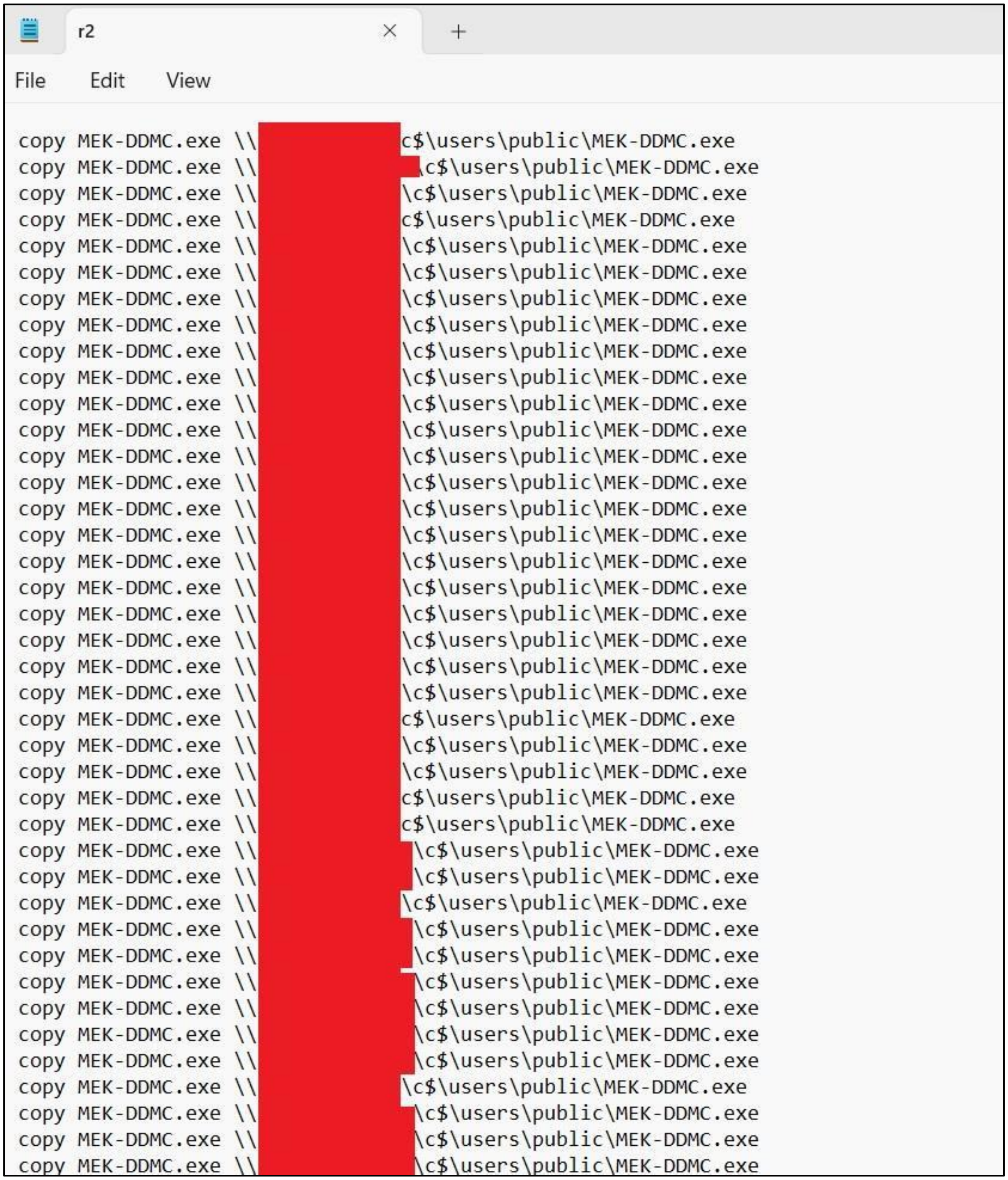


Figura 8. Detaje të skedarit r2.bat.



```
r2
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$\users\public\MEK-DDMC.exe
copy MEK-DDMC.exe \\[redacted]\c$\users\public\MEK-DDMC.exe
```

Figura 9. Përmbajtja e skedarit r2.bat.

Ky skedar i njëjtë me skedarin **r.bat**, kryen transportimin e keqdashës **MEK-DDMC.exe** drejt kompjuterave të evidentuar në rrjetin e infrastrukturës, nëpërmjet direktorisë shared të "***C:\Users\Public.***" që ka qenë i aksesueshëm në rrjet.

Analiza e skedarit r3.bat

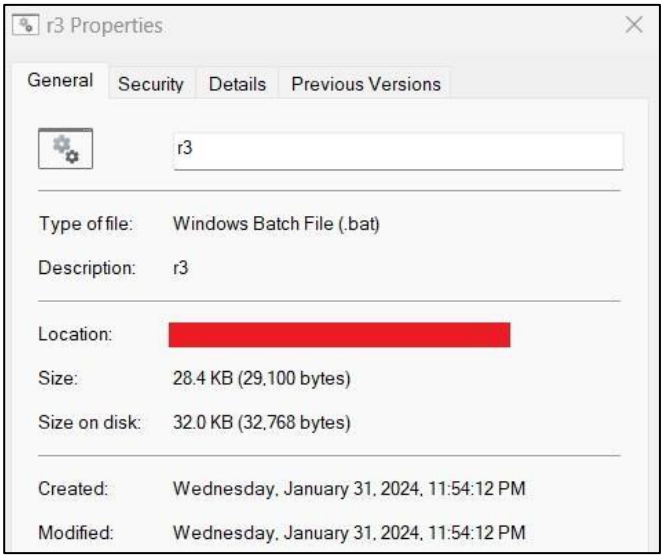


Figura 10. Detaje të skedarit r3.bat.

Figura 11. Përmbajtja e skedarit r3.bat.

Skedari ***r3.bat*** është në renditje i fundit, pasi kryen ekzekutimin nëpërmjet funksionit **wmic (Windows Management Instrumentation Command-line**) , ku kryhet thirrje në distancë (**remote**) për të aksesuar **cmd** dhe më pas komandën për të ekzekutuar **wiper MEK-DDMC.exe.**

Nga analiza e logeve të makinës virtuale evidentohet se ka aktivitet të lartë të përdorimit të protokollit **SMB**, para dhe gjatë sulmit të ndodhur. Evidentohet gjithashtu se aktiviteti i **SMB** është dhe i bllokuar nga disa pajisje kompjuterike ku është tentuar sulmi.

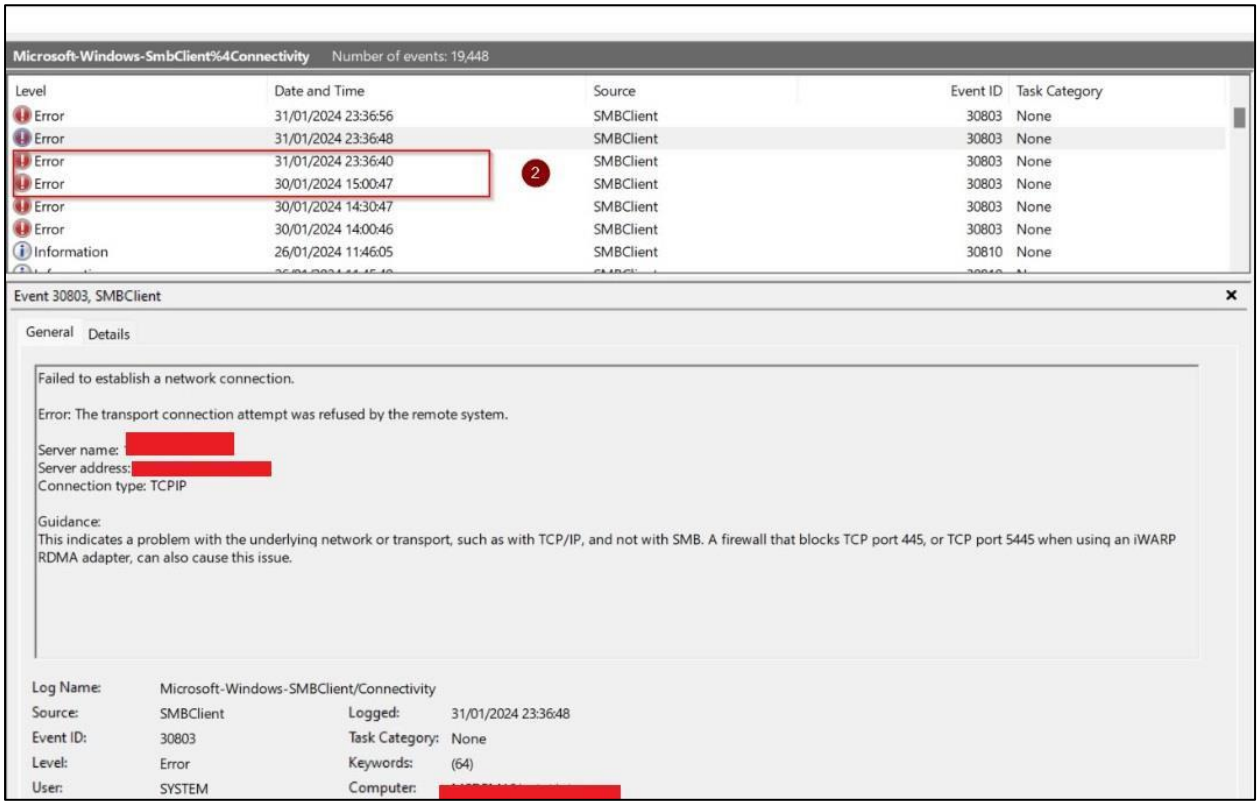


Figura 11. Tentativa SMB drejt rrjetit kur ka filluar komunikimi dhe momenti i sulmit.

.

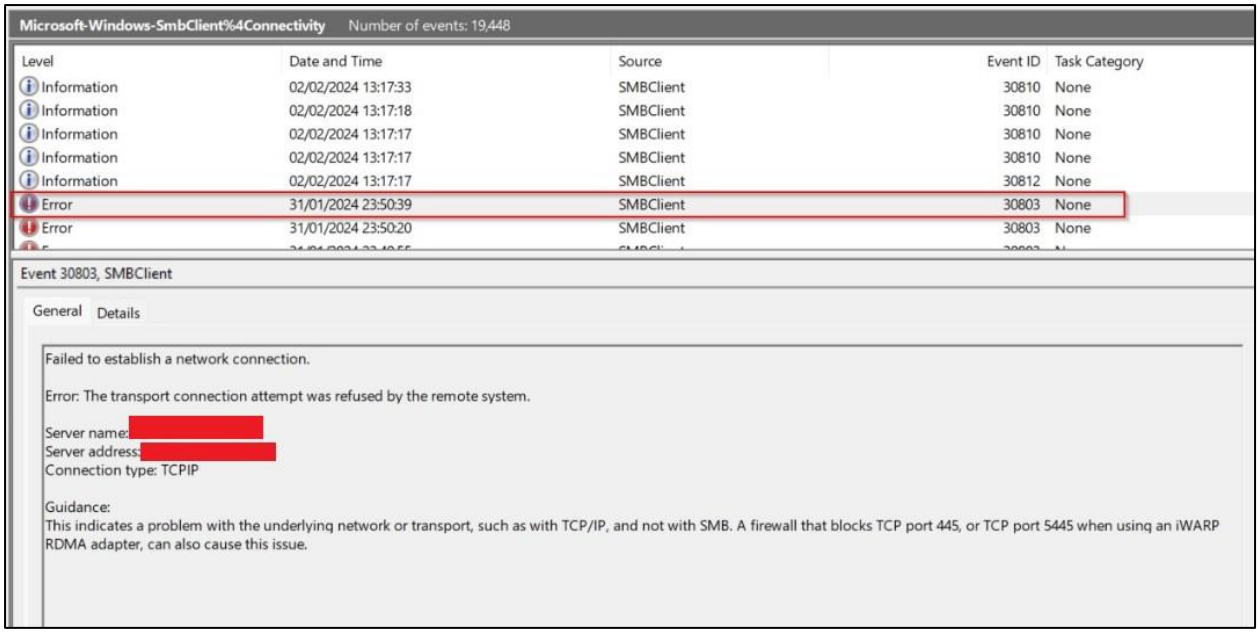


Figura 12. Log i fundit i komunikimit SMB.

Pas këtij momenti është kryer ***wiper*** mbi serverat ku cluster ka qenë i ngritur dhe nuk është arritur më tej të kryhet sulmi pasi ka humbur komunikimi me makinën virtuale dhe rrjetin. Aktualisht nga evidentimet dhe analizimet e kryera rezulton se kur janë ekzekutuar skedarët **.bat,** disa nga pajisjet kompjuterike kanë bllokuar veprimet duke e bërë sulmin të dështojë drejt tyre.

Ndërsa për pajisjet të cilat, kopjimi ka përfunduar me sukses , por ekzekutimi i skedarit **MEK-DDMC.exe** nuk ka ndodhur , kjo për arsye sepse gjatë ekzekutimit të skedarit **r3.bat** me komandën **WMIC**, kjo makinë virtuale ka qenë në renditje më para se pajisjet e tjera kompjuterike që nuk janë prekur nga sulmi. Gjithashtu tek kompjuterat që ka dështuar kopjimi dhe ekzekutimi, **WMIC** nuk ka qenë i aktivizuar si funksion në Windows.

Gjatë analizës evidentohet se drejt makinës virtuale që është përdorur për sulmin, është krijuar lidhje me **Remote Desktop Protocol** (**RDP**) nga një **IP** specifike e infrastrukturës deri në momentin që ka humbur lidhja dhe ka përfunduar sulmi.

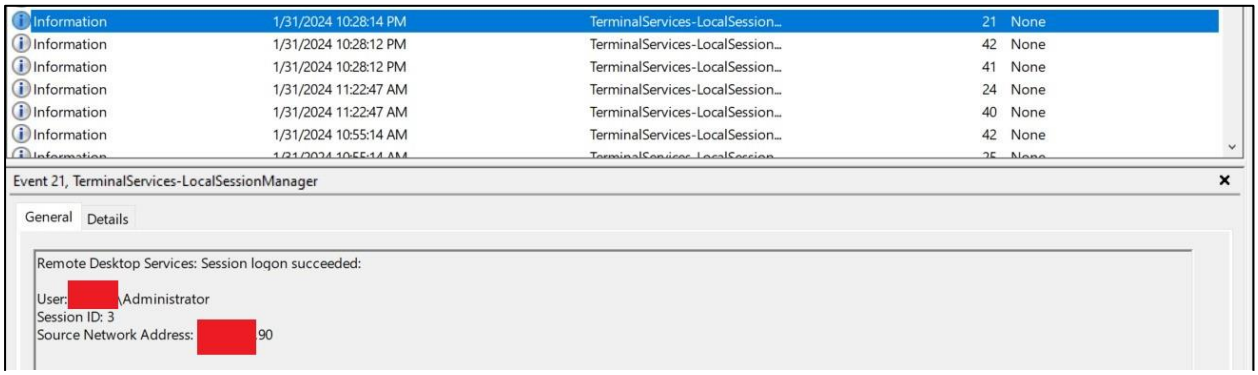


Figura 13. Momenti fillestar i lidhjes RDP drejt makinës virtuale.

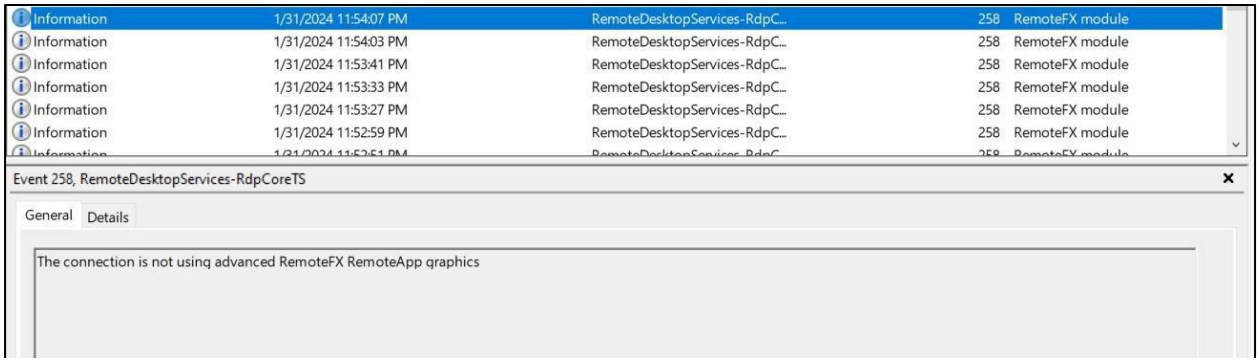


Figura 14. Procesi i shkeputjes së lidhjes RDP dhe përfundimi i sulmit duke përfshirë makinën virtuale..

Analiza e skedarit (detajet e skedarit) *wiper* "*MEK-DDMC.exe"*

- **Analiza Statike:**

Ekzekutuesi ***MEK-DDMC.exe*** vepron si një fshirës i cili është shkruajtur në gjuhën **C/C++** me Visual Studio 2022 version 17.5.

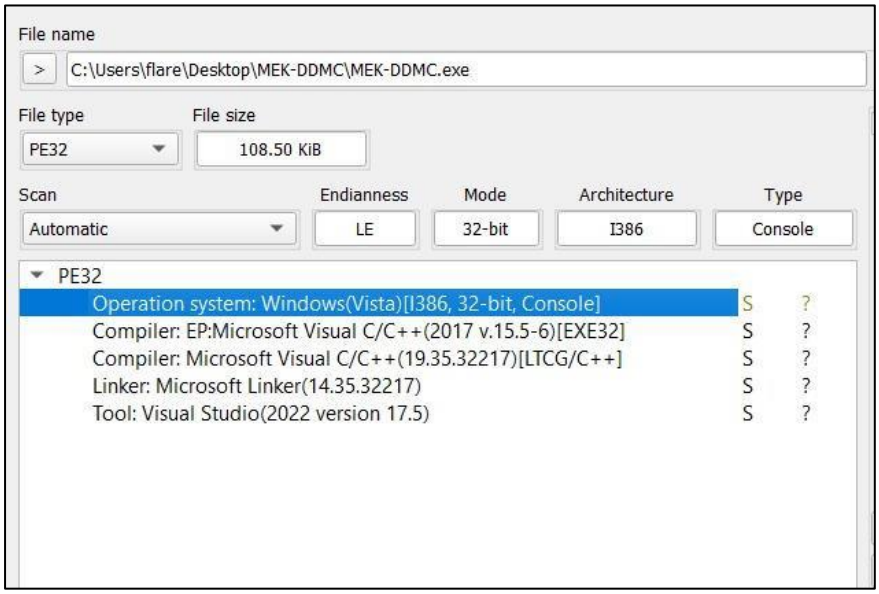


Figura 16. Informacion mbi kodin e wiperit.

Gjatë analizës së kodit të dekompiluar evidentohet se në sektorin ***Debug Data*** kodi përmban informacionin në një program databaze (**PDB**) të Microsoft **.NET,** i cili përdoret për të ruajtur informacionet për dekompilimin dhe debugimin e aplikacioneve **.NET.**
"**RSDS**", vijon një **GUID** (**Global Unique Identifier**) të cilat janë 59 a2 a6 af a4 ... etj., që përdoret për të identifikuar në mënyrë unike skedarin PDB që përputhet me skedarin e ekzekutueshëm të aplikacionit. Pjesa e fundit përshkruan rrugën e skedarit PDB në sistemin e skedarëve, të dhënë si ***"C:\Users\sysprogram...".*** Kjo tregon vendndodhjen fizike të skedarit **PDB** në diskun e kompjuterit ku është krijuar ose modifikuar për herë të fundit.Gjatë kërkimit të karaktereve apo fjalëve të dekompiluara evidentohet stringu **"u"\\\\.\\%c:"** .Nëse klikojmë në këtë string dekompiluesi të dërgon në funksionin **void FUN_00401010(void)** nga ku arrihet në konkluzionin se në këtë funksion ndodh pjesa e fshirjes së të dhënave.
Ekzekutuesi *MEK-DDMC.exe dërgon komandën* ***IOCTL_DISK_DELETE_DRIVE_LAYOUT*** duke përdorur ***DeviceIoControl.*** Kjo komandë bën të mundur fshirjen e nënshkrimit *(boot signature)* nga MBR, duke rezultuar që kompjuteri të mos jetë në gjendje më të aksesohet si pasojë e fshirjes së gjithë diskut.
Në kod duken variabla dhe shënjues, ku ngarkohet ***kernel32.dll*** duke përdorur ***LoadLibraryW*** dhe përdor funksionin ***GetProcAddress*** për të gjetur adresat e disa funksioneve që janë përcaktuar e

më pas kontrollon nëse është e pasaktë. Nëse nuk është do të thërrasi ***DeviceIoControl*** me **proces handle** e hapur më parë dhe flagun **0x7c100.**
Flagu ***0x7c100*** është ***IOCTL_DISK_DELETE_DRIVE_LAYOUT*** që përdoret për të fshirë particionimin e tabelës dhe informacionin e diskut.

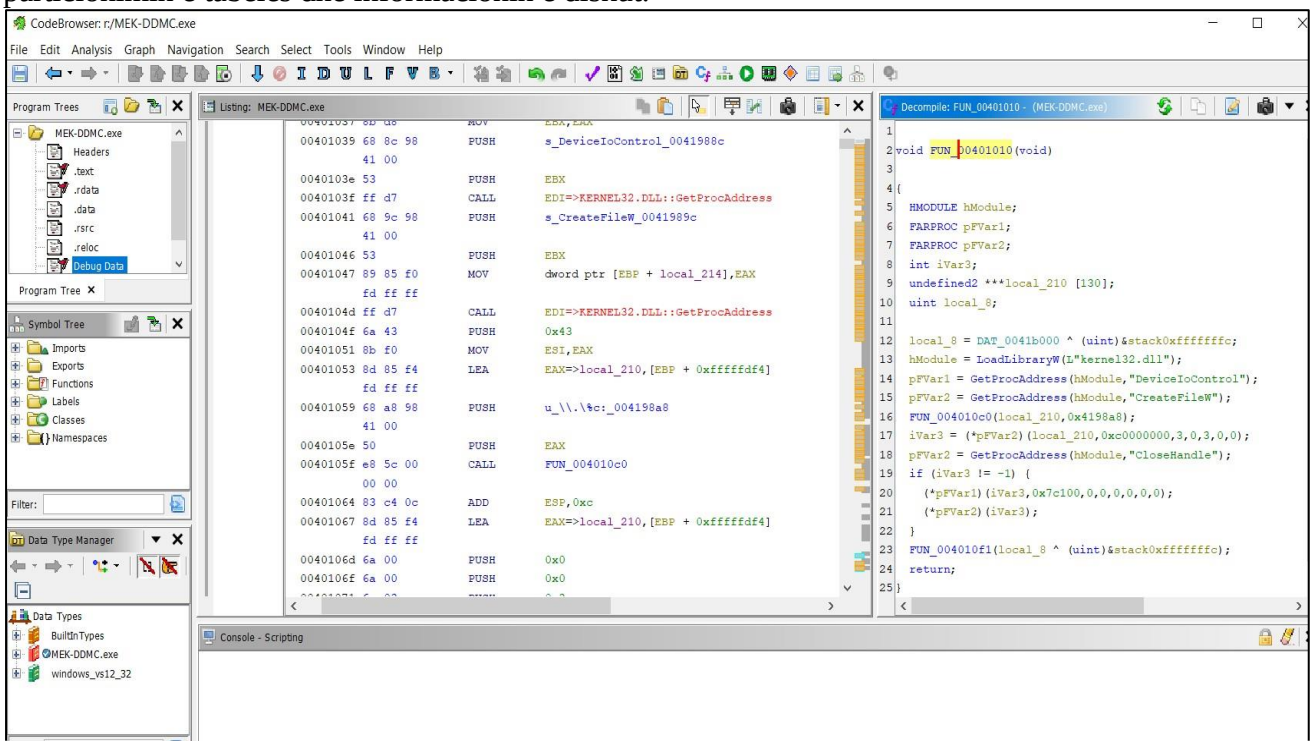


Figura 17. Kodi që realizon fshirjen e të dhënave.

Nëse ndryshojmë formatin e dokumentit nga **.exe** ne **.7z** dhe tentojmë ta ekstraktojmë, evidentohet se ka skedarë të ndryshëm si në figurën e mëposhtme:

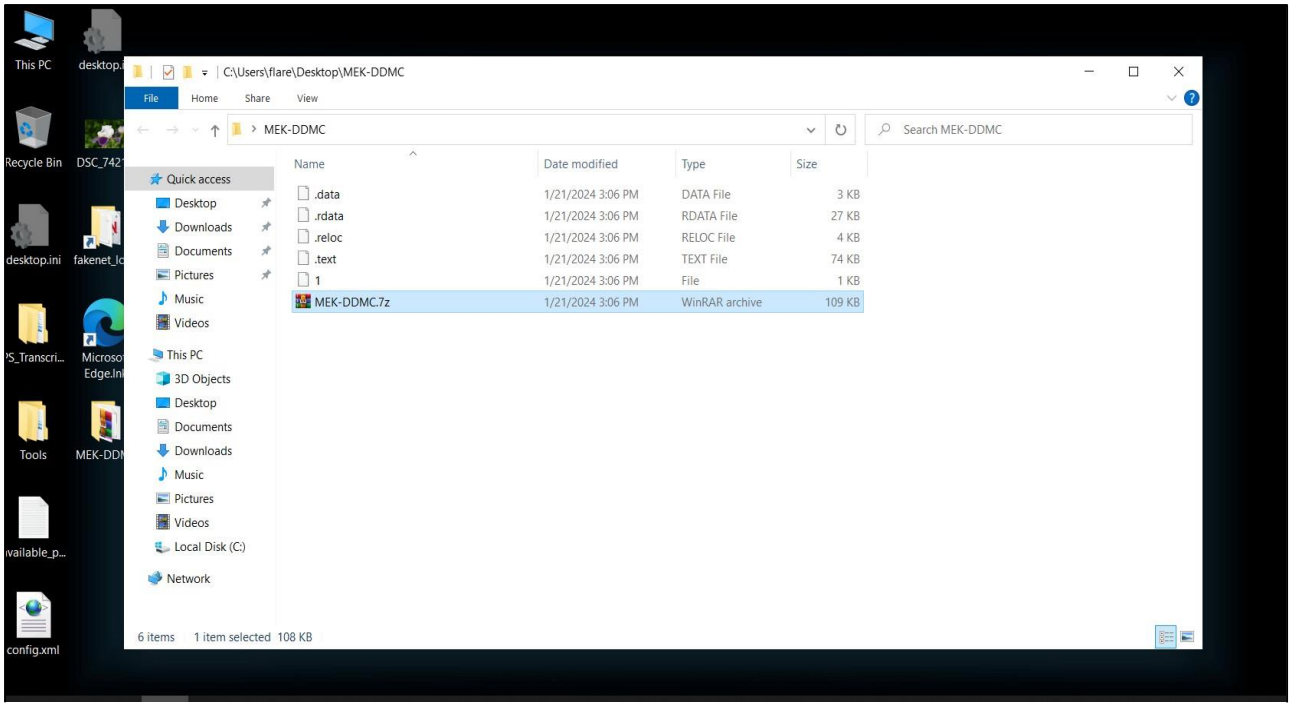


Figura 18. Ekstraktimi i MEK-DDMC.7z.

Skedari me emër "***1"*** është një skedar që nëse hapet me anë të **Notepad ++,** ai përmban një format **XML** ,nga ku përcakton se aplikacioni do të ekzekutohet me të njëjtin nivel privilegji si procesi që e thërret. **level='asInvoker',** ku do të thotë se aplikacioni nuk kërkon ***privilegje të larta*** për tu ekzekutuar dhe uiAccess='false' specifikon se aplikacioni nuk ka akses në ndërfaqet e përdoruesit që janë të privilegjuara (UI).

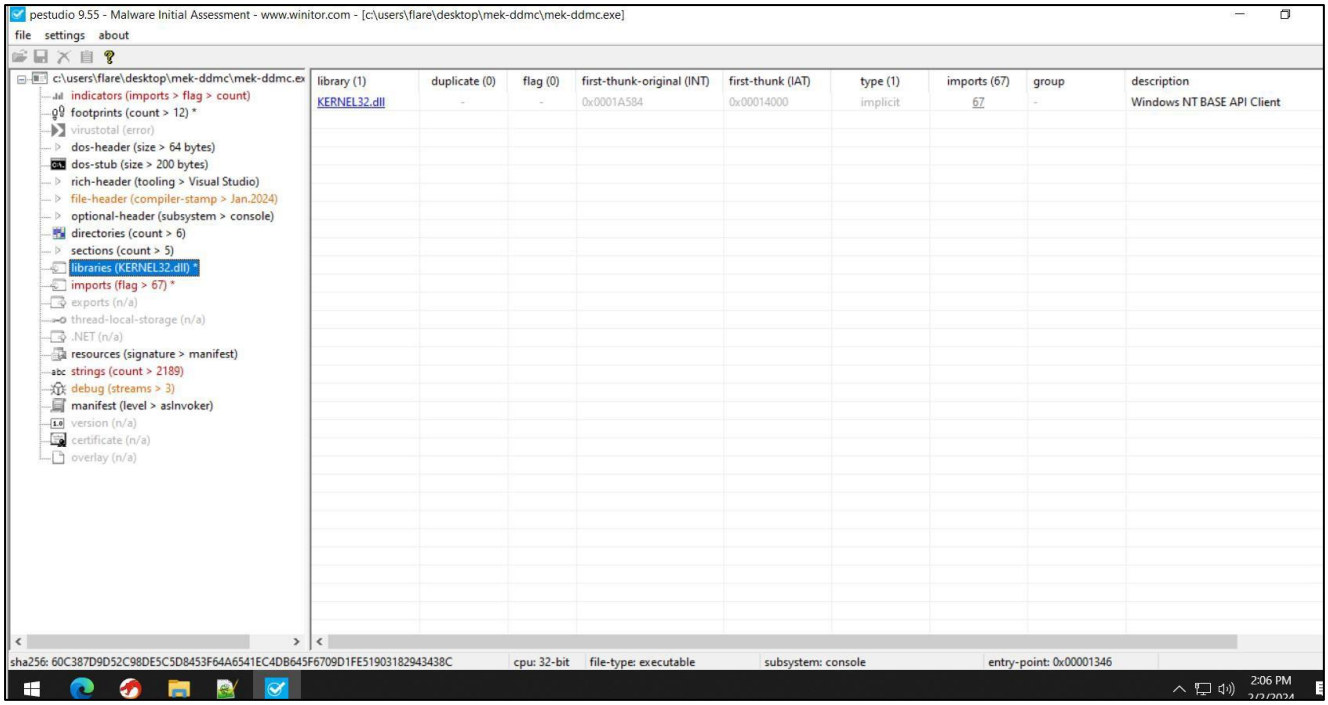


Figura 19. Importimi i Kernel32.dl.

IOCTL_DISK_DELETE_DRIVE_LAYOUT	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.

Figura 20. IOCTL DISK DELETE

Aftësitë e MEK-DDMC.exe:

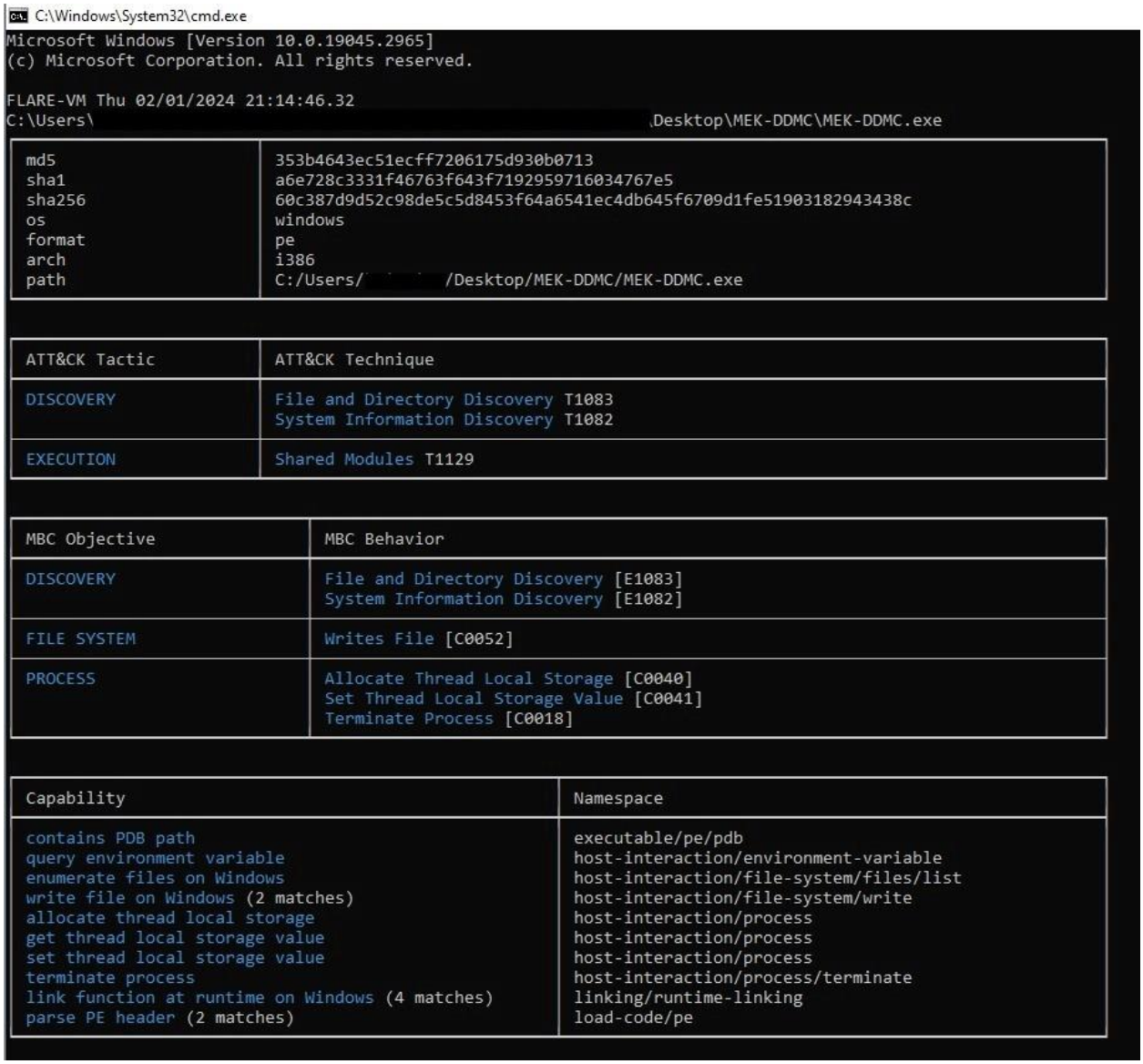


Figura 5. Aftësitë e Malware

- **Analiza Dinamike:**

Për të kuptuar sjelljen e malware u krye analiza dinamike që paraqet ekzekutimin e tij.

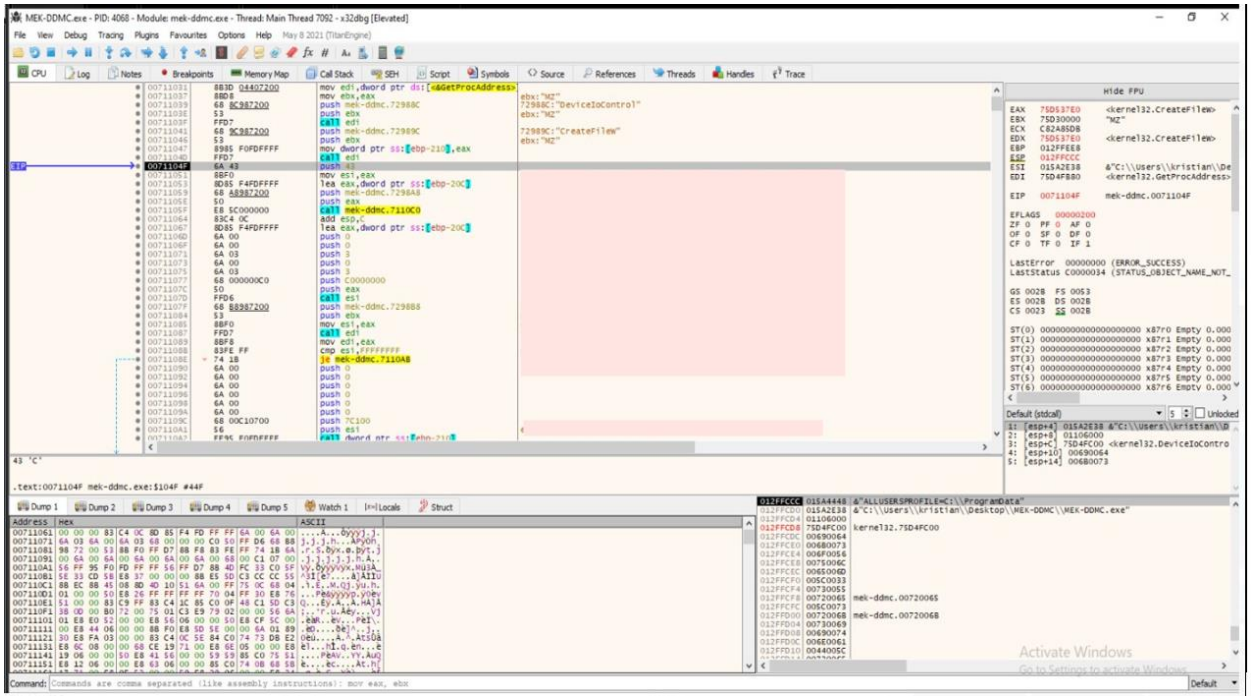


Figura 22. Debug i MEK-DDMC.exe.

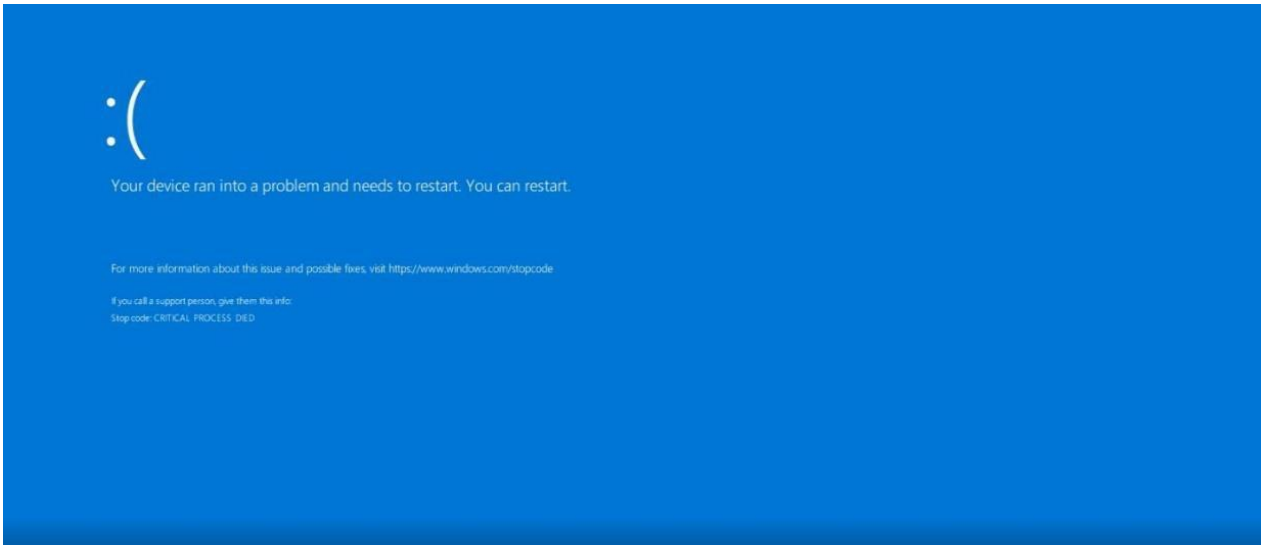


Figura 23. Tentativat pas reboot.

Pas ekzekutimit të ***MEK-DDMC.exe,*** sistemi operativ kryen një restart të detyruar dhe kur tentohet startimi i sistemit operativ, dështon në gjetjen e direktorisë ***BOOT.***

Përditësim 1.2 – Riparimi i Sistemit Operativ

Nga testimet e kryera në ambjentet e laboratoreve të AKCESK, u analizua sjellja e skedarit **MEK-DDMC.exe** dhe u tentua në disa sisteme operative procesi i riparimit dhe i rikthimit fillimisht të skedarëve të rregullt të një sistemi operativ dhe më pas rikthimi i plotë i gjithë sistemit. Faza e testimit përfshihet në ambjente sistemesh te ngritura në makina ***fizike*** si dhe makina ***virtuale***.

Nga analiza e kryer evidentohet se skedari malinj prek vetëm rekordin e ***BOOT*** dhe nuk prek detaje të tjera për të kompromentuar sistemin operativ. Fillimisht u tentua të rikthehen ***Partition*** që gjenden në diskun kryesor ku sistemi operativ është i instaluar.

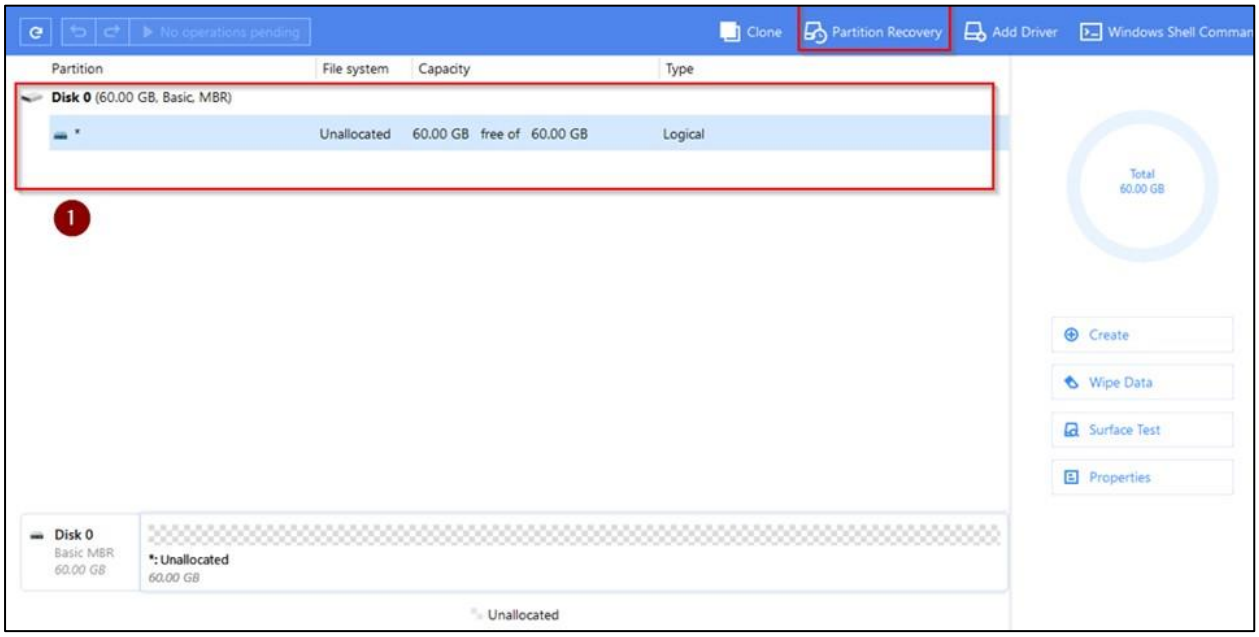


Figura 24. Procesi i rikthimit të Partition.

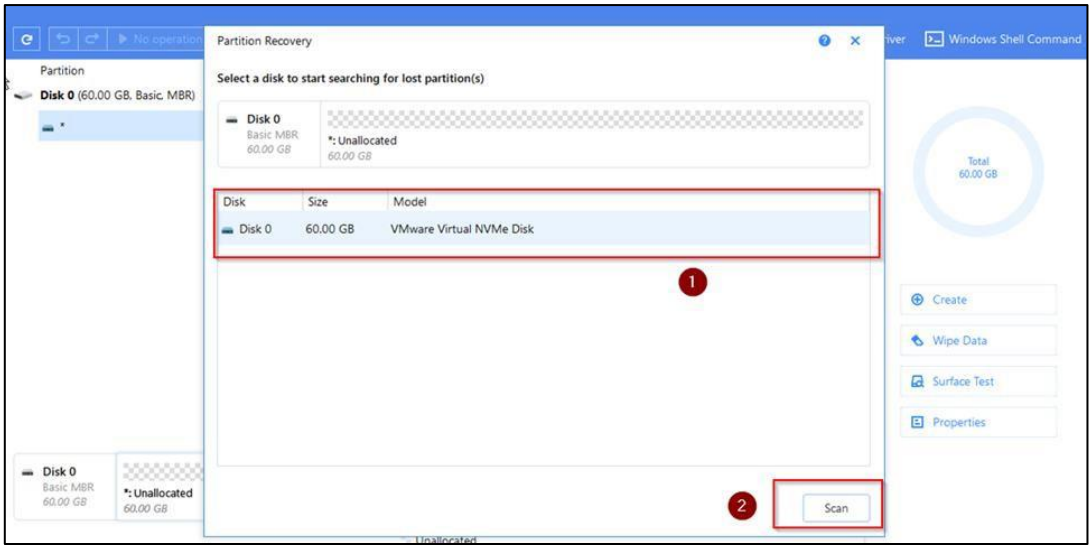


Figura 25. Fillimi i skanimit për Partitions të humbur në diskun kryesor të sistemit operativ.

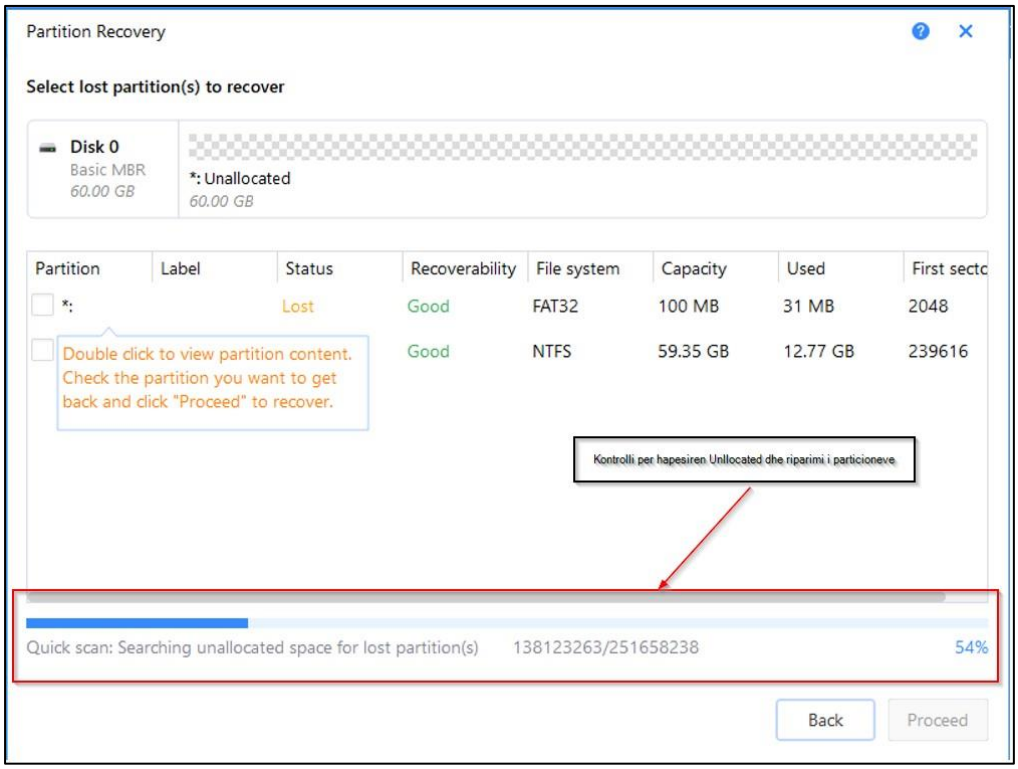


Figura 26. Procesi i skanimit ku rikthehen Partitions të humbur.

Gjatë procesit të skanimit evidentohet se rikthehen të gjithë ***Partitions*** që kanë qenë të konfiguruar në diskun kryesor të sistemit operativ.

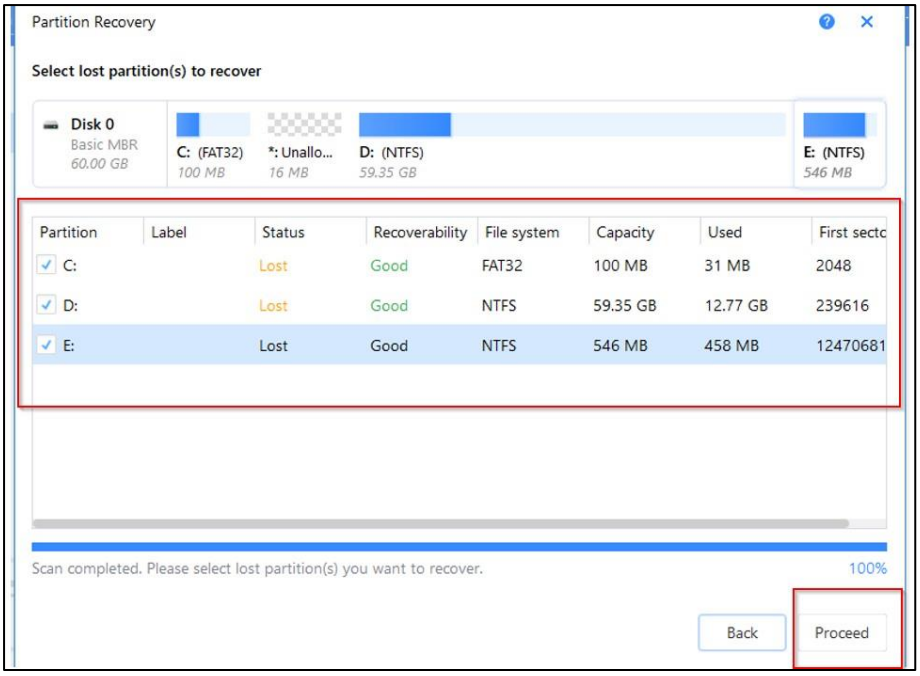


Figura 27. Përfundimi i skanimit për Partitions të humbur.

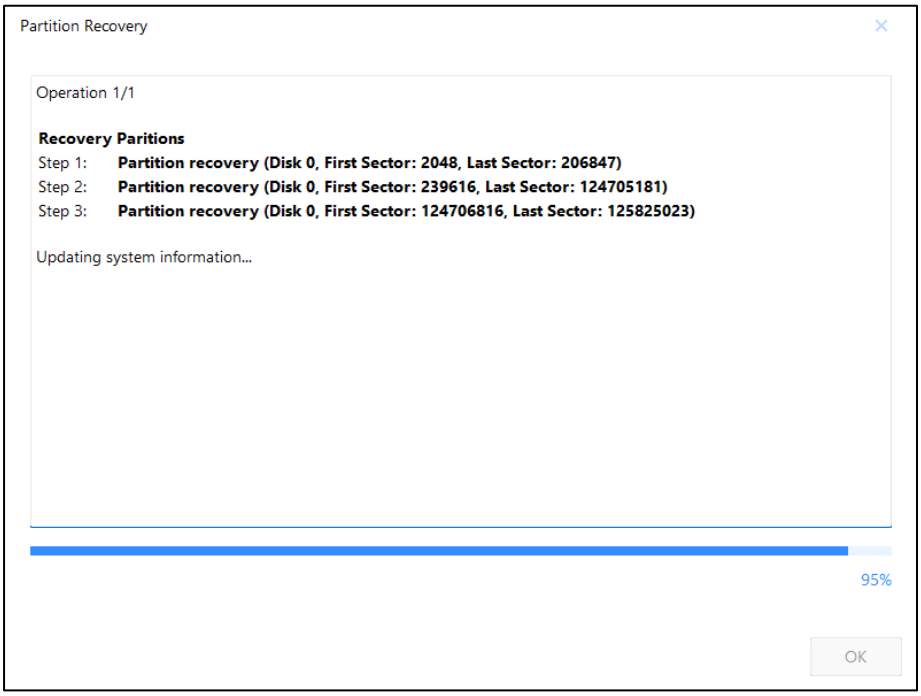


Figura 28. Partition të rikthyer.

Më tej u krye një kontroll për paraqitjen e partition nga ku evidentohet se janë të dukshme në ***Disk Management,*** gjithashtu se skedarët legjitim nuk janë prekur nga ***wiper.***

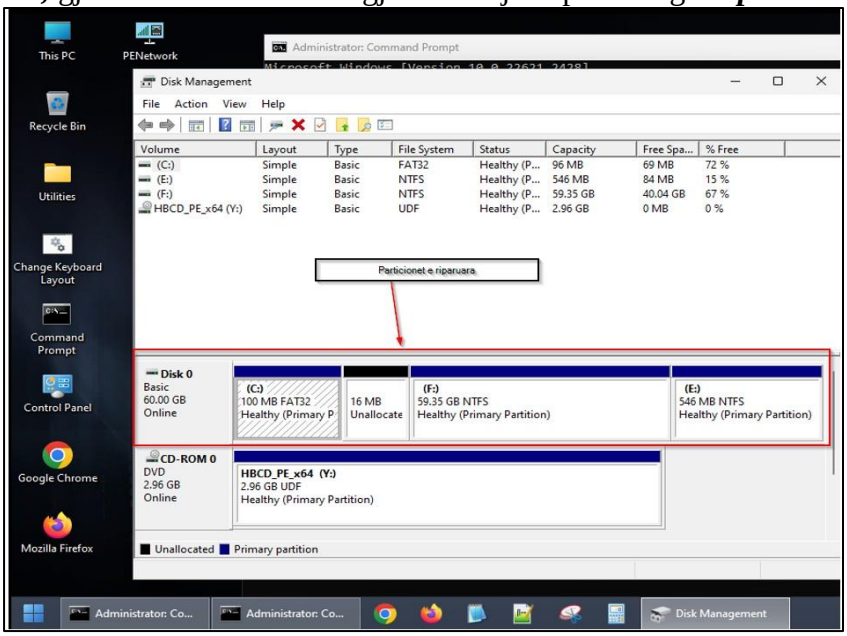


Figura 29. Renditja e Partition Volume të rikthyer.

Pas evidentimeve të kryera është e nevojshme të riparohet **BCD Boot** i sistemit operativ që rikthimi në Windows të jetë përfundimtar. Nëse tentohet të riniset sistemi operativ pa riparuar skedarin e Boot do të paraqesë errorin ***0xc000000e.***

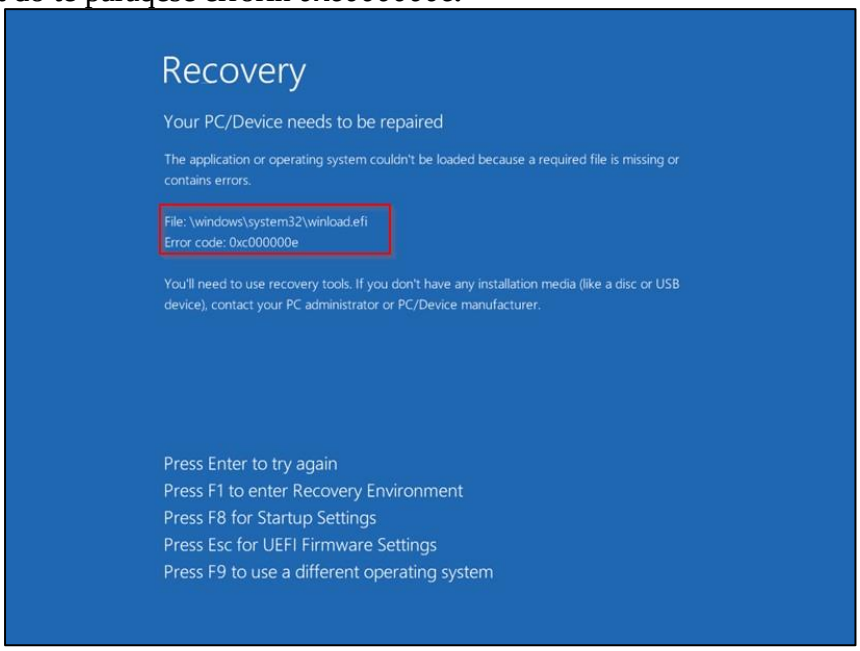


Figura 30. winload.efi error 0xc000000e.

Riparimi i BCD BOOT

Fillimisht duhet të zgjidhet aktiv partition **EFI** ku është i konfiguruar automatikisht **BootLoader** i sistemit operativ.

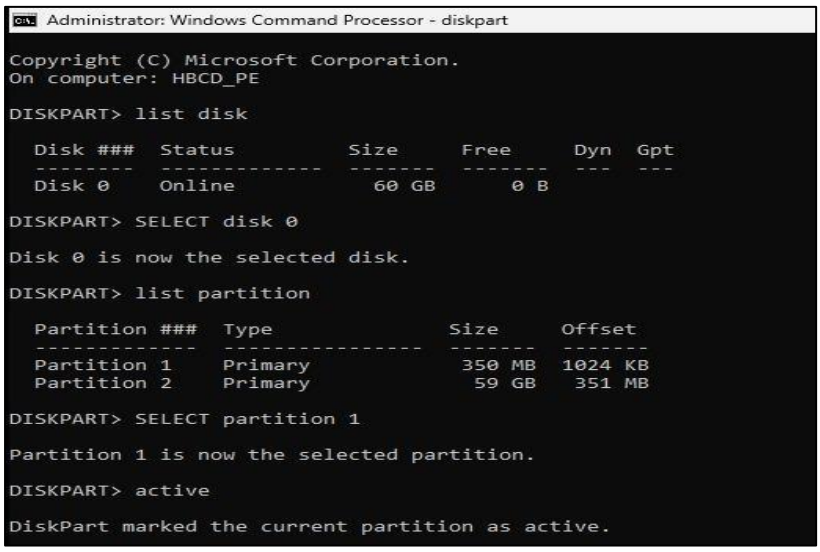


Figura 31. Procesi i kryerjes aktiv të Partition EFI.

Pas aktivizimit të partition **EFI** kryhet riparimi i **BCD** .

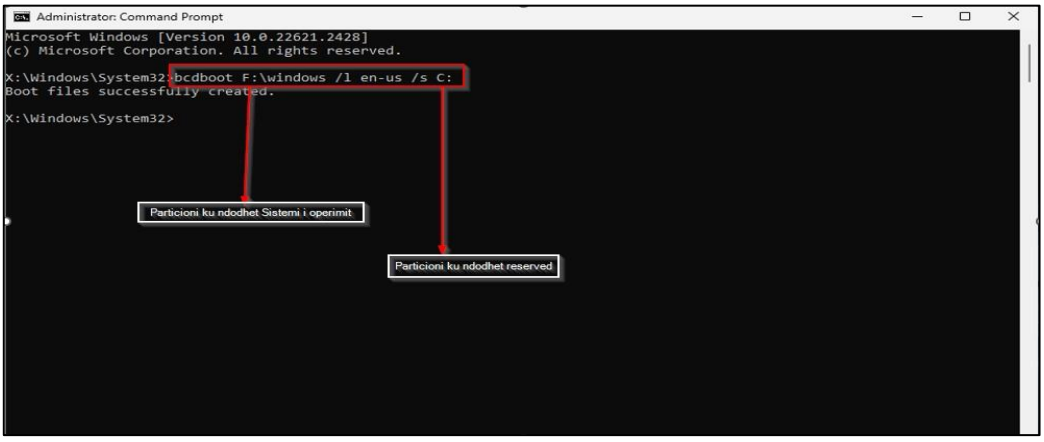


Figura 32. Komanda për riparimin e BCDBOOT.

Shkronjat e Volume Partition ndryshojnë sipas sistemit të operimit apo konfigurimeve të kryera më parë.

Më pas tentohet rinisja për sistemin operativ dhe nga të gjitha testet e kryera rezulton funksional.

Indikatorët e kompromitetit

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

md5 - 353b4643ec51ecff7206175d930b0713
sha1 - a6e728c3331f46763f643f7192959716034767e5
sha256 - 60c387d9d52c98de5c5d8453f64a6541ec4db645f6709d1fe51903182943438c

HASH: ***r.bat***
sha256 -
B936B644AEBA0266798C791147B41C3486BFBCE34B6EF82ACC9F28526D74D8DB

HASH: ***r2.bat***

sha256 -
6CA2DB9BDFF6455B4E71CAD59A4A329D17F36510230A3B961516B4F2C033AB3F

HASH: r3.bat

sha256 –
37D2AD10ACB355896BF4D1747E809A9709F14892B199EF8C182812D306D3565B