Memory Analysis

With the analysis of volatility tools, I find a malicious executing file which is named “clickme.exe” on “C:\Users\ADF20221\Downloads\” location. And the file process ID or PID is 2012.

```
chrome.exe pid:   1240
Command line : "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --display-capture-permissions-p
r=1 --num-raster-threads=1 --renderer-client-id=29 --time-ticks-at-unix-epoch=-1666618329235540 --launch-time-ticks=19
0695841114253820519,131072 /prefetch:1
************************************************************************
chrome.exe pid:   4556
Command line : "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --display-capture-permissions-p
r=1 --num-raster-threads=1 --renderer-client-id=30 --time-ticks-at-unix-epoch=-1666618329235540 --launch-time-ticks=19
0695841114253820519,131072 /prefetch:1
************************************************************************
chrome.exe pid:    648
Command line : "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --display-capture-permissions-p
r=1 --num-raster-threads=1 --renderer-client-id=31 --time-ticks-at-unix-epoch=-1666618329235540 --launch-time-ticks=20
0695841114253820519,131072 /prefetch:1
************************************************************************
chrome.exe pid:   4852
Command line : "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --display-capture-permissions-p
r=1 --num-raster-threads=1 --renderer-client-id=32 --time-ticks-at-unix-epoch=-1666618329235540 --launch-time-ticks=20
0695841114253820519,131072 /prefetch:1
************************************************************************
dllhost.exe pid:   3672
Command line : C:\Windows\system32\DllHost.exe /Processid:{973D20D7-562D-44B9-B70B-5A0F49CCDF3F}
************************************************************************
WmiPrvSE.exe pid:   6396
Command line : C:\Windows\system32\wbem\wmiprvse.exe
************************************************************************
cmd.exe pid:    856
Command line : "C:\Windows\system32\cmd.exe"
************************************************************************
conhost.exe pid:   3604
Command line : \??\C:\Windows\system32\conhost.exe 0x4
************************************************************************
clickme.exe pid:   2012
Command line : "C:\Users\ADF20221\Downloads\clickme.exe"
************************************************************************
cmd.exe pid:   4892
************************************************************************
FTK Imager.exe pid:   1204
Command line : "C:\Program Files\AccessData\FTK Imager\FTK Imager.exe"
************************************************************************
svchost.exe pid:   4460
Command line : C:\Windows\System32\svchost.exe -k LocalServiceAndNoImpersonation -p -s wcncsvc
************************************************************************
 pid:      0
```

We can see here that the file was executed by the ADF20221 user. We dump the file from the memory file on my local PC by the volatility tools. The file is downloaded with “executable.2012.exe” name. We can see here the PID 2012 is added.

And I make scans by virustotal online tools.

60d645236bcabd0f9754ae49ee8b73fd7349af9a960439981fd69124532e560a

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 4

Basic properties

MD5	32de42a20c013aa80dc138b9bbc430ef
SHA-1	45ef2de4b50c15aa1c02894ffe2f0ec7b964344b
SHA-256	60d645236bcabd0f9754ae49ee8b73fd7349af9a960439981fd69124532e560a
Vhash	074046155d051028z2e32tz27z
Authentihash	404e78bf44e0dc2af6c12b07c25db481c0d6ffe88aba1c171872c107253a1ffd
Imphash	481f47bbb2c9c21e108d65f52b04c448
Rich PE header hash	a7016ce5cb15a8644d2a00d0e692d936
SSDEEP	384:liEfQUjoa9PaTmvXAVDXaUHH06zfAdYRcWmU5q3:liE9oAwBXpCQq3
TLSH	T13C735C93C5E85C42F17B3B7C5ABA2E168C74BE386C74C65D2684251CCDE4690CF22BB6
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (37.8%) | Microsoft Visual C++ compiled executable (generic) (20%) | Win64 Executable (generic) (12.7%) | Win32 Dynamic Link Library (generic) (7.9%) | Win16 NE executable (generic) (6.1%)
DetectItEasy	PE32 | Linker: Microsoft Linker (6.0*) [GUI32]
File size	72.00 KB (73728 bytes)

History

Creation Time	2009-05-24 04:44:43 UTC
First Submission	2023-01-12 18:45:38 UTC
Last Submission	2023-01-12 18:45:38 UTC
Last Analysis	2023-01-12 18:45:38 UTC

Names

executable.2012.exe

ab.exe

48 / 71

?

Community Score

48 security vendors and 1 sandbox flagged this file as malicious

60d645236bcabd0f9754ae49ee8b73fd7349af9a960439981fd69124532e560a

ab.exe

peexe | idle

72.00 KB
Size

2023-01-12 18:45:38 UTC
2 hours ago

EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 4

Security vendors' analysis

AhnLab-V3	Trojan/Win32.Shell.R1283	ALYac	Trojan.CryptZ.Gen
Arcabit	Trojan.CryptZ.Gen	Avast	Win32:Meterpreter-C [Trj]
AVG	Win32:Meterpreter-C [Trj]	Avira (no cloud)	TR/Patched.Gen2
BitDefender	Trojan.CryptZ.Gen	BitDefenderTheta	Gen:NN.ZexaF.36212.eq0@ay8ZxSni
ClamAV	Win.Trojan.Swrort-5710536-0	Comodo	TrojWare.Win32.Rozena.A@4jwdqr
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cybereason	Malicious.20c013
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W32/Swrort.B	Elastic	Windows.Trojan.Metasploit
Emsisoft	Trojan.CryptZ.Gen (B)	eScan	Trojan.CryptZ.Gen

ESET-NOD32	A Variant Of Win32/Rozena.AA	F-Secure	Trojan.TR/Patched.Gen2
Fortinet	W32/Swrort.C!tr	GData	Win32.Trojan.PSE.12DT0MV
Google	Detected	Ikarus	Trojan.Win32.Swrort
K7AntiVirus	Trojan (005856601)	K7GW	Trojan (005856601)
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes	Trojan.Rozena
MAX	Malware (ai Score=84)	MaxSecure	Trojan.Malware.7164915.susgen
McAfee	Swrort.d	McAfee-GW-Edition	Swrort.d
Microsoft	Trojan:Win32/Meterpreter.O!MTB	NANO-Antivirus	Virus.Win32.Gen-Crypt.ccnc
Panda	Trj/Genetic.gen	QuickHeal	Trojan.Swrort.A
Rising	HackTool.Swrort!1.6477 (CLASSIC)	Sangfor Engine Zero	HackTool.Win32.Reverse_Bin_v2_5_thr...
SecureAge	Malicious	Sophos	ML/PE-A + Mal/EncPk-ACE
Symantec	Packed.Generic.347	Trellix (FireEye)	Generic.mg.32de42a20c013aa8
TrendMicro	Backdoor.Win32.SWRORT.SMAL01	TrendMicro-HouseCall	Backdoor.Win32.SWRORT.SMAL01
VIPRE	Trojan.CryptZ.Gen	Yandex	Trojan.Rosena.Gen.1
Zillya	Trojan.Rozena.Win32.170611	ZoneAlarm by Check Point	HEUR:Trojan.Win32.Generic

So, Now we know that the clickme.exe or PID 2012 is a malicious file and it is a trojan.

By checking the behavior section of virustotal of this trojan, I noticed that the attacker attacked by the 443 port or HTTPS.

60d645236bcabd0f9754ae49ee8b73fd7349af9a960439981fd69124532e560a

Activity Summary

System Information Discovery T1082
Reads software policies

Command and Control TA0011

Application Layer Protocol T1071
Uses HTTPS

Encrypted Channel T1573
Uses HTTPS for network communication, use the SSL MITM Proxy cookbook for further analysis
Uses HTTPS

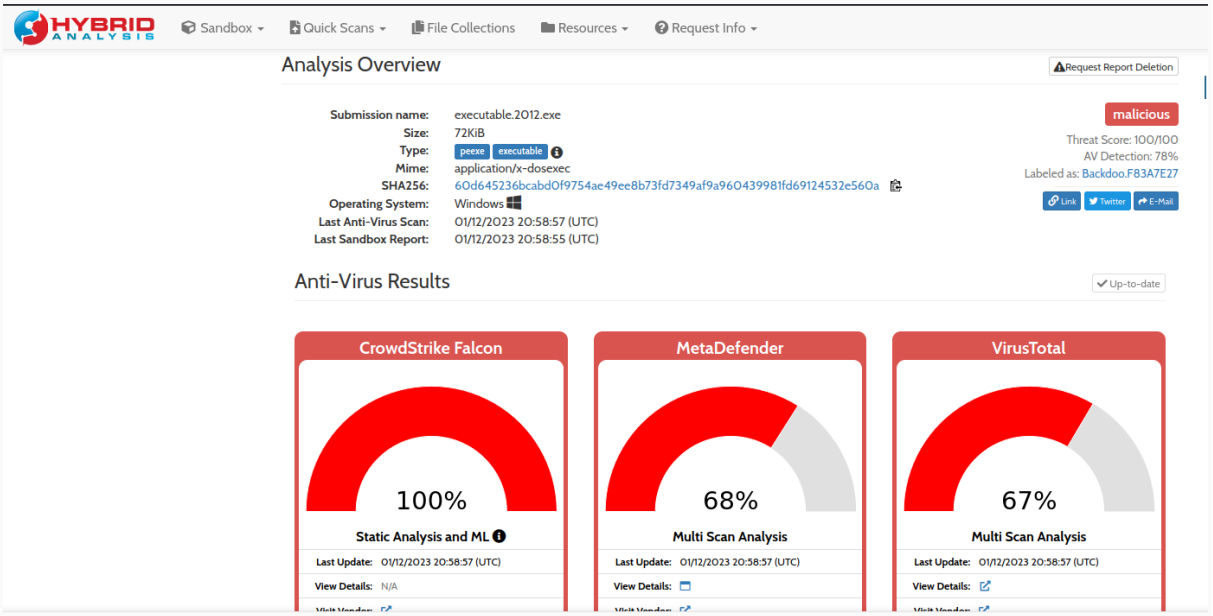
Network Communication

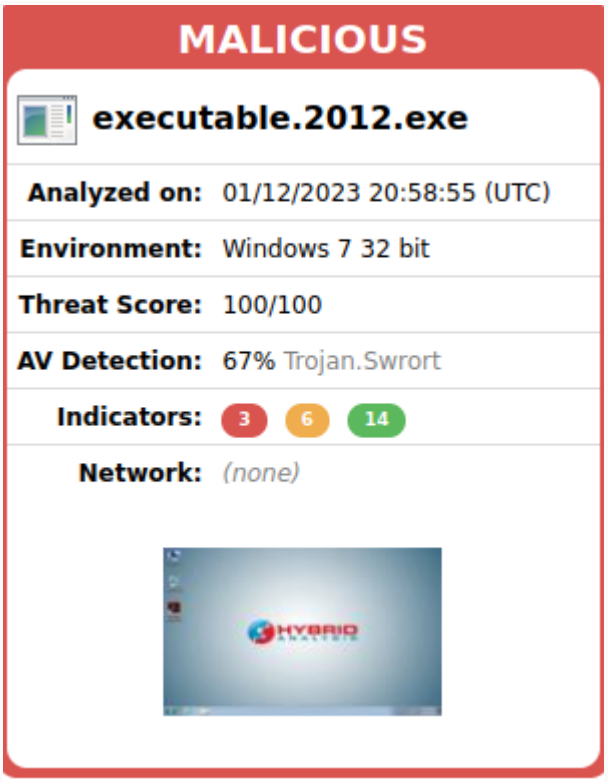
IP Traffic

192.168.56.101:443 (TCP)
20.99.184.37:443 (TCP)
23.216.147.76:443 (TCP)

File system actions

I also scan the file with Hybrid-analysis online tools. Where the file also scans as malicious. And the name of this malware is “Trojan.Swrort” or “Trojan Win32”. And this is a backdoor trojan. Which makes a remote connection to the attacker.





After checking the scripts of clickme.exe file by volatility, I can see that the file has read and write permission.

```
0xb8360039 0000              ADD [EAX], AL
0xb836003b 0000              ADD [EAX], AL
0xb836003d 0000              ADD [EAX], AL
0xb836003f 00                DB 0x0

Process: clickme.exe Pid: 2012 Address: 0x30000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: PrivateMemory: 1, Protection: 6

0x00030000  fc e8 8f 00 00 00 60 31 d2 64 8b 52 30 8b 52 0c   ......`1.d.R0.R.
0x00030010  8b 52 14 89 e5 31 ff 8b 72 28 0f b7 4a 26 31 c0   .R...1..r(..J&1.
0x00030020  ac 3c 61 7c 02 2c 20 c1 cf 0d 01 c7 49 75 ef 52   .<a|.,......Iu.R
0x00030030  57 8b 52 10 8b 42 3c 01 d0 8b 40 78 85 c0 74 4c   W.R..B<...@x..tL

0x00030000 fc                CLD
0x00030001 e88f000000        CALL 0x30095
0x00030006 60                PUSHA
0x00030007 31d2              XOR EDX, EDX
0x00030009 648b5230          MOV EDX, [FS:EDX+0x30]
0x0003000d 8b520c            MOV EDX, [EDX+0xc]
0x00030010 8b5214            MOV EDX, [EDX+0x14]
0x00030013 89e5              MOV EBP, ESP
0x00030015 31ff              XOR EDI, EDI
0x00030017 8b7228            MOV ESI, [EDX+0x28]
0x0003001a 0fb74a26          MOVZX ECX, WORD [EDX+0x26]
0x0003001e 31c0              XOR EAX, EAX
0x00030020 ac                LODSB
0x00030021 3c61              CMP AL, 0x61
0x00030023 7c02              JL 0x30027
0x00030025 2c20              SUB AL, 0x20
0x00030027 c1cf0d            ROR EDI, 0xd
0x0003002a 01c7              ADD EDI, EAX
0x0003002c 49                DEC ECX
0x0003002d 75ef              JNZ 0x3001e
0x0003002f 52                PUSH EDX
0x00030030 57                PUSH EDI
0x00030031 8b5210            MOV EDX, [EDX+0x10]
0x00030034 8b423c            MOV EAX, [EDX+0x3c]
0x00030037 01d0              ADD EAX, EDX
0x00030039 8b4078            MOV EAX, [EAX+0x78]
0x0003003c 85c0              TEST EAX, EAX
0x0003003e 744c              JZ 0x3008c

Process: clickme.exe Pid: 2012 Address: 0x430000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: PrivateMemory: 1, Protection: 6

0x00430000  4d 5a e8 00 00 00 00 5b 52 45 55 89 e5 81 c3 56   MZ.....[REU....V
0x00430010  45 00 00 ff d3 81 c3 a3 64 02 00 89 3b 53 6a 04   E.......d...;Sj.
0x00430020  50 ff d0 00 00 00 00 00 00 00 00 00 00 00 00 00   P...............
0x00430030  00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00   ................

0x00430000 4d                DEC EBP
0x00430001 5a                POP EDX
0x00430002 e800000000        CALL 0x430007
```

And I also find that a malicious connection was established which was happening for the execution of the trojan.

```
trinity@trinity-HP-Pavilion-Laptop-15-cc0xx:~/Documents/sajid$ volatility -f Memory.mem --profile=Win10x64_17134 netscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0xdb0e1ef4c1a0     UDPv4    0.0.0.0:5355                   *:*                                   1272     svchost.exe    2022-10-24 13:32:32 UTC+0000
0xdb0e1ef4c1a0     UDPv6    :::5355                        *:*                                   1272     svchost.exe    2022-10-24 13:32:32 UTC+0000
0xdb0e1ef4c6e0     UDPv4    0.0.0.0:53407                  *:*                                   1272     svchost.exe    2022-10-24 13:43:19 UTC+0000
0xdb0e1ef4c6e0     UDPv6    :::53407                       *:*                                   1272     svchost.exe    2022-10-24 13:43:19 UTC+0000
0xdb0e1ef4cc20     TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        780      svchost.exe    2022-10-24 13:32:30 UTC+0000
0xdb0e1ef4cc20     TCPv6    :::135                         :::0                 LISTENING        780      svchost.exe    2022-10-24 13:32:30 UTC+0000
0xdb0e1ef4d160     TCPv4    0.0.0.0:47001                  0.0.0.0:0            LISTENING        4        System         2022-10-24 13:34:40 UTC+0000
0xdb0e1ef4d160     TCPv6    :::47001                       :::0                 LISTENING        4        System         2022-10-24 13:34:40 UTC+0000
0xdb0e1ef4d7f0     TCPv4    0.0.0.0:49665                  0.0.0.0:0            LISTENING        1028     svchost.exe    2022-10-24 13:32:31 UTC+0000
0xdb0e1ef4d940     TCPv4    0.0.0.0:5985                   0.0.0.0:0            LISTENING        4        System         2022-10-24 13:34:40 UTC+0000
0xdb0e1ef4d940     TCPv6    :::5985                        :::0                 LISTENING        4        System         2022-10-24 13:34:40 UTC+0000
0xdb0e1ef4dd30     TCPv4    0.0.0.0:49665                  0.0.0.0:0            LISTENING        1028     svchost.exe    2022-10-24 13:32:31 UTC+0000
0xdb0e1ef4dd30     TCPv6    :::49665                       :::0                 LISTENING        1028     svchost.exe    2022-10-24 13:32:31 UTC+0000
0xdb0e219f95a0     UDPv4    0.0.0.0:3702                   *:*                                   1872     svchost.exe    2022-10-24 13:41:53 UTC+0000
0xdb0e219f95a0     UDPv6    :::3702                        *:*                                   1872     svchost.exe    2022-10-24 13:41:53 UTC+0000
0xdb0e219f9060     TCPv4    0.0.0.0:7680                   0.0.0.0:0            LISTENING        2476     svchost.exe    2022-10-24 13:34:30 UTC+0000
0xdb0e219f9060     TCPv6    :::7680                        :::0                 LISTENING        2476     svchost.exe    2022-10-24 13:34:30 UTC+0000
0xdb0e210219e0     TCPv4    10.0.2.15:49800                23.48.165.149:443    ESTABLISHED      -1                      3884-06-03 12:01:31 UTC+0000
0xdb0e216dd110     TCPv4    10.0.2.15:49731                144.2.9.1:443        ESTABLISHED      -1                      3884-06-03 12:01:31 UTC+0000
0xdb0e223d69a0     TCPv4    10.0.2.15:49788                178.249.97.70:443    ESTABLISHED      -1                      3884-06-03 12:01:31 UTC+0000
0xdb0e22ad8830     UDPv4    0.0.0.0:3702                   *:*                                   2268     dasHost.exe    2022-10-24 13:32:38 UTC+0000
0xdb0e22ad9e80     UDPv6    fe80::c50d:519f:96a4:e108:1900 *:*                                   2676     svchost.exe    2022-10-24 13:32:37 UTC+0000
0xdb0e22ad0c00     TCPv4    10.0.2.15:49816                204.79.197.222:443   ESTABLISHED      -1                      3884-06-03 12:01:29 UTC+0000
0xdb0e25035050     TCPv4    10.0.2.15:49727                144.2.15.25:443      CLOSE_WAIT       -1                      3884-06-03 12:01:31 UTC+0000
0xdb0e2a0b3270     TCPv4    10.0.2.15:49775                178.249.97.23:443    ESTABLISHED      -1                      3884-06-03 12:01:31 UTC+0000
0xdb0e2b3edbf0     TCPv4    10.0.2.15:49684                172.217.169.67:443   ESTABLISHED      -1                      3884-06-03 12:01:31 UTC+0000
0xdb0e30bbcbf0     TCPv4    10.0.2.15:49811                13.107.6.158:443     ESTABLISHED      -1                      3884-06-03 12:01:29 UTC+0000
0xdb0e3b5cbb00     TCPv4    10.0.2.15:49809                204.79.197.220:443   ESTABLISHED      -1                      3884-06-03 12:01:29 UTC+0000
0xdb0e3b5d9820     TCPv4    10.0.2.15:49690                216.58.212.195:443   ESTABLISHED      -1                      3884-06-03 12:01:31 UTC+0000
0xdb0e3b5ef400     UDPv4    0.0.0.0:5353                   *:*                                   1272     svchost.exe    2022-10-24 13:32:32 UTC+0000
0xdb0e3b5ef6a0     UDPv4    0.0.0.0:0                      *:*                                   1272     svchost.exe    2022-10-24 13:32:32 UTC+0000
0xdb0e3b5ef6a0     UDPv6    :::0                           *:*                                   1272     svchost.exe    2022-10-24 13:32:32 UTC+0000
0xdb0e3b5ee2f0     TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        780      svchost.exe    2022-10-24 13:32:30 UTC+0000
0xdb0e3b5ee440     TCPv4    0.0.0.0:49666                  0.0.0.0:0            LISTENING        820      svchost.exe    2022-10-24 13:32:31 UTC+0000
0xdb0e3b5eeec0     TCPv4    0.0.0.0:49666                  0.0.0.0:0            LISTENING        820      svchost.exe    2022-10-24 13:32:31 UTC+0000
0xdb0e3b5eeec0     TCPv6    :::49666                       :::0                 LISTENING        820      svchost.exe    2022-10-24 13:32:31 UTC+0000
0xdb0e3e935c20     UDPv4    0.0.0.0:3702                   *:*                                   1984     svchost.exe    2022-10-24 13:32:37 UTC+0000
0xdb0e3e9366a0     TCPv4    0.0.0.0:49667                  0.0.0.0:0            LISTENING        1260     spoolsv.exe    2022-10-24 13:32:33 UTC+0000
0xdb0e45849bb0     TCPv4    10.0.2.15:49784                104.18.70.113:443    ESTABLISHED      -1                      3884-06-03 12:01:31 UTC+0000
0xdb0e49b20830     TCPv4    10.0.2.15:49680                20.190.159.64:443    CLOSED           -1                      3884-06-03 12:01:29 UTC+0000
0xf8077519a400     UDPv4    0.0.0.0:5353                   *:*                                   1272     svchost.exe    2022-10-24 13:32:32 UTC+0000
0xf8077519a6a0     UDPv4    0.0.0.0:0                      *:*                                   1272     svchost.exe    2022-10-24 13:32:32 UTC+0000
0xf8077519a6a0     UDPv6    :::0                           *:*                                   1272     svchost.exe    2022-10-24 13:32:32 UTC+0000
0xf80775199 2f0    TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        780      svchost.exe    2022-10-24 13:32:30 UTC+0000
0xf80775199440     TCPv4    0.0.0.0:49666                  0.0.0.0:0            LISTENING        820      svchost.exe    2022-10-24 13:32:31 UTC+0000
0xf80775199ec0     TCPv4    0.0.0.0:49666                  0.0.0.0:0            LISTENING        820      svchost.exe    2022-10-24 13:32:31 UTC+0000
0xf80775199ec0     TCPv6    :::49666                       :::0                 LISTENING        820      svchost.exe    2022-10-24 13:32:31 UTC+0000
```

Here I can also notice that the foreign IP establishes a connection with the local machine.

So the attacker attacked the victim's machine with “clickme.exe” or PID 2012 and which is a trojan.

We know that Trojan.Swrort or Trojan Win32 is a very harmful Trojan. For stopping this trojan, there have a lot of ways. Such as:

- Go to PowerShell and kill Process 2012.
- Remove the clickme.exe from the registry.
- Install Malwarebytes for permanent protection from Trojans.