FormBook Malware Technical Analysis - CYFIRMA

Archived: 2026-04-05 15:57:38 UTC

Published On : 2021-11-17

Overview

Risk Score: 8

Confidence Level: High

Suspected Malware: FormBook Malware/Trojan

Function: Information Stealing, Credential Harvesting and download/drops stealthier malware

Tactic Used: Process Injection/Process Hollowing

Threat actor Associations: ng-Code

Other Malware related to FormBook: XLoader

First Seen: July 2016

Latest Seen: Nov 2021

Target Industry: Multiple

Target Countries: Multiple/Global Effect but predominately the US

Relevancy: Global Effect and used the latest zero-day vulnerability of Office-365 in 2021.

Brief Introduction: FormBook Malware is quite popular among attackers. It is basically an information stealer/trojan and is available in darkweb market as a Malware-as-Service. It is first seen in July 2016 and has been quite active since then. In 2020 it affected 4% of organizations worldwide and was among the top 3 list of trending malware. It logs and monitors keystrokes, searches and accesses files, takes screenshots, harvests credentials from different browsers, drops files, downloads, and executed stealthier malware as per commands received from Command-and-Control-Server (C2).

XLoader appears in 2020, consider as the successor of FormBook having similarities on the base of code and also advertise for sale in the same dark-web forums where FormBook was earlier sold. XLoader also has the capability to compromise macOS.

FormBook is mainly distributed using email campaigns, various infecting mechanisms and different types of file attachments including pdfs, doc, RTF document, exe, zip, rar etc. It takes advantage of various vulnerabilities like CVE-2012-0158 (Microsoft Windows Common Controls ActiveX Control Arbitrary Code Execution Vulnerability), CVE-2017-01182 (Microsoft Office Memory Corruption Vulnerability), CVE-2017-0199 (Microsoft Office/WordPad Remote Code Execution Vulnerability), and recently used an Office-365 zero-day vulnerability CVE-2021-40444 (Microsoft MSHTML Remote Code Execution Vulnerability).

File Details: As shown in Figure1, the following are the details related to the malware “FormBook”

File Type: Windows PE-32 Executable

MD5: c504f8e950801fd90e45b01023c29702

SHA256: be24cc41a8c8b2c292743055cccd8a9ca25eddcaa26aa984a63a6dff70ddae55

Subsystem: GUI

Compilation Time: April 2016

Figure 1

```
formbook3_be24.exe: PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Microsoft executable, portable (PE)
402064        0x62290         XML document, version: "1.0"
402976        0x62620         LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, missing uncompressed size
408718        0x63C8E         LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, missing uncompressed size
```

Figure1 above shows that FormBook Malware is a Windows PE-32 Executable and has the signature of Nullsoft Installer. The file has different parts, one PE executable along with an embedded XML document and two lzma compressed files.

Figure2 and Figure 3 show the different hash values corresponding to our malware file. Figure 2 also other basic information like it has GUI subsystem and compilation time of April 2016.

property	value
md5	C504F8E950801FD90E45B01023C29702
sha1	BCFB99843E09FA0426D9BAA404C9364BBCD20E5C
sha256	BE24CC41A8C8B2C292743055CCCD8A9CA25EDDCAA26AA984A63A6DFF70DDAE55
md5-without-overlay	F5537CA97FD6E9330EBFD504EAA9FD7E
sha1-without-overlay	9B4995B5995D96582FF804D82095F6182F817E5C
sha256-without-overlay	6ED962996B7CD129407629CB51B4173085CA2BF8C552A379646F318C61750AC6
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z ..... @ .....
file-size	659405 (bytes)
size-without-overlay	402944 (bytes)
entropy	5.443
imphash	n/a
signature	n/a
entry-point	81 EC 84 01 00 00 53 55 56 57 33 DB 68 01 80 00 00 89 5C 24 20 C7 44 24 14 68 91 40 00 89 5C 24 1C
file-version	n/a
description	n/a
file-type	**executable**
cpu	**32-bit**
subsystem	GUI
compiler-stamp	0x56FF3A65 (Sat Apr 02 08:50:05 2016)

Figure2

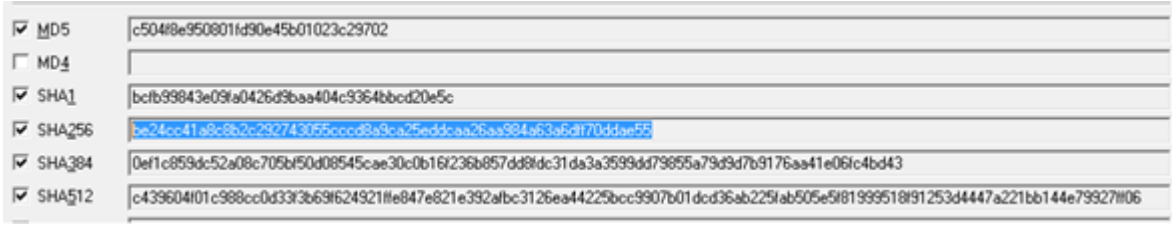

Figure3

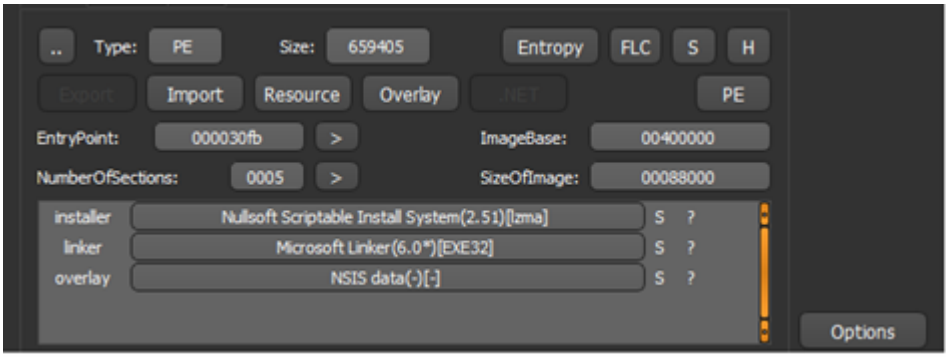

Figure4

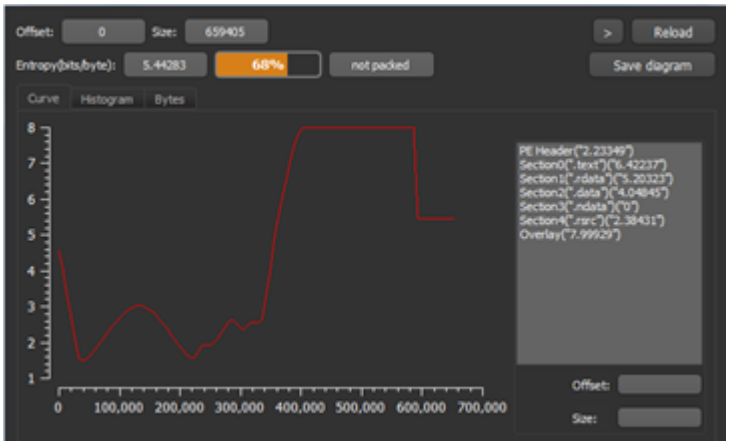

Figure5

Figure4 above shows that the malware has an NSIS installer, and it is present in the overlay part. We further examine and extract it. Figure5 shows the entropy curve corresponding to the malware. It mentioned it as not packed but the curve at the end is somewhat flat with high entropy provides us an indication of the presence of some packed code inside the executable file.

Figure6

Elastic	malicious (high confidence)
McAfee	Artemis!C504F8E95080
Sangfor	Trojan.Win32.Injector.EQKW
Alibaba	Trojan:Win32/Lokibot.98f995d6
Cyren	W32/Injector.AMK.gen!Eldorado
Symantec	Packed.Generic.606
ESET-NOD32	a variant of Win32/Injector.EQKW
APEX	Malicious
Paloalto	generic.ml
Kaspersky	UDS:Trojan-Spy.Win32.Noon.gen
BitDefender	Dropped:Trojan.GenericKDZ.79521
MicroWorld-eScan	Dropped:Trojan.GenericKDZ.79521
Avast	Win32:PWSX-gen [Trj]
Ad-Aware	Dropped:Trojan.GenericKDZ.79521
Emsisoft	Dropped:Trojan.GenericKDZ.79521 (B)
McAfee-GW-Edition	BehavesLike.Win32.Dropper.jm
FireEye	Generic.mg.c504f8e950801fd9
Ikarus	Trojan.NSIS.Agent
GData	Dropped:Trojan.GenericKDZ.79521
Arcabit	Trojan.NSISX.Spy.Gen.1
Microsoft	Trojan:Win32/Lokibot.SISN!MTB
MAX	malware (ai score=86)
Malwarebytes	Trojan.Injector
SentinelOne	Static AI - Suspicious PE
AVG	Win32:PWSX-gen [Trj]
Cybereason	malicious.950801
Panda	Trj/CI.A

When we check, the malicious file in different anti-virus engines then it is detected as primarily a trojan/spyware/information stealer which is the main function of the FormBook malware.

Figure7

property	value	value	value	value	value
name	.text	.rdata	.data	.ndata	.rsrc
md5	C8ACF839F47203D12AD6CE...	94F06CEBBBCCED874AA75B...	87BF5D11434348EF3F172E2A...	n/a	865290A656F1AC54775FB2B...
entropy	6.422	5.203	4.048	n/a	2.384
file-ratio (60.95%)	3.57 %	0.70 %	0.23 %	n/a	56.45 %
raw-address	0x00000400	0x00006000	0x00007200	0x00000000	0x00007800
raw-size (401920 bytes)	0x00005C00 (23552 bytes)	0x00001200 (4608 bytes)	0x00000600 (1536 bytes)	0x00000000 (0 bytes)	0x0005AE00 (372224 bytes)
virtual-address	0x00401000	0x00407000	0x00409000	0x00425000	0x0042D000
virtual-size (543257 bytes)	0x00005AEB (23275 bytes)	0x00001196 (4502 bytes)	0x0001B038 (110648 bytes)	0x00008000 (32768 bytes)	0x0005AD60 (372064 bytes)
entry-point	0x000030FB	-	-	-	-
writable	-	-	x	x	-
executable	x	-	-	-	-

Figure7 above shows us different sections present in the FormBook. All are quite normal except .ndata which is totally a virtualized section means only available in memory.

Figure8

library (7)	blacklist (0)	type (1)	imports (152)	description
kernel32.dll	-	implicit	58	Windows NT BASE API Client DLL
user32.dll	-	implicit	62	Multi-User Windows USER API Client DLL
gdi32.dll	-	implicit	8	GDI Client DLL
shell32.dll	-	implicit	6	Windows Shell Common Dll
advapi32.dll	-	implicit	10	Advanced Windows 32 Base API
comctl32.dll	-	implicit	4	Common Controls Library
ole32.dll	-	implicit	4	Microsoft OLE for Windows

Figure8 above shows different libraries imported by the FormBook. All are important and provide us an indication of the functionality the malware incorporates. It includes memory, low-level functioning, user interface, graphical manipulation, registry access and manipulation capabilities. Shell32.dll and Ole32.dll are quite important here as ole32.dll is used for handling ole objects and is required for embedding ole objects of different applications to another application like excel-sheet embedded into a word document whereas shell32.dll is used to open webpages and files.

Figure9

name (152)	group (13)	MITRE-Technique (5)
SetWindowPos	windowing	-
GetMessagePos	windowing	-
CallWindowProcA	windowing	-
IsWindowVisible	windowing	-
SetForegroundWindow	windowing	-
GetWindowLongA	windowing	-
RegisterClassA	windowing	-
DispatchMessageA	windowing	-
PeekMessageA	windowing	-
SendMessageA	windowing	-
DefWindowProcA	windowing	-
CreateWindowExA	windowing	-
SetWindowLongA	windowing	-
SendMessageTimeoutA	windowing	-
FindWindowExA	windowing	-
IsWindow	windowing	-
DestroyWindow	windowing	-
ShowWindow	windowing	-
GetTickCount	system-information	T1124
GetWindowsDirectoryA	system-information	-
GetSystemDirectoryA	system-information	-
ExpandEnvironmentStringsA	system-information	-
GetSystemMetrics	system-information	-
WaitForSingleObject	synchronization	-
SetCurrentDirectoryA	storage	-
SearchPathA	storage	-
GetDiskFreeSpaceA	storage	-
LoadCursorA	resource	-
GetPrivateProfileStringA	registry	-
WritePrivateProfileStringA	registry	-
RegDeleteValueA	registry	T1112
RegOpenKeyExA	registry	-
RegDeleteKeyA	registry	T1112
RegEnumValueA	registry	T1012
RegCloseKey	registry	-
RegCreateKeyExA	registry	-
RegSetValueExA	registry	T1112
RegQueryValueExA	registry	-
RegEnumKeyA	registry	T1012
GlobalUnlock	memory	-
GlobalLock	memory	-
GlobalFree	memory	-
GlobalAlloc	memory	-
CoTaskMemFree	memory	-
IsWindowEnabled	keyboard-and-mouse	-
EnableWindow	keyboard-and-mouse	-
GetShortPathNameA	file	-
GetFullPathNameA	file	-
MoveFileA	file	-
GetFileAttributesA	file	-
SetFileAttributesA	file	-
CompareFileTime	file	-
GetFileSize	file	-
CopyFileA	file	-
GetTempPathA	file	-
CreateDirectoryA	file	-
RemoveDirectoryA	file	-
CreateFileA	file	-
GetTempFileNameA	file	-
SetFileTime	file	-
FindFirstFileA	file	-
FindNextFileA	file	-
DeleteFileA	file	-
SetFilePointer	file	-
ReadFile	file	-
FindClose	file	-
WriteFile	file	-
SHGetSpecialFolderLocation	file	-
SHGetPathFromIDListA	file	-
SHBrowseForFolderA	file	-
SHGetFileInfoA	file	-
SHFileOperationA	file	-
SetFileSecurityA	file	-
GetCurrentProcess	execution	-
ExitProcess	execution	-
Sleep	execution	T1497
CreateThread	execution	-
CreateProcessA	execution	T1106
GetExitCodeProcess	execution	-
GetCommandLineA	execution	-
PostQuitMessage	execution	-
ShellExecuteA	execution	T1106
GetModuleFileNameA	dynamic-link-library	-
GetProcAddress	dynamic-link-library	-
LoadLibraryExA	dynamic-link-library	T1106
GetModuleHandleA	dynamic-link-library	-
FreeLibrary	dynamic-link-library	-
GetLastError	diagnostic	-
CloseClipboard	data-exchange	-
SetClipboardData	data-exchange	-
EmptyClipboard	data-exchange	-
OpenClipboard	data-exchange	-
ExitWindowsEx	administration	-
lstrcmpiA	-	-
GetVersion	-	-
SetErrorMode	-	-
lstrcpynA	-	-
lstrcatA	-	-
CloseHandle	-	-
lstrcmpA	-	-
lstrlenA	-	-
MulDiv	-	-
MultiByteToWideChar	-	-
SetCursor	-	-
GetWindowRect	-	-
EnableMenuItem	-	-
GetSystemMenu	-	-
SetClassLongA	-	-
GetSysColor	-	-
EndDialog	-	-
ScreenToClient	-	-
CheckDlgButton	-	-
LoadBitmapA	-	-
TrackPopupMenu	-	-
AppendMenuA	-	-
CreatePopupMenu	-	-
SetDlgItemTextA	-	-
GetDlgItemTextA	-	-
MessageBoxIndirectA	-	-
CharPrevA	-	-
GetDC	-	-
InvalidateRect	-	-
BeginPaint	-	-
GetClientRect	-	-
FillRect	-	-
DrawTextA	-	-
SystemParametersInfoA	-	-
GetClassInfoA	-	-
DialogBoxParamA	-	-
CharNextA	-	-
SetTimer	-	-
LoadImageA	-	-
wsprintfA	-	-
GetDlgItem	-	-
EndPaint	-	-
CreateDialogParamA	-	-
SetWindowTextA	-	-
SelectObject	-	-
SetBkMode	-	-
CreateFontIndirectA	-	-
SetTextColor	-	-
DeleteObject	-	-
GetDeviceCaps	-	-
CreateBrushIndirect	-	-
SetBkColor	-	-
ImageList_AddMasked	-	-
ImageList_Destroy	-	-
ImageList_Create	-	-
17 (InitCommonControls)	-	-
OleUninitialize	-	-
OleInitialize	-	-
CoCreateInstance	-	-

Figure9 above shows the various APIs/Functions corresponding to the above-mentioned libraries in Figure8 and provides us important information that the FormBook malware has the following capabilities:

1. Anti-Debugging Capability.
2. Capability to collect system information.
3. Capability to handle windows/GUI functions.
4. Ability to create new threads, processes, and their manipulation.
5. Synchronization capability to handle multiple processes and threads and to access shared resources.
6. Have the capability to access native APIs to perform low-level functions like handling/manipulation of hardware, memory, and processes directly.
7. Ability to access and manipulate registry entries.
8. Capability to load other DLLs, libraries, and processes in memory.
9. Ability to handle, search, open, close, write, access and manipulating files.
10. Capability to search Drives, Folders.

Figure10

Figure10 above shows the XML code present as manifest in the file. It contains meta-data corresponding to different files that are part of the same group or package. The privileges are used as “asInvoker” which means adopting any privilege assigned to the user. This further demonstrates the dependency on NullSoft NSIS and its version number. NSIS is a free framework used to bundle many elements of an application together including DLL or executable, and an NSIS script is also bundled along with the application/file/malware to control how all can be extracted and executed.

Figure 11 below also shows the overlay part present in the file. It also has the Nullsoft signature. FormBook most likely used it to bypass anti-viruses and load or extract the code/files present in the overlay section which are packed by using Nullsoft installer.

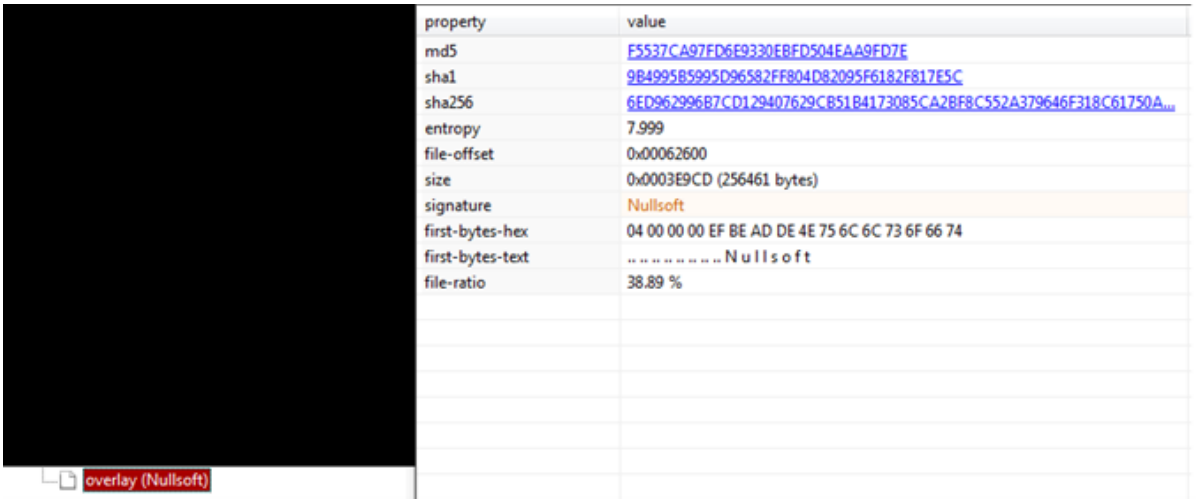

Figure11

We further extracted the hidden files present in our malicious executable as shown in Figure12 which are dropped by the file when it gets executed and used accordingly. There are three more files present in our malicious executable, one is the DLL “jnjvrzet.dll” which is present in the folder named $PLUGINSDIR and the second is the .nsi file which is the NSIS script to control that how to extract and use these files as mentioned above. The third file is “6ce1nlzjaolgh5df” which is in lzma compressed and encrypted also and most probably is an executable or DLL and the main payload.

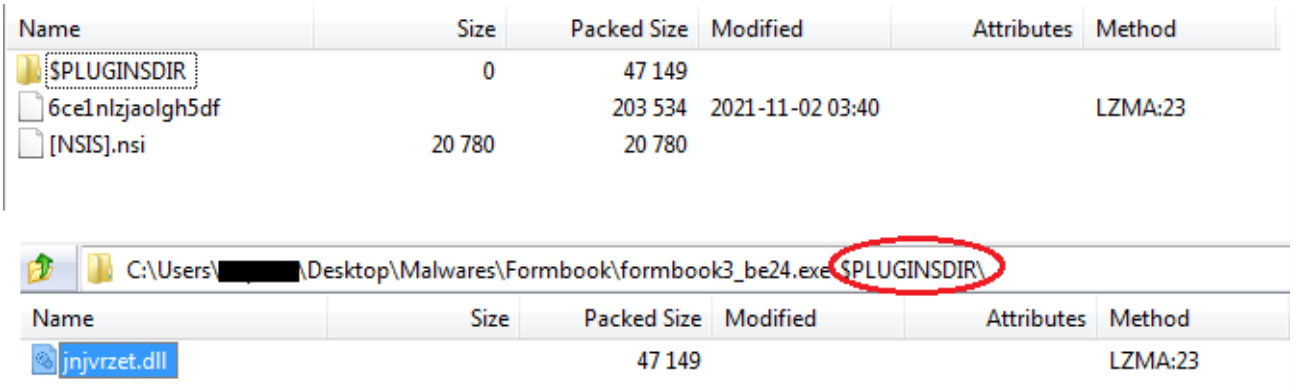

Figure12

Figure13 and Figure14 show hexdump corresponding to the file DLL “jnjvrzet.dll” and “6ce1nlzjaolgh5df”.

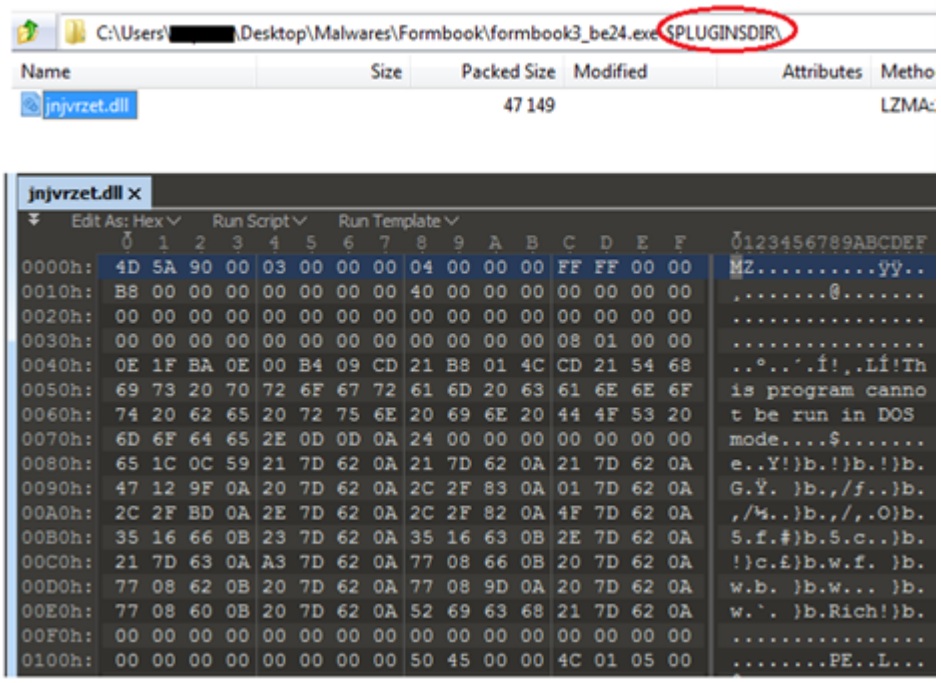

Figure13

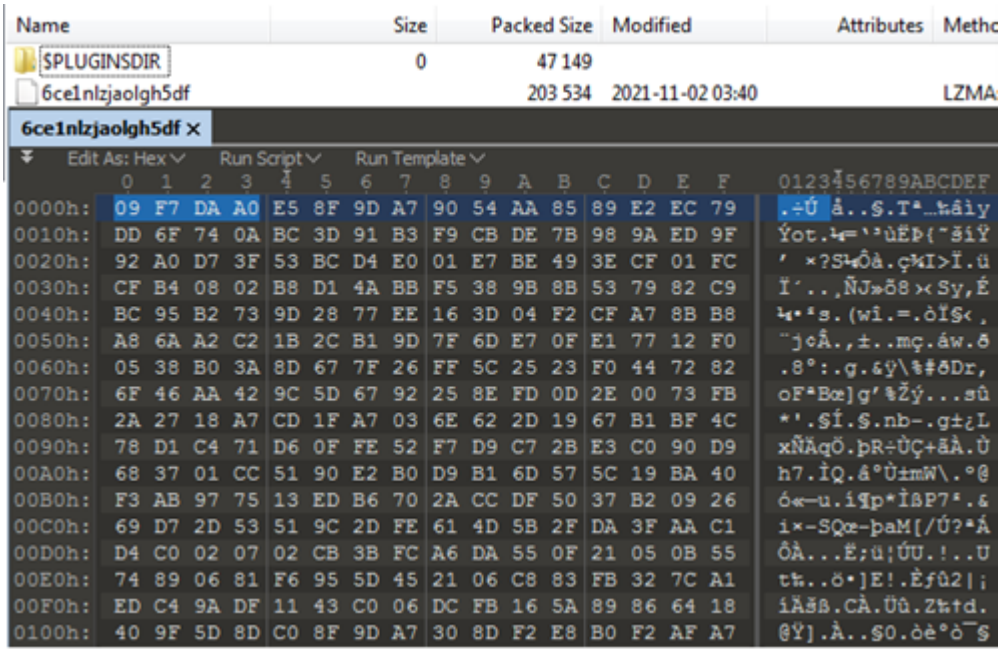

Figure14

```
; NSIS script NSIS-2 BadCmd=11
; Install

SetCompressor lzma
SetCompressorDictSize 8

; ---------------------
; HEADER SIZE: 29658
; START HEADER SIZE: 300
; MAX STRING LENGTH: 1024
; STRING CHARS: 7036

OutFile [NSIS].exe
!include WinMessages.nsh


; ---------------------
; LANG TABLES: 1
; LANG STRINGS: 49

Name cskebu
BrandingText "Nullsoft Install System v2.51"

; LANG: 1033
LangString LSTR_0 1033 "Nullsoft Install System v2.51"


  InstType $(LSTR_39)    ;  Custom
  InstallDir $TEMP
  ; wininit = $WINDIR\wininit.ini


  Function func_0
    DetailPrint hyczqjspgrdno
    FileReadByte $5 $R6
    FileWriteByte $1 2785
    CopyFiles $INSTDIR\hoodwinked\grandeur.xls $INSTDIR\overtired.gif    ; $(LSTR_7)$INSTDIR\overtired.gif    ;  "Copy to "
    DeleteRegKey HKLM SOFTWARE\copacetic
    MessageBox MB_OKCANCEL zkbsrlsxpgkj
    CreateDirectory $INSTDIR\compiling
    MessageBox MB_ABORTRETRYIGNORE infprnnpqiyls
    StrCpy $5 ucboxqtxxj
    Push $INSTDIR\veronica\pygmy\audit.cvs
    Nop
    Delete $INSTDIR\evade\obeying\peacetime.mp4
    Rename $INSTDIR\undoubtedly\orientation\hateful.aiff $INSTDIR\toby\boarder\team.eps ;  $INSTDIR\undoubtedly\orientation\hateful.aiff->$INSTDIR\toby\boarder\team.eps
    Push $INSTDIR\bait\scanning
    RegDLL $INSTDIR\shelves.dll
    RegDLL $INSTDIR\veronica\concluded\cowed.dll
    Push kzmtpiycrpj
    DetailPrint uttoxyxbtcmnq
    MessageBox MB_ABORTRETRYIGNORE axlvskvgzp
    ExecWait $INSTDIR\bitsy.bat
    ClearErrors
    StrCpy $3 rwczspflibqoqda
  FunctionEnd
```

Figure15

```
Function func_64
  Call func_0
  StrCpy $R8 rbzutkopbmo
  Pop $R0
  ReadEnvStr $R0 APPDATA
  StrCpy $3 uxftxlfgtgryzt
  Call func_0
  StrCpy $6 cfzyyfxayfq
  FindNext $R6 $R8
  StrCpy $2 lxfxmrmqqpv
  Push $INSTDIR\rendered.hqx
  Exch $R4
    ; Push $R4
    ; Exch
    ; Pop $R4
  DetailPrint cewxkgkkyms
  Push $INSTDIR\deliberate\incensed\acted
  CreateDirectory $INSTDIR\fellahs
FunctionEnd


Function func_81
  GetFullPathName $R5 $INSTDIR\slut\commendable\sick.hqx
  Exch $9
    ; Push $9
    ; Exch
    ; Pop $9
  Exch $R9
    ; Push $R9
    ; Exch
    ; Pop $R9
  DetailPrint kmrwjmobcozxg
  Call func_23
  SetErrorLevel 0
  Push 44510
  DetailPrint eqeuaeallvy
  StrCpy $R0 rubkemrjmjbbiw
    ; ShowWindow $HWNDPARENT ${SW_SHOW}
  BringToFront
  Delete $INSTDIR\belonging.ra
  GetCurrentAddress $R7 ; StrCpy $R7 98
  MessageBox MB_YESNO ehwndbzvpqfzc
  Nop
FunctionEnd


Function func_101
  ReadRegDWORD $R9 HKLM SOFTWARE\manic\offbeat hpgunjlhktekb
  DetailPrint xsvlmhyljar
```

Figure16

Figure15 and Figure16 show the snippets of .nsi script corresponding to Nullsoft Installer to control the process of extracting these embedded files and how to use them for further exploitation. It accesses various folders, creating

files, copying, and doing initialization, etc.

We further checked the extracted .DLL file “jnjvrzet.dll” as shown below in Figure17. It is Windows 32-bit DLL. We checked it through different anti-virus engines and found it to be malicious and they categorized it as mainly trojan as shown in Figure 18.

property	value
md5	A500638A0197E27649CD3EF3D574F6E7
sha1	4244D9126D8AD7D545B98FF0173372EFE50FA5A4
sha256	5F02D1A61E6C20966CCF55AB8E028EC839283E114E94556FD5AC8689D1B64754
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z . . . . . @ . . . . .
file-size	102912 (bytes)
size-without-overlay	n/a
entropy	6.480
imphash	n/a
signature	n/a
entry-point	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
file-version	n/a
description	n/a
file-type	**dynamic-link-library**
cpu	**32-bit**
subsystem	Native
compiler-stamp	0x618065D4 (Tue Nov 02 03:40:28 2021)
debugger-stamp	0x618065D4 (Tue Nov 02 03:40:28 2021)

Figure17

Elastic	malicious (high confidence)
MicroWorld-eScan	Trojan.GenericKDZ.79521
FireEye	Generic.mg.a500638a0197e276
Sangfor	Trojan.Win32.Injector.EQKW
Alibaba	Trojan:Win32/Lokibot.ad3c4a5e
CrowdStrike	win/malicious_confidence_60% (W)
Cyren	W32/Injector.AMK.gen!Eldorado
APEX	Malicious
BitDefender	Trojan.GenericKDZ.79521
Avast	Win32:PWSX-gen [Trj]
Ad-Aware	Trojan.GenericKDZ.79521
McAfee-GW-Edition	Artemis!Trojan
Microsoft	Trojan:Win32/Lokibot.SISN!MTB
GData	Trojan.GenericKDZ.79521
Cynet	Malicious (score: 100)
McAfee	Artemis!A500638A0197
MAX	malware (ai score=84)
Malwarebytes	Trojan.Injector
Fortinet	W32/Injector.EOLV!tr
AVG	Win32:PWSX-gen [Trj]
Panda	Trj/GdSda.A

Figure18

library (7)	blacklist (4)	type (1)	imports (109)	description
ws2_32.dll	x	implicit	6	Windows Socket 2.0 32-Bit DLL
wsnmp32.dll	x	implicit	5	Microsoft WinSNMP v2.0 Manager API
setupapi.dll	x	implicit	4	Windows Setup API
wsock32.dll	x	implicit	4	Windows Socket 32-Bit DLL
kernel32.dll	-	implicit	55	Windows NT BASE API Client DLL
ole32.dll	-	implicit	8	Microsoft OLE for Windows
oleaut32.dll	-	implicit	27	© Microsoft Corporation. All rights reserved.

Figure19

The imported libraries corresponding to the extracted DLL are shown in Figure19 above. The presence of ws2_32.dll and wsnmp32.dll indicates that our extracted DLL is responsible for handling and managing network connections. Setupapi.dll is also quite important as it is used for setting up and installing the applications means the extracted DLL also helps in installing or setting up other malicious files for execution and most probably the main payload.

name (109)	group (10)	MITRE-Technique (3)
IsProcessorFeaturePresent	system-information	-
IsDebuggerPresent	system-information	T1082
DeleteCriticalSection	synchronization	-
InitializeCriticalSectionAndSpi...	synchronization	-
LeaveCriticalSection	synchronization	-
EnterCriticalSection	synchronization	-
GetVolumeNameForVolumeM...	storage	-
SetupDiGetClassDevsW	setup	-
SetupDiGetDriverInfoDetailA	setup	-
SetupDiClassGuidsFromNameW	setup	-
SetupInitializeFileLogW	setup	-
57 (gethostvalue)	network	-
10 (ioctlsocket)	network	-
17 (recvfrom)	network	-
5 (getpeervalue)	network	-
113 (WSACancelBlockingCall)	network	-
6 (getsockvalue)	network	-
1116	network	-
1119	network	-
1120	network	-
1109	network	-
HeapAlloc	memory	-
GetProcessHeap	memory	-
VirtualProtect	memory	-
GetStringTypeW	memory	-
HeapFree	memory	-
SetFilePointerEx	file	-
FlushFileBuffers	file	-
WriteFile	file	-
CreateFileW	file	-
GetFileType	file	-
GetCurrentThreadId	execution	-
TlsSetValue	execution	-
TlsGetValue	execution	-
TerminateProcess	execution	-
GetCurrentProcess	execution	-
Sleep	execution	T1497
ExitProcess	execution	-
SetUnhandledExceptionFilter	exception-handling	-
UnhandledExceptionFilter	exception-handling	-
LoadLibraryExW	dynamic-link-library	T1106
GetProcAddress	dynamic-link-library	-
GetModuleFileNameW	dynamic-link-library	-
GetModuleHandleExW	dynamic-link-library	-
SetLastError	diagnostic	-
OutputDebugStringW	diagnostic	-
GetLastError	diagnostic	-
SetConsoleActiveScreenBuffer	console	-
SetStdHandle	console	-
GetConsoleMode	console	-
GetConsoleCP	console	-
GetStdHandle	console	-
WriteConsoleW	console	-

SetDefaultCommConfigA	-	-
SetCommBreak	-	-
_lopen	-	-
GetDateFormatA	-	-
lstrlenW	-	-
CloseHandle	-	-
RtlUnwind	-	-
LCMapStringW	-	-
GetCPInfo	-	-
GetOEMCP	-	-
GetACP	-	-
IsValidCodePage	-	-
WideCharToMultiByte	-	-
MultiByteToWideChar	-	-
DecodePointer	-	-
EncodePointer	-	-
105 (SnmpSetTimeout)	-	-
603 (SnmpCountVbl)	-	-
401 (SnmpContextToStr)	-	-
320 (SnmpSetPort)	-	-
102 (SnmpGetRetransmitMode)	-	-
OleSetAutoConvert	-	-
HMENU_UserFree	-	-
HkOleRegisterObject	-	-
OleBuildVersion	-	-
OleLoadFromStream	-	-
OleSetMenuDescriptor	-	-
WriteFmtUserTypeStg	-	-
HWND_UserFree	-	-
176	-	-
173	-	-
167 (VarXor)	-	-
159	-	-
158	-	-
157	-	-
156	-	-
155	-	-
154	-	-
153 (VarIdiv)	-	-
152	-	-
143 (VarDiv)	-	-
318 (VarCat)	-	-
142	-	-
141	-	-
11 (VariantCopyInd)	-	-
10 (VariantCopy)	-	-
9 (VariantClear)	-	-

Figure20

Figure20 above shows the imported APIs/Functions by our extracted DLL. The DLL also has the following capabilities in-addition to the capabilities we mention for our malicious executable:

1. Capability to deactivate/sleep to hide its functionality or capability to wait for any trigger to continue
2. Capability to manage network connections
3. File handling, searching and manipulation capability
4. Capability to handle Critical Sections/locks to handle shared resources
5. Capability to access Thread local storage area and handling of multiple threads
6. Several anonymous functions and their validity or usage are not yet confirmed
7. Ant-debugging capability

Time ...	Process Name	PID	Operation	Path
12:33:...	formbook3_be2...	816	Process Start	
12:33:...	formbook3_be2...	816	Thread Create	
12:33:...	formbook3_be2...	816	Load Image	C:\Users\dilpreet\Desktop\Malwares\FormBookMalware\formbook3_be24.exe
12:33:...	formbook3_be2...	816	Load Image	C:\Windows\System32\ntdll.dll
12:33:...	formbook3_be2...	816	Load Image	C:\Windows\SysWOW64\ntdll.dll
12:33:...	formbook3_be2...	816	CreateFile	C:\Windows\Prefetch\FORMBOOK3_BE24.EXE-37FD187E.pf
12:33:...	formbook3_be2...	816	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
12:33:...	formbook3_be2...	816	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DisableUserModeCallbackFi
12:33:...	formbook3_be2...	816	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
12:33:...	formbook3_be2...	816	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
12:33:...	formbook3_be2...	816	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANAGER\CWDIllegalInDLLSearch
12:33:...	formbook3_be2...	816	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER
12:33:...	formbook3_be2...	816	CreateFile	C:\Windows
12:33:...	formbook3_be2...	816	CreateFile	C:\Windows\System32\wow64.dll
12:33:...	formbook3_be2...	816	QueryBasicInfor...	C:\Windows\System32\wow64.dll
12:33:...	formbook3_be2...	816	CloseFile	C:\Windows\System32\wow64.dll
12:33:...	formbook3_be2...	816	CreateFile	C:\Windows\System32\wow64.dll
12:33:...	formbook3_be2...	816	CreateFileMapp...	C:\Windows\System32\wow64.dll
12:33:...	formbook3_be2...	816	CreateFileMapp...	C:\Windows\System32\wow64.dll
12:33:...	formbook3_be2...	816	Load Image	C:\Windows\System32\wow64.dll
12:33:...	formbook3_be2...	816	CloseFile	C:\Windows\System32\wow64.dll
12:33:...	formbook3_be2...	816	CreateFile	C:\Windows\System32\wow64win.dll
12:33:...	formbook3_be2...	816	Load Image	C:\Windows\SysWOW64\user32.dll
12:33:...	formbook3_be2...	816	Load Image	C:\Windows\SysWOW64\gdi32.dll
12:33:...	formbook3_be2...	816	Load Image	C:\Windows\SysWOW64\lpk.dll
12:33:...	formbook3_be2...	816	Load Image	C:\Windows\SysWOW64\usp10.dll
12:33:...	formbook3_be2...	816	Load Image	C:\Windows\SysWOW64\msvcrt.dll
12:33:...	formbook3_be2...	816	Load Image	C:\Windows\SysWOW64\advapi32.dll
12:33:...	formbook3_be2...	816	CreateFile	C:\Windows\SysWOW64\sechost.dll
12:33:...	formbook3_be2...	816	QueryBasicInfor...	C:\Windows\SysWOW64\sechost.dll
12:33:...	formbook3_be2...	816	CloseFile	C:\Windows\SysWOW64\sechost.dll
12:33:...	formbook3_be2...	816	CreateFile	C:\Windows\SysWOW64\sechost.dll
12:33:...	formbook3_be2...	816	CreateFileMapp...	C:\Windows\SysWOW64\sechost.dll
12:33:...	formbook3_be2...	816	CreateFileMapp...	C:\Windows\SysWOW64\sechost.dll
12:33:...	formbook3_be2...	816	Load Image	C:\Windows\SysWOW64\sechost.dll
12:33:...	formbook3_be2...	816	CloseFile	C:\Windows\SysWOW64\sechost.dll
12:33:...	formbook3_be2...	816	Load Image	C:\Windows\SysWOW64\rpcrt4.dll
12:33:...	formbook3_be2...	816	Load Image	C:\Windows\SysWOW64\sspicli.dll
12:33:...	formbook3_be2...	816	Load Image	C:\Windows\SysWOW64\cryptbase.dll
12:33:...	formbook3_be2...	816	Load Image	C:\Windows\SysWOW64\shell32.dll
12:33:...	formbook3_be2...	816	Load Image	C:\Windows\SysWOW64\shlwapi.dll
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryValue	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryValue	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryValue	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryValue	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryValue	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryValue	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryValue	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryValue	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
2:33:...	formbook3_be2...	816	RegQueryValue	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
2:33:...	formbook3_be2...	816	RegQueryKey	HKCR\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder

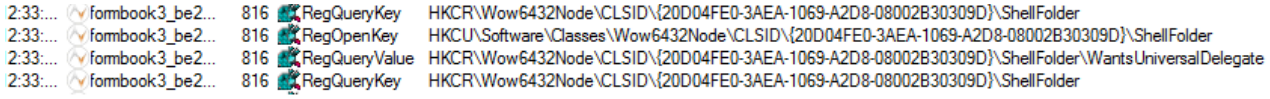

Figure21

Figure21 mentioned above shows the processes spawned by the malicious executable when it runs. It starts and creates various processes and threads, loads various system libraries, and accesses many registry entries.

List of IOCs

Sr No.	Indicator	Type	Remarks
1	c504f8e950801fd90e45b01023c29702	File Hash	MD5
2	be24cc41a8c8b2c292743055cccd8a9ca25eddcaa26aa984a63a6dff70ddae55	File Hash	SHA256
3	c439604f01c988cc0d33f3b69f624921ffe847e821e392afbc3126ea44225bcc9907b01dcd36ab225fab505e5f81999518f91253d4447a221bb144e79927ff06	File Hash	SHA512
4	a500638a0197e27649cd3ef3d574f6e7	DLL Hash	MD5
5	5f02d1a61e6c20966ccf55ab8e028ec839283e114e94556fd5ac8689d1b64754	DLL Hash	SHA256
6	46ecee6911deff33081034dc3aea0ed652c8b5bdafaa4658d1d79fc62c277143c2fe792cf4e96537f7b7cff76a07b1515e0417a57293e392fc6c416bd7f8d8f2	DLL Hash	SHA512
7	ad764a0e99f9b236779a9656ecce9779	Encrypted File Hash	MD5
8	ec0d3cc02378ff9ac99adcfa457e7fb92e9c70185da93e5fb310977b5ac7462a	Encrypted File Hash	SHA256
9	e993c06999395ee9e757d0a4d4f55ff4d1fee25c594c3527236b0e3226963f9874381b5ac5c47708f7813db735f5e5d51e1b9d49b69cd8137cce4836b3a7b4d7	Encrypted File Hash	SHA512
10	e730637b16ffd64e5daab0751c074b8f	NSI Script Hash	MD5
11	8bbdb9ec034c1b308b9e93078ae14979d2aa9b29d5f075b7d3041cd19dbbf201	NSI Script Hash	SHA256
12	c2d02a89e6f96b6d1d757a7f35a938390a3059b15b6587ff19f823d13f8f5a7f8bdca4c2b99d5a9140e3681df4350ea5ae1d70f82fdfea37ffcfe658cdda938e	NSI Script Hash	SHA512

Mitre Attack Tactics and Techniques

Sr No.	Tactic	Technique
1	Initial Access (TA0001)	Email Campaigns
		Spear Phishing
2	Execution (TA0002)	Malicious File
		User Execution
3	Persistence (TA0003)	Registry Keys
4	Defense Evasion (TA0005)	Disabling Security Tools
		Process Hollowing
		Obfuscation
		Anti-Debugging/Sandbox Evasion
	Credential Access (TA0031)	Credentials from Web Browsers
5	Discovery (TA0007)	Query Registry
		System Information Discovery
6	Collection (TA0035)	Input Capture
		Screen Capture
7	Command and Control (TA0011)	Application Layer Protocol
8	Exfiltration (TA0036)	Over C2 Channel

Source: https://www.cyfirma.com/outofband/formbook-malware-technical-analysis/