

MALWARE ANALYSIS PROJECT

AIM: Analyse the given malware and prepare a report on the same.

MALWARE SAMPLE: DopeBotv0.22_UnCrippled_Feb2007

Tools & Websites Used:

- Virus Total (website)
- PeStudio tool
- CFF Explorer tool
- Dependency Walker tool
- IDA Pro tool
- Process Explorer tool
- Process Monitor tool
- RegShot tool
- Hybrid Analysis (website)

Static Analysis:

Virus Total (website):

54 / 70

54 security vendors and no sandboxes flagged this file as malicious

2014ced97466e3f290d4dd785be7df12f37f4795cf32543145229b15a8d20857
2014ced97466e3f290d4dd785be7df12f37f4795cf32543145229b15a8d20857.dll
pedll

3.00 KB
Size

2022-07-27 01:04:27 UTC
2 months ago

DETECTION DETAILS RELATIONS COMMUNITY 2

Security Vendors' Analysis

Ad-Aware	Backdoor.Irc.Sdbot.BF	AhnLab-V3	Worm/Win.IRCBot.R447587
Alibaba	Trojan.Win32/ATRAPS.e05f57bb	ALYac	Backdoor.Irc.Sdbot.BF
Antiy-AVL	Trojan/Generic.ASMalwS.330C	Arcabit	Backdoor.Irc.Sdbot.BF
Avast	Win32.Malware-gen	AVG	Win32.Malware-gen
Avira (no cloud)	TR/ATRAPS.Gen2	BitDefender	Backdoor.Irc.Sdbot.BF
BitDefenderTheta	Gen.NN.ZedlaF.34806.ai4@a0DZuTj	ClamAV	Win.Trojan.Sdbot-329
Comodo	Backdoor@#1qcjkpahyrc7	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 99)
Cyren	W32/Sdbot.NLAQ-3555	DrWeb	BackDoor.IRC.Sdbot.1026
Elastic	Malicious (high Confidence)	Emsisoft	Backdoor.Irc.Sdbot.BF (B)
Elastic	Malicious (high Confidence)	Emsisoft	Backdoor.Irc.Sdbot.BF (B)
eScan	Backdoor.Irc.Sdbot.BF	ESET-NOD32	A Variant Of Generik.KUMEOKL
F-Secure	Trojan.TR/ATRAPS.Gen2	Fortinet	W32/Sdbotworm
GData	Backdoor.Irc.Sdbot.BF	Ikarus	Trojan.Agent
Jiangmin	Trojan/Genome.qdn	K7AntiVirus	Trojan (0001140e1)
K7GW	Trojan (0001140e1)	Kaspersky	HEUR:Trojan.Win32.Generic
Lionic	Trojan.Win32.Generic.4lc	MAX	Malware (ai Score=100)
MaxSecure	Trojan.Malware.1891678.susgen	McAfee	GenericRXAA-AAI6A6C1DAD9B52
McAfee-GW-Edition	Artemis!Virus	Microsoft	Backdoor.Win32/Ursaplrts
NANO-Antivirus	Trojan.Win32.Sdbot.qsiyc	Palo Alto Networks	Generic.ml
Panda	Generic.Malware	Rising	Trojan.Ymacco!8.11BE1 (CLOUD)
Sangfor Engine Zero	Backdoor.Win32.Ursap.rts	SecureAge	Malicious
Sophos	ML/PE-A	Symantec	ML.Attribute.HighConfidence
TACHYON	Backdoor/W32.SdBot.3072	Tencent	Malware.Win32.Gencirc.11d493be
Trellix (FireEye)	Generic.mg.6a6c1dad9b52057f	VBA32	Backdoor.IRC.Sdbot
VIPRE	Backdoor.Irc.Sdbot.BF	VinIT	Backdoor.Win32.Sdbot.BNM

- Firstly, we are trying to fetch general information of the malware in the virus total. Here in the detection section most off the vendors have flagged this malware as backdoor.

Names ⓘ

2014ced97466e3f290d4dd785be7df12f37f4795cf32543145229b15a8d20857.dll
 6a6c1dad9b52057f815b9d4ca5e962cb_hook.dll
 6a6c1dad9b52057f815b9d4ca5e962cb.dll
 hook.dll
 6a6c1dad9b52057f815b9d4ca5e962cb.vir
 6A6C1DAD9B52057F815B9D4CA5E962CB
 aa
 vviVObsIM.dwg
 pJh4hMJkFP.docx

Imports

- + SHLWAPI.dll
- + KERNEL32.dll
- + MSVCRT.dll

PE Resource Parents (10) ⓘ

Scanned	Detections	Type	Name
2017-12-21	47 / 68	Win32 EXE	dopebot_debug.exe
2020-12-18	55 / 70	Win32 EXE	d10c1c49b63af1377f871c23c4faa5b3.virus
2013-04-23	35 / 46	Win32 EXE	VirusShare_84725461b4cbef09817a032d880be0c1
2021-01-04	51 / 70	Win32 EXE	VirusShare_02c487918b125f6ea612cca4196a86a4
2017-10-26	43 / 67	Win32 EXE	dopebot_debug.exe
2017-12-21	49 / 68	Win32 EXE	dopebot_debug.exe
2020-02-19	59 / 73	Win32 EXE	test.txt
2017-10-26	42 / 66	Win32 EXE	dopebot_debug.exe
2021-02-05	44 / 71	Win32 EXE	aa
2014-02-04	34 / 48	Win32 EXE	0e335fe3436b05d91194fdae44def1113edc301-fdc96b777df8ec1e2eba9fdb6eada68d.01.exe1428.vir

- Additional information we've retrieved is the different names of the malware, importing dll files such as shlwapi.dll, kernale43.dll, msvcrt.dll etc.
- We also get it's relation with different malwares.

PeStudio tool:

pestudio 9.39 - Malware Initial Assessment - www.winitor.com [c:\users\dhairya changela\desktop\dopebot v0.22 uncriddled- feb 2007\resources\files\hook.dll]

file settings about

property	value
md5	6A6C1DAD9B52057F815B9D4CA5E962CB
sha1	C3BA84E7AC1641768219290825779E8A2009BB63
sha256	2014CED97466E3F290D4DD785BE7DF12F37F4795CF32543145229B15A8D20857
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 40 00 00 00 00 00 00 00 00
first-bytes-text	M Z
file-size	3072 bytes
entropy	4.105
imphash	0B69D5093BECB476150C8C4A428DC314
signature	n/a
tooling	Visual Studio 6.0
entry-point	8B 44 24 08 48 74 04 B0 01 EB 51 56 68 5D 11 14 13 BE 98 10 14 13 68 88 10 14 13 56 E8 04 FD FF FF
file-version	n/a
description	n/a
file-type	dynamic-link-library
cpu	32-bit
subsystem	GUI
compiler-stamp	Thu Feb 08 19:29:42 2007 UTC
debugger-stamp	n/a
resources-stamp	n/a
import-stamp	Thu Jan 01 00:00:00 1970 UTC
exports-stamp	n/a

- After loading the file in Pestudio tool, we are getting general information such as md5, sha1, sha256 values, file type, subsystem etc. Also, first-byte-text is "M Z" hence we get to know that it is an executable file.

pestudio 9.39 - Malware Initial Assessment - www.winitor.com [c:\users\dhairya changela\desktop\dopebot v0.22 uncriddled- feb 2007\resources\files\hook.dll]

file settings about

indicator (27)	detail	level
functions > flag	count: 5	1
strings > flag	count: 9	1
entry-point > non-executable section	location: yes	1
section > first > writable	section: .data	1
sections > executable > count	value: 0	1
size-of-code > suspicious	value: 0x00000000	1
strings > threshold	count: 46	2
file > os > target	name: Windows NT 4.0	3
function > group	name: dynamic-library	3
function > group	name: file	3
function > group	name: memory	3
file > entry-point > location	section: .data:0x0000138B	3
functions > count	value: 12	3
libraries > count	value: 3	3
strings > ascii	count: 46	4
file > subsystem > type	name: GUI	4
file > tooling	name: Visual Studio 6.0	4
security > protection	name: address-space-layout-randomization (ASLR) > OFF	4
security > protection	name: code-integrity (CI) > OFF	4
security > protection	name: control-flow-guard (CFG) > OFF	4
security > protection	name: data-execution-prevention (DEP) > OFF	4
file > type	name: dynamic-link-library	4
security > protection	name: stack-buffer-overflow-detection (GS) > OFF	4
rich-header > checksum	status: valid	4
rich-header > offset	value: 0x00000080	4
dos-stub > size	value: 152 bytes	4
sections > file-ratio	value: 66.67%	4

- We are getting 27 indicators as above.

MALWARE ANALYSIS

pestudio 9.39 - Malware Initial Assessment - www.winitor.com [c:\users\dhairya changela\desktop\dopebot v0.22 uncrrippled- feb 2007\resources\files\hook.dll]

name (15)	size (bytes)	location (address)	location (section)	time-stamp	invalid (0/15)	missing (0/15)	null (12/15)
export-table	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
import-name	0x00000050 (80)	0x000013FC	.data	0x00000000 (Thu Jan 01 00:00:00 1970 UTC)	-	-	-
resource	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
exception	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
security	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
relocation	0x00000050 (80)	0x00002000	.reloc	0x00000000 (Thu Jan 01 00:00:00 1970 UTC)	-	-	-
debug	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
architecture	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
global-pointer	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
thread-storage	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
load-configuration	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
bound-import	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
import-address	0x0000003C (60)	0x00001000	.data	0x00000000 (Thu Jan 01 00:00:00 1970 UTC)	-	-	-
delay-loaded	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x
.NET	0x00000000 (0)	0x00000000	n/a	n/a	-	-	x

- We get 3 directories named import-name, relocation, import-address.

pestudio 9.39 - Malware Initial Assessment - www.winitor.com [c:\users\dhairya changela\desktop\dopebot v0.22 uncrrippled- feb 2007\resources\files\hook.dll]

library (3)	flag (0)	type (1)	functions (12)	description
kernel32.dll	-	implicit	9	Windows NT BASE API Client DLL
msvcrt.dll	-	implicit	2	Windows NT CRT DLL
shlwapi.dll	-	implicit	1	Shell Light-weight Utility Library

pestudio 9.39 - Malware Initial Assessment - www.winitor.com [c:\users\dhairya changela\desktop\dopebot v0.22 uncrrippled- feb 2007\resources\files\hook.dll]

functions (12)	flag (5)	ordinal (0)	library (3)
VirtualProtect	x	-	kernel32.dll
FindFirstFileA	x	-	kernel32.dll
FindNextFileA	x	-	kernel32.dll
FindFirstFileW	x	-	kernel32.dll
FindNextFileW	x	-	kernel32.dll
GetProcAddress		-	kernel32.dll
GetModuleHandleA		-	kernel32.dll
lstrcmpiA		-	kernel32.dll
WideCharToMultiByte		-	kernel32.dll
_stricmp		-	msvcrt.dll
sprintf		-	msvcrt.dll
PathStripPathA		-	shlwapi.dll

- It includes 3 libraries named kernel32.dll, msvcrt.dll, shlwapi.dll.
- Found various functions such as “VirtualProtect”, “FindFirstFileA”, “GetProcAddress”, “GetModuleHandleA” etc.

MALWARE ANALYSIS

pestudio 9.39 - Malware Initial Assessment - www.winator.com [c:\users\dhairya changela\desktop\dopebot v0.22 uncrippled- feb 2007\resources\files\hook.dll]

file settings about

c:\users\dhairya changela\desktop\dopebot v0.2

encoding (1)	size (bytes)	location	flag (9)	hint (21)	value (46)
ascii	12	0x00000448	x	function	FindNextFile
ascii	13	0x00000458	x	function	FindFirstFile
ascii	12	0x00000478	x	function	FindNextFile
ascii	13	0x00000488	x	function	FindFirstFile
ascii	14	0x0000088A	x	function	VirtualProtect
ascii	13	0x000008CE	x	function	FindFirstFile
ascii	12	0x000008E0	x	function	FindNextFile
ascii	13	0x00000906	x	function	FindFirstFile
ascii	12	0x00000918	x	function	FindNextFile
ascii	12	0x00000468	-	library	kernel32.dll
ascii	12	0x00000498	-	library	KERNEL32.DLL
ascii	12	0x00000926	-	library	KERNEL32.dll
ascii	10	0x0000093E	-	library	MSVCRT.dll
ascii	11	0x0000095C	-	library	SHLWAPI.dll
ascii	14	0x0000089C	-	function	GetProcAddress
ascii	15	0x000008AE	-	function	GetModuleHandle
ascii	8	0x000008C2	-	function	lstrcpm
ascii	19	0x000008F0	-	function	WideCharToMultiByte
ascii	13	0x0000094C	-	function	PathStripPath

- We are getting various flagged strings as above.

CFF Explorer tool:

CFF Explorer VIII - [hook.dll]

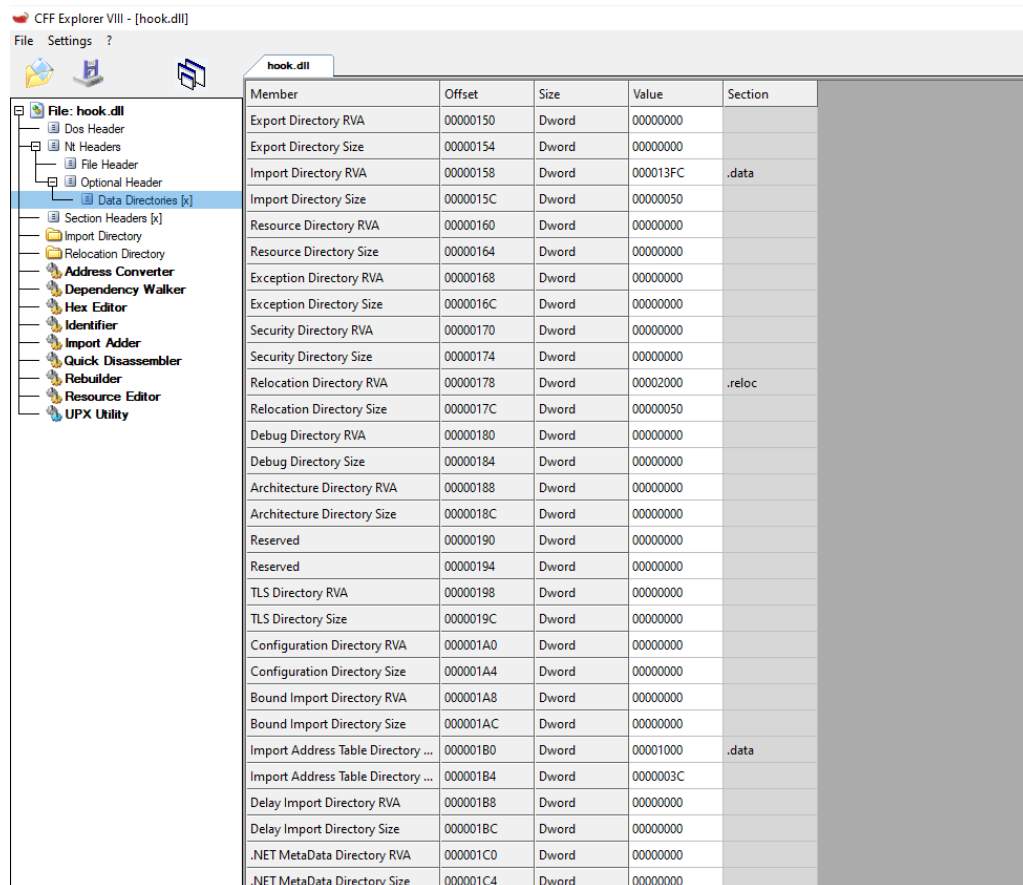
File Settings ?

hook.dll

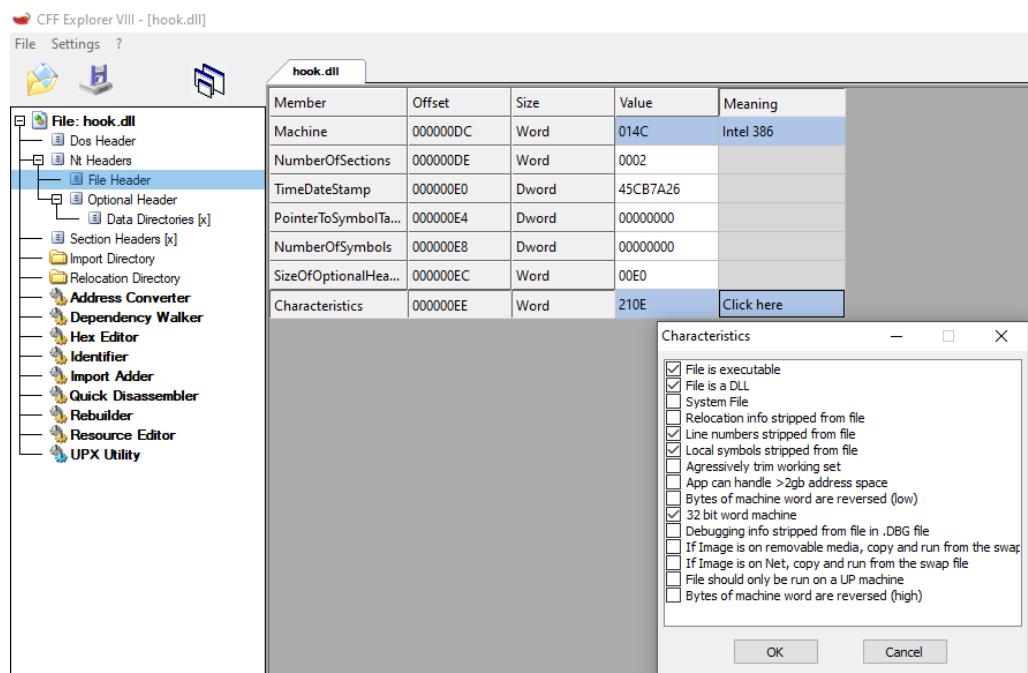
Property	Value
File Name	C:\Users\Dhairya Changela\Desktop\DopeBot v0.22 UnCrippled- Feb ...
File Type	Portable Executable 32
File Info	No match found.
File Size	3.00 KB (3072 bytes)
PE Size	3.00 KB (3072 bytes)
Created	Friday 10 January 2014, 18.05.24
Modified	Saturday 13 August 2022, 23.05.24
Accessed	Sunday 16 October 2022, 13.05.11
MD5	96A264E198AFC56E22EA8CB82833388A
SHA-1	3249C54C6963D3A7DA5EA91882666A62AE51D5F4

Property	Value
Empty	No additional info available

MALWARE ANALYSIS



- Here we are not getting any additional information.
- But we have additional functionalities like we can check characteristics of the malware as below.



MALWARE ANALYSIS

Dependency Walker tool:

Dependency Walker - [hook.dll]

File Edit View Options Profile Window Help

HOOK.DLL

- KERNEL32.DLL
 - API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
 - API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL
 - NTDLL.DLL
 - KERNELBASE.DLL

Errors were detected when processing "c:\users\dhairya changela\desktop\dopebot v0.22 uncriddled- feb 2007\resources\files\HOOK.DLL". See the log window for details.

Module File Time S...

- API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL Error opening file. The system cannot find the file specified (2).
- API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL Error opening file. The system cannot find the file specified (2).
- API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL Error opening file. The system cannot find the file specified (2).
- API-MS-WIN-CORE-ATOMS-L1-1-0.DLL Error opening file. The system cannot find the file specified (2).
- API-MS-WIN-CORE-COMM-L1-1-0.DLL Error opening file. The system cannot find the file specified (2).
- API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL Error opening file. The system cannot find the file specified (2).

Error: At least one required implicit or forwarded dependency was not found.

Error: Modules with different CPU types were found.

Error: A circular dependency was detected.

Warning: At least one delay-load dependency module was not found.

Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

CFF Explorer VIII - [hook.dll]

File Settings ?

hook.dll

File: hook.dll

- Dos Header
- File Headers
- Optional Header
- Section Headers [x]
- Import Directory
- Relocation Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

api-ms-win-core-rtlsupport-l1-1-0.dll

api-ms-win-core-rtlsupport-l1-2-0.dll

ntdll.dll

KERNELBASE.dll

api-ms-win-eventing-provider-l1-1-0.dll

api-ms-win-core-processthreads-l1-1-0.dll

api-ms-win-core-processthreads-l1-1-3.dll

api-ms-win-core-processthreads-l1-1-2.dll

api-ms-win-core-processthreads-l1-1-1.dll

api-ms-win-core-registry-l1-1-0.dll

api-ms-win-core-heap-l1-1-0.dll

api-ms-win-core-heap-l2-1-0.dll

api-ms-win-core-memory-l1-1-1.dll

api-ms-win-core-memory-l1-1-2.dll

api-ms-win-core-handle-l1-1-0.dll

api-ms-win-core-synch-l1-1-0.dll

api-ms-win-core-synch-l1-2-1.dll

api-ms-win-core-synch-l1-2-0.dll

api-ms-win-core-file-l1-1-0.dll

api-ms-win-core-file-l1-2-0.dll

api-ms-win-core-file-l1-2-1.dll

api-ms-win-core-delayload-l1-1-0.dll

api-ms-win-core-io-l1-1-0.dll

api-ms-win-core-io-l1-1-1.dll

api-ms-win-core-job-l1-1-0.dll

api-ms-win-core-threadpool-legacy-l1-1-0.dll

api-ms-win-core-threadpool-private-l1-1-0.dll

api-ms-win-core-libraryloader-l1-2-2.dll

Property	Value
File Name	C:\Windows\SysWOW64\KERNEL32.dll
File Type	Portable Executable 32
File Info	No match found.
File Size	622.77 KB (637712 bytes)
PE Size	608.00 KB (622592 bytes)
Created	Thursday 18 August 2022, 09.52.17
Modified	Thursday 18 August 2022, 09.52.17
Accessed	Thursday 20 October 2022, 08.14.49
MD5	C9FDF863B56CCA2A80726CEEC54F7D7F
SHA-1	1C336BD54F1CD755898EB9C3FF20A7F97F84DF78

Property	Value
CompanyName	Microsoft Corporation
FileDescription	Windows NT BASE API Client DLL
FileVersion	10.0.19041.1889 (WinBuild.160101.0800)
InternalName	kernel32
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	kernel32
ProductName	Microsoft® Windows® Operating System

- As I was getting error while loading the file in dependency walker, I've gathered the information from cff explorer, here we can see the dependencies of the dll files.

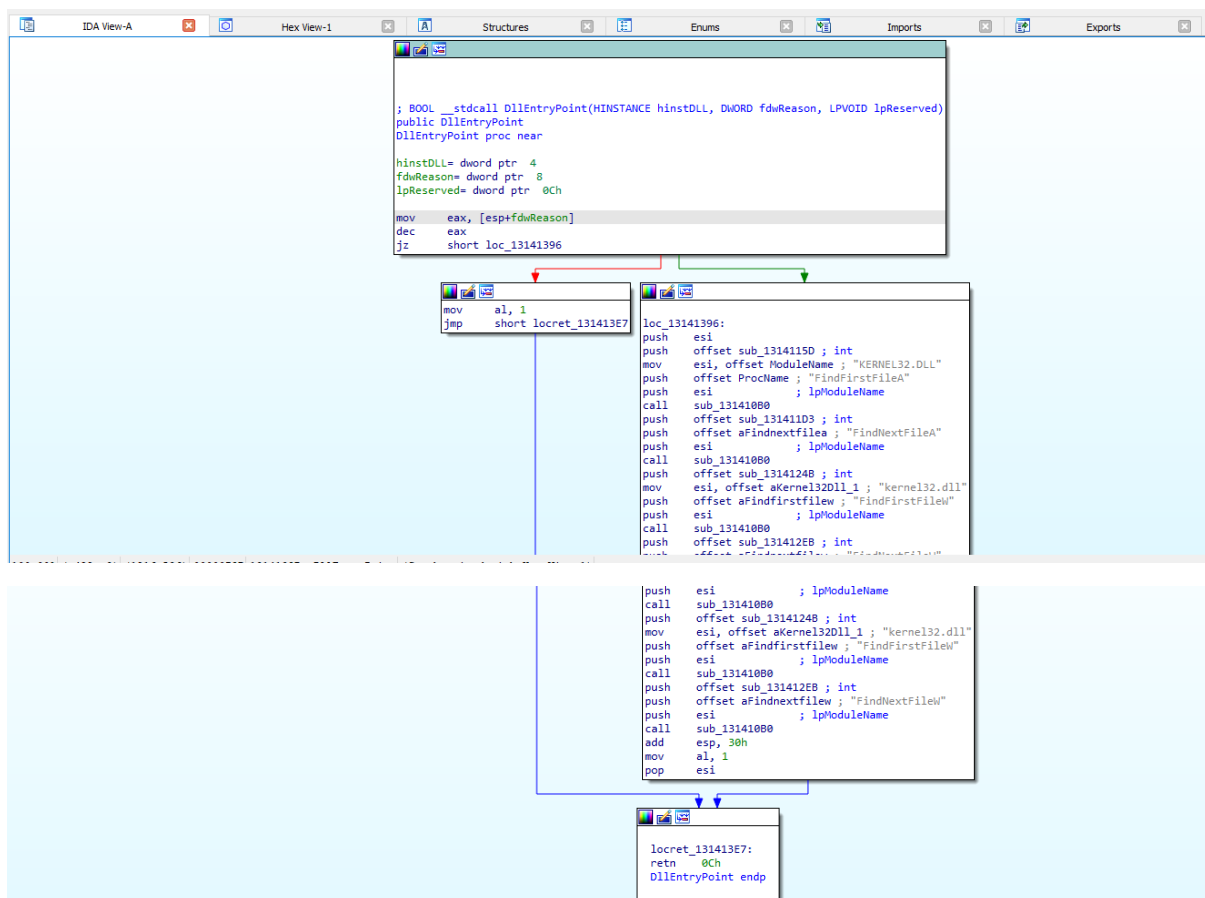
IDA Pro tool:

```

.idata:13141000 ;
.idata:13141000 ;
.idata:13141000 ; This file was generated by The Interactive Disassembler (IDA)
.idata:13141000 ; Copyright (c) 2021 Hex-Rays, <support@hex-rays.com>
.idata:13141000 ; License info: 48-6CCC-38BF-48
.idata:13141000 ; IDA PRO 7.6 SP1
.idata:13141000 ;
.idata:13141000 ;
.idata:13141000 ; Input SHA256 : 2014CED97466E3F29004D0785BE7DF12F37F4795CF32543145229815A8D20857
.idata:13141000 ; Input MD5 : 6A6C1DAD9852057F81589D4CA5E962CB
.idata:13141000 ; Input CRC32 : A7173870
.idata:13141000 ;
.idata:13141000 ; File Name : C:\Users\Dhairya Changela\Desktop\DopeBot v0.22 UnCrippled- Feb 2007\Resources\Files\hook.dll
.idata:13141000 ; Format : Portable executable for 80386 (PE)
.idata:13141000 ; Imagebase : 13140000
.idata:13141000 ; Timestamp : 45CB7A26 (Thu Feb 08 19:29:42 2007)
.idata:13141000 ; Section 1. (virtual address 00001000)
.idata:13141000 ; Virtual size : 00000574 ( 1396.)
.idata:13141000 ; Section size in file : 00000600 ( 1536.)
.idata:13141000 ; Offset to raw data for section: 00000400
.idata:13141000 ; Flags C0000040: Data Readable Writable
.idata:13141000 ; Alignment : default
.idata:13141000 ;
.idata:13141000 ; Imports from KERNEL32.dll
.idata:13141000 ;
.idata:13141000 ;
.idata:13141000 ; .686p
.idata:13141000 ; .mmx
.idata:13141000 ; .model flat
.idata:13141000 ;
.idata:13141000 ; =====
.idata:13141000 ; Segment type: Externs
.idata:13141000 ; _idata
.idata:13141000 ; BOOL (__stdcall *VirtualProtect)(LPVOID lpAddress, SIZE_T dwSize, DWORD flNewProtect, PDWORD lpfOldProtect)
.idata:13141000 ; extrn VirtualProtect:DWORD
.idata:13141000 ; ; CODE XREF: sub_131410B0+8F4p
.idata:13141000 ; ; sub_131410B0+A04p

```

- Here we are retrieving general information including file name, format, sha, md5, crc32 hash values.



MALWARE ANALYSIS

- We also get entire graph of the malware which uses different instructions.

File	IDA View-A	Hex View-1	Names	Signatures	IDA View-B
13141030	00 00 00 00 ?? ?? ?? ??	00 00 00 00 40 10 14 13????.0...		
13141040	5F 64 6F 70 65 5F 00 00	46 69 6E 64 4E 65 78 74	_dope?...FindNext		
13141050	46 69 6C 65 57 00 00 00	46 69 6E 64 46 69 72 73	FileW...FindFirs		
13141060	74 46 69 6C 65 57 00 00	68 65 72 6E 65 6C 33 32	tFileW...kernel32		
13141070	2E 64 6C 6C 00 00 00 00	46 69 6E 64 4E 65 78 74	.dll....FindNext		
13141080	46 69 6C 65 41 00 00 00	46 69 6E 64 46 69 72 73	FileA...FindFirs		
13141090	74 46 69 6C 65 41 00 00	48 45 52 4E 45 4C 33 32	tFileA...KERNEL32		
131410A0	2E 44 4C 4C 00 00 00 00	00 00 00 00 00 00 00 00	.DLL.....		
131410B0	55 88 EC 51 51 53 56 88	35 08 10 14 13 57 6A 00	U<iQQVS<...Wj.		
131410C0	FF 06 FF 75 0C 88 F8 FF	75 08 FF D6 50 FF 15 04	yöyü.öyü.yöPy...		
131410D0	10 14 13 88 D8 85 D8 74	7D 66 81 3F 4D 5A 75 76	...<0üf>f.MZuv		
131410E0	8B 47 3C 03 C7 81 38 50	45 00 00 75 69 88 B0 80	<G<.C.8PE...ui<€		
131410F0	00 00 00 03 F7 38 F0 74	5D 88 46 0C 85 C0 74 16>öt>f...Ät.		
13141100	F7 75 08 03 C7 50 E8 E5	02 00 00 59 85 C0 59 74	yü..CPä8...Y.YÄt		
13141110	05 83 C6 14 EB E3 83 7E	0C 00 74 3A 88 76 10 03	.fæ.æäf...t<v...		
13141120	F7 88 06 85 C0 74 2F 38	C3 74 05 83 C6 04 EB F1	+<...Ät/>Ät.fæ.æñ		
13141130	8B 3D 00 10 14 13 8D 45	FC 50 6A 40 6A 04 56 FF	<...EUPj@j.VY		
13141140	07 88 45 10 89 06 8D 45	F8 50 FF 75 FC 6A 04 56	x<E.ë...EöPyüj.V		
13141150	FF 07 8B C3 EB 02 33 C0	5F 5E 5B C9 C3 55 8B EC	y<x<Äe.3Ä...[EÄU<i		
13141160	81 EC 0C 02 00 00 53 88	1D 10 10 14 13 56 57 FF	.i....S<...WVj		
13141170	75 0C FF 75 08 FF D3 FF	75 08 89 45 FC 8D 85 F8	u.yü.yöyü.æÜ...ø		
13141180	FE FF FF 50 E8 61 02 00	00 59 8D 85 F8 FE FF FF	pöyPëa...Y.yøpöy		
13141190	59 50 FF 15 34 10 14 13	FF 35 3C 10 14 13 8D 85	YPy.4...y5<...µ		
131411A0	F8 FE FF FF 8D B0 F4 FD	FF FF 8D 85 F4 FD FF FF	øpyy...Xöyy...öyy		
131411B0	A5 50 66 A5 FF 15 0C 10	14 13 85 C0 75 08 FF 75	xPfx...Äu.yü		
131411C0	0C 0F 75 08 FF D3 89 45	FC 88 45 FC 5F 5E 5B C9	yü.yö&Ü<EÜ...[É		
131411D0	C2 08 00 55 8B EC 81 EC	0C 02 00 00 53 8B 1D 14	Ä...U<i.i...S<...		
131411E0	10 14 13 56 8B 75 0C 57	56 FF 75 08 FF D3 89 45	...V<u.WVjü.yö&E		
131411F0	FC 83 C6 2C 8D 85 F8 FE	FF FF 56 50 E8 E9 01 00	üfæ...øpyyVpëe...		
13141200	00 59 8D 85 F8 FE FF FF	59 50 FF 15 34 10 14 13	.Y...øpyyYPy.4...		
13141210	FF 35 3C 10 14 13 8D 85	F8 FE FF FF 8D B0 F4 FD	y5<...µpyy...Xöy		
13141220	FF FF 8D 85 F4 FD FF FF	A5 50 66 A5 FF 15 0C 10	yü...öyyyxpfx...		
13141230	14 13 85 C0 75 08 FF 75	0C FF 75 08 FF D3 89 45	...Äu.yü.yü.yö&E		
13141240	FC 80 45 FC 5F 5E 5B C9	C2 08 00 55 8B EC 81 EC	U<EÜ...[ÉÄ.U<i.i		
13141250	0C 02 00 00 66 A1 F8 13	14 13 53 56 88 75 0C 57	...fj&...SV<u.W		
13141260	6A 40 66 89 85 F8 FE FF	FF 59 33 C0 8D B0 FA FE	j@fk...øpyyY3Ä.Xüp		
13141270	FF FF 8B 1D 1C 10 14 13	56 FF 75 08 F3 AB 66 AB	yü<...Vjü.ä&f<...		
13141280	FF D3 33 C9 89 45 FC 51	8B 04 01 00 00 51 8D 95	y03É&EÜQ...<Q.*		

Address	Ordinal	Name	Library
13141000		VirtualProtect	KERNEL32
13141004		GetProcAddress	KERNEL32
13141008		GetModuleHandleA	KERNEL32
1314100C		lstrcpmA	KERNEL32
13141010		FindFirstFileA	KERNEL32
13141014		FindNextFileA	KERNEL32
13141018		WideCharToMultiByte	KERNEL32
1314101C		FindFirstFileW	KERNEL32
13141020		FindNextFileW	KERNEL32
13141028		_stricmp	MSVCRT
1314102C		sprintf	MSVCRT
13141034		PathStripPathA	SHLWAPI

- We also get entire view of hex values, which file it is importing and which files it is exporting.

MALWARE ANALYSIS

Function name	Segment
sub_131410B0	.data
sub_1314115D	.data
sub_131411D3	.data
sub_1314124B	.data
sub_131412EB	.data
DllEntryPoint	.data
sprintf	.data
_strcmp	.data

- We can see the various functions and pseudo code of any particular function as below.

```
IDA View-A Hex View-1 Pseudocode-A
1 HANDLE __stdcall sub_1314115D(LPCSTR lpFileName, LPWIN32_FIND_DATA lpFindFileData)
2 {
3     int String1; // [esp+Ch] [ebp-20Ch] BYREF
4     __int16 v4; // [esp+10h] [ebp-208h]
5     int Buffer; // [esp+110h] [ebp-108h] BYREF
6     __int16 v6; // [esp+114h] [ebp-104h]
7     HANDLE FirstFileA; // [esp+214h] [ebp-4h]
8
9     FirstFileA = FindFirstFileA(lpFileName, lpFindFileData);
10    sprintf((char *const)&Buffer, lpFileName);
11    PathStripPathA((LPSTR)&Buffer);
12    String1 = Buffer;
13    v4 = v6;
14    if ( !strcmpA((LPCSTR)&String1, lpString2) )
15        return FindFirstFileA(lpFileName, lpFindFileData);
16    return FirstFileA;
17 }
```

Name	Start	End	R	W	X	D	L	Align	Base	Type
.idata	13141000	1314103C	R	W	.	.	L	para	0002	public
.data	1314103C	13142000	R	W	.	.	L	para	0001	public

- Two segments were found in the malware named “.idata” and “.data”.

Functions				Strings				Segments				Se			
Address	Length	Type	String												
[S] .data:13141088	0000000F	C	FindFirstFileA												
[S] .data:131414CE	0000000F	C	FindFirstFileA												
[S] .data:13141058	0000000F	C	FindFirstFileW												
[S] .data:13141506	0000000F	C	FindFirstFileW												
[S] .data:13141078	0000000E	C	FindNextFileA												
[S] .data:131414E0	0000000E	C	FindNextFileA												
[S] .data:13141048	0000000E	C	FindNextFileW												
[S] .data:13141518	0000000E	C	FindNextFileW												
[S] .data:131414AE	00000011	C	GetModuleHandleA												
[S] .data:1314149C	0000000F	C	GetProcAddress												
[S] .data:13141098	0000000D	C	KERNEL32.DLL												
[S] .data:13141526	0000000D	C	KERNEL32.dll												
[S] .data:1314153E	0000000B	C	MSVCRT.dll												
[S] .data:1314154C	0000000F	C	PathStripPathA												
[S] .data:1314155C	0000000C	C	SHLWAPI.dll												
[S] .data:1314148A	0000000F	C	VirtualProtect												
[S] .data:131414F0	00000014	C	WideCharToMultiByte												
[S] .data:13141040	00000007	C	_dope_												
[S] .data:1314156A	00000009	C	_stricmp												
[S] .data:13141068	0000000D	C	kernel32.dll												
[S] .data:131414C2	0000000A	C	lstrcmpiA												
[S] .data:13141536	00000008	C	sprintf												

- We can also see what are the different strings are there with its address value.

Dynamic Analysis:

- There are various cpp files which are interconnected to other files

Name	Date modified	Type	Size
Protocol	8/13/2022 11:05 PM	File folder	
bot	8/13/2022 11:05 PM	CPP File	31 KB
bot.h	8/13/2022 11:05 PM	H File	3 KB
bt1	8/13/2022 11:05 PM	CPP File	28 KB
bt1.h	8/13/2022 11:05 PM	H File	3 KB
crypto	8/13/2022 11:05 PM	CPP File	1 KB
crypto.h	8/13/2022 11:05 PM	H File	1 KB
download	8/13/2022 11:05 PM	CPP File	3 KB
download.h	8/13/2022 11:05 PM	H File	1 KB
EliRT.h	8/13/2022 11:05 PM	H File	2 KB
EliRT_COFF.lib	8/13/2022 11:05 PM	LIB File	4 KB
file	8/13/2022 11:05 PM	CPP File	3 KB
file.h	8/13/2022 11:05 PM	H File	1 KB
fwb	8/13/2022 11:05 PM	CPP File	2 KB
fwb.h	8/13/2022 11:05 PM	H File	1 KB
injection	8/13/2022 11:05 PM	CPP File	2 KB
injection.h	8/13/2022 11:05 PM	H File	1 KB
install	8/13/2022 11:05 PM	CPP File	5 KB
install.h	8/13/2022 11:05 PM	H File	1 KB
keylogger	8/13/2022 11:05 PM	CPP File	5 KB
keylogger.h	8/13/2022 11:05 PM	H File	1 KB
klgger	8/13/2022 11:05 PM	CPP File	5 KB
klgger.h	8/13/2022 11:05 PM	H File	1 KB
melt	8/13/2022 11:05 PM	CPP File	3 KB
melt.h	8/13/2022 11:05 PM	H File	1 KB
misc	8/13/2022 11:05 PM	CPP File	5 KB
misc.h	8/13/2022 11:05 PM	H File	1 KB
netinfo	8/13/2022 11:05 PM	CPP File	2 KB
netinfo.h	8/13/2022 11:05 PM	H File	1 KB
process	8/13/2022 11:05 PM	CPP File	3 KB
process.h	8/13/2022 11:05 PM	H File	1 KB
registry	8/13/2022 11:05 PM	CPP File	2 KB
registry.h	8/13/2022 11:05 PM	H File	1 KB
rootkit	8/13/2022 11:05 PM	CPP File	4 KB
rootkit.h	8/13/2022 11:05 PM	H File	1 KB
rt07	8/13/2022 11:05 PM	CPP File	3 KB
rt07.h	8/13/2022 11:05 PM	H File	1 KB

- Let's execute the main .dll file.

```
Windows PowerShell
PS C:\Users\Dhairya.Changela\Desktop\DopeBot v0.22 UnCrippled- Feb 2007\Resources\Files> regsvr32.exe /s hook.dll
PS C:\Users\Dhairya.Changela\Desktop\DopeBot v0.22 UnCrippled- Feb 2007\Resources\Files>
```

MALWARE ANALYSIS

Process Explorer tool:

Before executing:

Process Monitor - Sysinternals.com/sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
22.03.	Explorer.EXE	3960	RegQueryKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegQueryKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegQueryKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	CreateFile	HKEY\Software\Classes\CLSID\{56AD0A2D-5000-4F85-...	NAME NOT FOUND	Desired Access: Read
22.03.	Explorer.EXE	3960	QueryNameInformationFile	C:\Users\Diaryha Chingela\Desktop\MA Tools\ProcessMonitor\Frocon64.exe	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Replaces Parent, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, Op...
22.03.	Explorer.EXE	3960	QueryBasicInformationFile	C:\Users\Diaryha Chingela\Desktop\MA Tools\ProcessMonitor\Frocon64.exe	SUCCESS	CreationTime: 6/22/2021 2:57:42 PM, LastAccessTime: 10/16/2022 2:20:28 PM, LastWriteTime: 8/28/2024 11:13 PM, ChangeTime: 10/12/2022 4:54:14
22.03.	Explorer.EXE	3960	CloseFile	C:\Users\Diaryha Chingela\Desktop\MA Tools\ProcessMonitor\Frocon64.exe	SUCCESS	
22.03.	Explorer.EXE	3960	CreateFile	C:\Users\Diaryha Chingela\Desktop\MA Tools\ProcessMonitor\Frocon64.exe	SUCCESS	Desired Access: Read Data/Lit Directory, Synchronization, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, FileInformationClass: FileBothDirectoryInformation, File: Users, 2, Users
22.03.	Explorer.EXE	3960	CloseFile	C:\Users\Diaryha Chingela\Desktop\MA Tools\ProcessMonitor\Frocon64.exe	SUCCESS	
22.03.	Explorer.EXE	3960	CreateFile	C:\Users\Diaryha Chingela\Desktop\MA Tools\ProcessMonitor\Frocon64.exe	SUCCESS	Desired Access: Read Data/Lit Directory, Synchronization, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, FileInformationClass: FileBothDirectoryInformation, File: Desktop, 2, Desktop
22.03.	Explorer.EXE	3960	QueryDirectory	C:\Users\Diaryha Chingela\Desktop\MA Tools\ProcessMonitor\Frocon64.exe	SUCCESS	
22.03.	Explorer.EXE	3960	CreateFile	C:\Users\Diaryha Chingela\Desktop\MA Tools\ProcessMonitor\Frocon64.exe	SUCCESS	Desired Access: Read Data/Lit Directory, Synchronization, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, FileInformationClass: FileBothDirectoryInformation, File: MA Tools, 2, MA Tools
22.03.	Explorer.EXE	3960	CloseFile	C:\Users\Diaryha Chingela\Desktop\MA Tools\ProcessMonitor\Frocon64.exe	SUCCESS	
22.03.	Explorer.EXE	3960	ReadFile	C:\Windows\System32\windows.storage	SUCCESS	Offset: 6,912,000, Length: 12,288, I/O Page: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
22.03.	Explorer.EXE	3960	RegQueryKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Query: Name
22.03.	Explorer.EXE	3960	RegOpenKey	HKEY\Software\Classes	SUCCESS	Desired Access: Read
22.03.	Explorer.EXE					

After executing:

Process Monitor - Sysinternals: www.sysinternals.com

File Edit View Filter Tools Options Help

MALWARE ANALYSIS

Process Monitor tool:

Before executing:

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-NFRPQDO\Dhairya Changela]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
ApplicationFrameHost.exe		8,516 K	29,932 K	3096	Application Frame Host	Microsoft Corporation	(Verified) Microsoft Windows	
audiodg.exe		6,300 K	11,972 K	6724				
conhost.exe	< 0.01	6,644 K	1,736 K	6200				
Cortana.exe	Susp...	27,148 K	73,324 K	7708	Cortana	Microsoft Corporation	(No signature was present in the subject) Microsoft Corporation	
csrss.exe	< 0.01	1,764 K	5,256 K	432				
csrss.exe		1,832 K	5,188 K	508				
ctfmon.exe		3,984 K	19,608 K	3644				
dllhost.exe		5,424 K	15,036 K	4728	COM Surrogate	Microsoft Corporation	(Verified) Microsoft Windows	
dllhost.exe		3,288 K	12,288 K	5560	COM Surrogate	Microsoft Corporation	(Verified) Microsoft Windows	
dwm.exe	2.47	49,072 K	97,036 K	932				
explorer.exe	< 0.01	64,584 K	197,296 K	3960	Windows Explorer	Microsoft Corporation	(Verified) Microsoft Windows	
fontdrvhost.exe		7,088 K	13,760 K	720				
fontdrvhost.exe		1,260 K	3,320 K	728				
GoogleCrashHandler.exe		1,736 K	360 K	7060				
GoogleCrashHandler64.exe		1,836 K	472 K	7124				
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs			
lsass.exe	Susp...	12,128 K	51,104 K	6172	Local Security...	Microsoft Corporation	(Verified) Microsoft Windows	
lsass.exe	< 0.01	7,460 K	19,384 K	600	Local Security Authority Process	Microsoft Corporation	(Verified) Microsoft Windows Publisher	
Memory Compression		256 K	44,284 K	1476				
Microsoft.Photos.exe	Susp...	40,232 K	1,856 K	2056			(No signature was present in the subject)	
MsMpEng.exe		249,824 K	213,976 K	3612	Antimalware Service Execut...	Microsoft Corporation	(Verified) Microsoft Windows Publisher	
MusNotification.exe		3,644 K	732 K	380	MusNotification.exe	Microsoft Corporation	(Verified) Microsoft Windows	
OneDrive.exe		32,876 K	80,584 K	8700	Microsoft OneDrive	Microsoft Corporation	(Verified) Microsoft Corporation	
osqueryd.exe		5,268 K	12,476 K	2596	osquery daemon and shell	Osquery Foundation	(The certificate is not valid for the requested usage) Osquery Foundation	
osqueryd.exe	< 0.01	8,620 K	1,304 K	5784				
PhoneExperienceHost.exe		67,380 K	142,020 K	5072	PhoneExperienceHost	Microsoft Corporation	(Verified) Microsoft Corporation	
process64.exe	82.71	20,520 K	47,244 K	6288	Sysinternals Process Explorer	Sysinternals - www.sysinter...	(Verified) Microsoft Corporation	
Registry		3,152 K	22,604 K	72				
RuntimeBroker.exe		6,172 K	26,312 K	5084	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe		14,060 K	41,488 K	5256	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe		8,348 K	32,636 K	6316	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe	< 0.01	2,536 K	16,808 K	6512	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe		3,580 K	22,696 K	7896	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe		4,324 K	24,300 K	7508	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe		2,176 K	11,024 K	7924	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe		5,200 K	18,392 K	8340	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
SearchApp.exe	Susp...	112,892 K	189,304 K	4384	Search application	Microsoft Corporation	(Verified) Microsoft Windows	
SearchApp.exe	Susp...	15,616 K	61,240 K	3252	Search application	Microsoft Corporation	(Verified) Microsoft Windows	
SearchIndexer.exe		31,952 K	45,996 K	3204	Microsoft Windows Search I...	Microsoft Corporation	(Verified) Microsoft Windows	
SecurityHealthService.exe		5,116 K	18,496 K	4260	Windows Security Health Se...	Microsoft Corporation	(Verified) Microsoft Windows Publisher	
SecurityHealthSystray.exe		1,784 K	13,388 K	6928	Windows Security notificatio...	Microsoft Corporation	(Verified) Microsoft Windows	
services.exe	2.47	4,980 K	9,488 K	592				
SgmBroker.exe		3,856 K	7,016 K	6888	System Guard Runtime Monit...	Microsoft Corporation	(Verified) Microsoft Windows Publisher	
ShellExperienceHost.exe	Susp...	10,112 K	44,244 K	6240	Windows Shell Experience H...	Microsoft Corporation	(Verified) Microsoft Windows	
shost.exe		6,740 K	31,180 K	3112	Shell Infrastructure Host	Microsoft Corporation	(Verified) Microsoft Windows	
smartscreen.exe		7,976 K	23,860 K	6712	Windows Defender SmartScr...	Microsoft Corporation	(Verified) Microsoft Windows	
smss.exe		1,060 K	1,116 K	340				
spoolsv.exe		5,112 K	13,060 K	2240	Spooler Sub-System App	Microsoft Corporation	(Verified) Microsoft Windows	
StartMenuExperienceHost.exe		21,632 K	63,724 K	5000			(Verified) Microsoft Windows	
svchost.exe	< 0.01	11,460 K	32,644 K	736	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher	

After executing:

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-NFRPQDO\Dhairya Changela]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
ApplicationFrameHost.exe		8,032 K	30,120 K	6736	Application Frame Host	Microsoft Corporation	(Verified) Microsoft Windows	
audiodg.exe		6,476 K	11,936 K	3096				
BackgroundTaskHost.exe	Susp...	3,160 K	16,632 K	1616	Background Task Host	Microsoft Corporation	(Verified) Microsoft Windows	
conhost.exe	< 0.01	6,640 K	1,032 K	5976				
Cortana.exe	Susp...	27,228 K	72,944 K	6884	Cortana	Microsoft Corporation	(No signature was present in the subject) Microsoft Corporation	
csrss.exe		1,932 K	5,416 K	432				
csrss.exe	< 0.01	1,776 K	5,356 K	508				
ctfmon.exe	< 0.01	4,348 K	21,628 K	3512				
dllhost.exe		5,744 K	15,652 K	4364	COM Surrogate	Microsoft Corporation	(Verified) Microsoft Windows	
dllhost.exe		3,616 K	12,424 K	2944	COM Surrogate	Microsoft Corporation	(Verified) Microsoft Windows	
dwm.exe	1.47	54,976 K	119,056 K	932				
explorer.exe	2.94	71,672 K	196,896 K	3748	Windows Explorer	Microsoft Corporation	(Verified) Microsoft Windows	
fontdrvhost.exe		3,164 K	7,264 K	720				
fontdrvhost.exe		1,260 K	3,368 K	728				
GoogleCrashHandler.exe		1,752 K	284 K	5864				
GoogleCrashHandler64.exe		1,836 K	340 K	6000				
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs			
lsass.exe	< 0.01	6,948 K	19,644 K	600	Local Security Authority Proc...	Microsoft Corporation	(Verified) Microsoft Windows Publisher	
Memory Compression		40 K	0 K	1596				
Microsoft.Photos.exe	Susp...	38,748 K	1,884 K	5180			(No signature was present in the subject)	
MsMpEng.exe		210,928 K	117,204 K	2588	Antimalware Service Execut...	Microsoft Corporation	(Verified) Microsoft Windows Publisher	
notepad.exe		12,476 K	27,768 K	3608				
OneDrive.exe		31,668 K	89,768 K	6224	Microsoft OneDrive	Microsoft Corporation	(Verified) Microsoft Corporation	
osqueryd.exe	< 0.01	5,276 K	14,060 K	2524	osquery daemon and shell	Osquery Foundation	(The certificate is not valid for the requested usage) Osquery Foundation	
osqueryd.exe		8,908 K	1,760 K	5868				
PhoneExperienceHost.exe		66,656 K	137,452 K	3396	PhoneExperienceHost	Microsoft Corporation	(Verified) Microsoft Corporation	
process64.exe	2.94	25,884 K	50,508 K	8100	Sysinternals Process Explorer	Sysinternals - www.sysinter...	(Verified) Microsoft Corporation	
Registry		4,376 K	79,144 K	72				
Regshot x64-ANSI.exe		302,952 K	313,136 K	6744				
RuntimeBroker.exe	< 0.01	6,120 K	26,104 K	5000	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe		15,964 K	46,968 K	4728	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe		4,544 K	24,300 K	2008	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe	< 0.01	2,760 K	16,008 K	928	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe		3,516 K	22,696 K	6888	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe		2,520 K	17,148 K	7260	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe		5,092 K	18,220 K	5352	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe	< 0.01	3,332 K	19,972 K	5992	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	
ScreenClippingHost.exe	< 0.01	19,316 K	73,988 K	7944			(Verified) Microsoft Windows	
SearchApp.exe	Susp...	141,736 K	227,000 K	3968	Search application	Microsoft Corporation	(Verified) Microsoft Windows	
SearchIndexer.exe	< 0.01	26,544 K	36,548 K	4072	Microsoft Windows Search I...	Microsoft Corporation	(Verified) Microsoft Windows	
SecurityHealthService.exe		5,092 K	18,572 K	3396	Windows Security Health Se...	Microsoft Corporation	(Verified) Microsoft Windows Publisher	
SecurityHealthSystray.exe		1,776 K	13,072 K	4436	Windows Security notificatio...	Microsoft Corporation	(Verified) Microsoft Windows	
services.exe		4,716 K	9,908 K	592				
SgmBroker.exe		3,652 K	6,948 K	6636	System Guard Runtime Monit...	Microsoft Corporation	(Verified) Microsoft Windows Publisher	
ShellExperienceHost.exe	< 0.01	9,916 K	43,656 K	8084	Windows Shell Experience H...	Microsoft Corporation	(Verified) Microsoft Windows	
shost.exe		6,084 K	28,152 K	2272	Shell Infrastructure Host	Microsoft Corporation	(Verified) Microsoft Windows	
smartscreen.exe		8,016 K	24,056 K	2412	Windows Defender SmartScr...	Microsoft Corporation	(Verified) Microsoft Windows	
smss.exe		1,076 K	1,248 K	340				
spoolsv.exe		5,064 K	15,452 K	2180	Spooler Sub-System App	Microsoft Corporation	(Verified) Microsoft Windows	
StartMenuExperienceHost.exe		20,956 K	65,620 K	4880			(Verified) Microsoft Windows	

RegShot tool:

- After taking the 2nd shot in regshot tool, following registry keys changes have been made.

```
Regshot 1.9.0 x64 ANSI
```

```
Comments:
```

```
Datetime: 2022/10/16 08:55:16 , 2022/10/16 09:19:42
```

```
Computer: DESKTOP-NFRPQDO , DESKTOP-NFRPQDO
```

```
Username: Dhairya Changela , Dhairya Changela
```

```
-----  
Keys deleted: 20359  
-----
```

```
-----  
Keys added: 19|  
-----
```

```
HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\36B12B49F9819ED74C9EBC380FC6568F5DACB2F7
```

```
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1044
```

```
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2840
```

```
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4112
```

```
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4736
```

```
-----  
Values deleted: 24066  
-----
```

```
HKLM\DRIVERS\DriverDatabase\Version: 0x0A000000
```

```
HKLM\DRIVERS\DriverDatabase\SchemaVersion: 0x00010000
```

```
HKLM\DRIVERS\DriverDatabase\UpdateDate: 60 59 85 E4 E5 DA D8 01
```

```
HKLM\DRIVERS\DriverDatabase\SetupStatus: 0x00000000
```

```
HKLM\DRIVERS\DriverDatabase\DeviceIds\*AEI0276\mdmmetri.inf: 01 FF 00 00
```

```
HKLM\DRIVERS\DriverDatabase\DeviceIds\*AEI9240\mdmti.inf: 01 FF 00 00
```

```
-----  
Total changes: 44736  
-----
```


HYBRID ANALYSIS:

Sandbox analysis (website):

- Here we've done sandbox analysis of the malware on hybrid-analysis website and found General information as below.

HYBRID ANALYSIS Sandbox Quick Scans File Collections Resources Request Info

Search: IP, Domain, Hash...

Analysis Overview

Submission name: hook.dll
 Size: 3KiB
 Type: [pefile](#) [executable](#)
 Mime: application/x-dosexec
 SHA256: 2014ced97466e3f290d4dd785be7df12f37f4795cf32543145229b15a8d20857
 Operating System: Windows
 Last Anti-Virus Scan: 11/12/2021 09:28:46 (UTC)
 Last Sandbox Report: 10/24/2021 06:15:41 (UTC)

malicious
 Threat Score: 100/100
 AV Detection: 81%
 Labeled as: Backdoor.Irc.Sdbot

[Link](#) [Twitter](#) [E-Mail](#)

Anti-Virus Results

CrowdStrike Falcon
 100%
 Static Analysis and ML
 Last Update: 11/12/2021 09:28:46 (UTC)
 View Details: N/A
 Visit Vendor: [Link](#)
[GET STARTED WITH A FREE TRIAL](#)

MetaDefender
 72%
 Multi Scan Analysis
 Last Update: 11/12/2021 09:28:46 (UTC)
 View Details: [Link](#)
 Visit Vendor: [Link](#)

VirusTotal
 72%
 Multi Scan Analysis
 Last Update: 11/12/2021 09:28:46 (UTC)
 View Details: [Link](#)
 Visit Vendor: [Link](#)

Falcon Sandbox Reports

MALICIOUS

hook.dll

Analyzed on: 10/22/2021 12:35:04 (UTC)

Environment: Windows 7 64 bit

Threat Score: 100/100

AV Detection: 72% Backdoor.Irc.Sdbot

Indicators: 3 2 3

Network: (none)

MALICIOUS

hook.dll

Analyzed on: 10/24/2021 06:15:41 (UTC)

Environment: Windows 7 32 bit

Threat Score: 100/100

AV Detection: 72% Backdoor.Irc.Sdbot

Indicators: 3 2 6

Network: (none)

MALWARE ANALYSIS

- Malicious and suspicious indicators were found in the file

Indicators

Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

Malicious Indicators3

External Systems

Sample was identified as malicious by a large number of Antivirus engines

Sample was identified as malicious by at least one Antivirus engine

Hiding 1 Malicious Indicators

All indicators are available only in the private selfservice or standalone version.

Suspicious Indicators

Unusual Characteristics

Entrypoint in PE header is within an uncommon section

details"2014ced97466e3f290d4dd785be7df12f37f4795cf32543145229b15a8d20857.bin" has an entrypoint in section ".data"

sourceStatic Parser

relevance10/10

Imports suspicious APIs

detailsGetModuleHandleA
FindNextFileW
VirtualProtect
FindNextFileA
FindFirstFileA
FindFirstFileW
GetProcAddress

sourceStatic Parser

relevance1/10

- The malware imports following files.

File Imports

KERNEL32.dll

MSVCRT.dll

SHLWAPI.dll

FindNextFileW

GetModuleHandleA

GetProcAddress

lstrcpmA

VirtualProtect

WideCharToMultiByte

- The metadata of the file.

File Metadata

File Compositions

Imported Objects

File Analysis

- 1.CPP Files compiled with CL.EXE 12.00 (Visual Studio 6) (build: 8168)
- 5 .LIB Files generated with LIB.EXE 7.10 (Visual Studio .NET 2003) (build: 4035)

File Metadata

File Compositions

Imported Objects

File Analysis

- File contains C++ code
- File is the product of a small codebase (1 files)

DHAIRYA CHANGELA (19162171007)

18

Behaviour:

- After manually analysed the code, one of the file initiates a bot which then logs in to the host system, opening a socket.
- Further this bot downloads and activates multiple other bots through the internet.
- These multiple bots downloaded have various purposes such as listed below:
 - A bot is http downloader which downloads various files required by the boat to perform their respective tasks.
 - Another bot is programmed to open, execute and delete various files (majorly cpp & header files) as and when required by the bots.
 - Another bot is a network sniffer that sniffs the whole network of the target system.
 - Another bot is a key logger which records all the keystrokes of the target and sends them over the internet to the host system.
 - Another bot is a bandwidth flooder which floods the network of the target system disallowing it to perform any other activity over the internet.
 - Another bot is a system information stealer which grabs all the target system information and sends it over the internet.
 - Another bot's task is to update the registry keys in order to allow smooth functioning of the backdoor.
 - Another bot is programmed to list the current processes and kill the processes.
 - Another bot is a IP grabber, which scans the whole network to which the target is connected.
 - Another bot is programmed to send the files over the internet using ftp, tftp protocols.
 - Another bot is programmed as a rootkit to access all the files and data on the target system which are not allowed to normal users.
 - Another bot is programmed to shutdown all the other bots after the task is completed.

Conclusion:

- Seeing The files created by the malware when it was executed shows that the whole malware was designed using c++ as a base language and the malware was professionally developed to grab each and every vital information on the target system ranging from its IP Address, registry keys, current processes to the files not visible to normal users. This clearly shows that when the malware gets executed it will straight away have admin or root level privileges on the target system. It was also observed that the malware was self-capable of deleting the files it had create and killing the processes it starts in the backhand. Hence, giving the user no clue about the execution of the malware.