Unknown.exe

Larry Schlack

Monday, March 14, 2022 12:34 PM

Basic Static Analysis

File type	64 bit exe, GUI subsystem	Written in NIM

Hash Values

Md5	B9497FFB7E9C6F49823B95851EC874E3
Sha1	6C8F50040545D8CD9AF4B51564DE654266E592E3
Sha256	3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E

Virus Total	13 of 64 found malicious (sample ID's)
Kaspersky	Backdoor.Win32.PMax.auos
Fortinet	Malicious_Behavior.SB
Alibaba	Backdoor:Win32/Meterpreter.09eb9990

Indicators - PE Studio

The file references string(s),	type: blacklist, count: 37,1
The file contains another file,	signature: unknown, location: overlay, offset: 0x0006EA00, size: 106379,1
The file references functions(s),	type: blacklist, count: 7,1
The file contains a virtualized section	,section: .bss,2
The count of section(s) is suspicious,	count: 18,2

Functions - PE Studio - X indicates Blocklisted

GetCurrentProcessId	,x,	kernel32.dll
GetCurrentThreadId	,x,	kernel32.dll
RtlAddFunctionTable	,x,	kernel32.dll
RtlLookupFunctionEntry	,x,	kernel32.dll
TerminateProcess	,x,	kernel32.dll
VirtualProtect	,x,	kernel32.dll
Getenv	,x,	msvcrt.dll

Strings - PE Studio 37 blocklisted

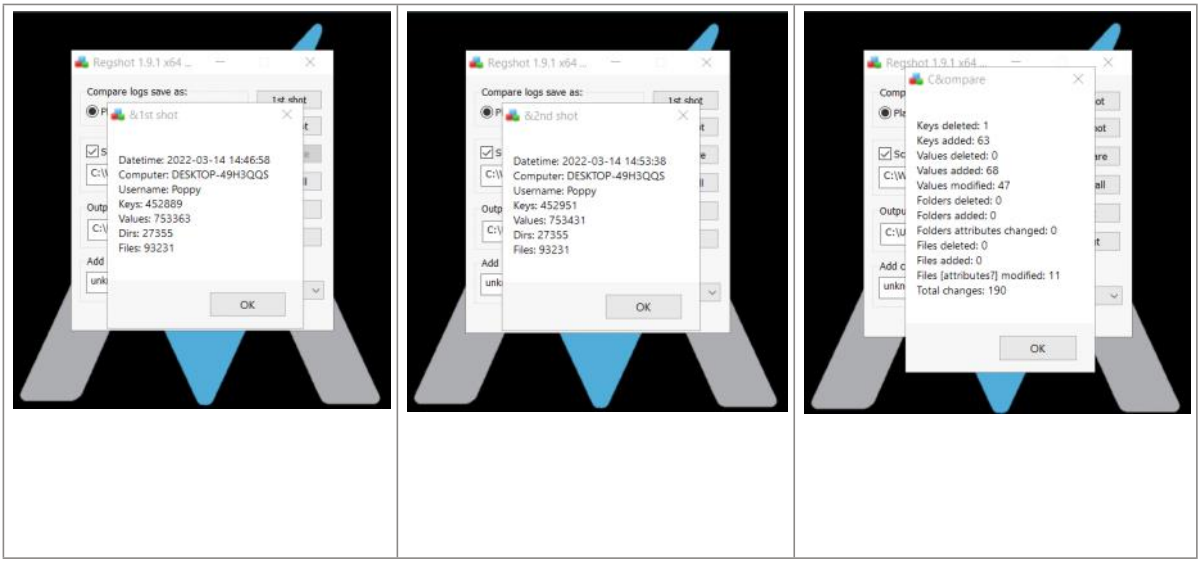
Size, Location Value

7,0x0001A0E5	utility,connect
4,0x0001A106	utility,send

6,0x0001A10B	utility,select
10,0x0001A06A	WSAStartup
6,0x0001A09B	socket
11,0x0001A0A2	closesocket
8,0x0001A0AE	WSAIoctl
11,0x0001A0CC	getaddrinfo
0x0001A0D8	freeaddrinfo
13,0x0001A0ED	FindFirstFile
12,0x0001A112	__WSAFDIsSet
4,0x0001A11F	recv
12,0x0001A480	InternetOpen
15,0x0001A48E	InternetOpenUrl
19,0x0001A49F	InternetCloseHandle
25,0x0001A85E	QueryPerformanceFrequency
6,0x0001B0EC	socket
19,0x00020FC6	GetCurrentProcessId
18,0x00020FDC	GetCurrentThreadId
19,0x000210AE	RtlAddFunctionTable
22,0x000210D8	,RtlLookupFunctionEntry
16,0x0002112C	TerminateProcess
14,0x00021188	VirtualProtect
6,0x00021356	getenv
19,0x0006A78D	GetCurrentProcessId
16,0x0006A7F9	TerminateProcess
22,0x0006A80A	RtlLookupFunctionEntry
18,0x0006A821	GetCurrentThreadId
14,0x0006A901	VirtualProtect
19,0x0006A9E2	RtlAddFunctionTable
6,0x0007C170	getenv
19,0x00085D95	GetCurrentProcessId
16,0x00085E18	TerminateProcess
,22,0x00085ECF	RtlLookupFunctionEntry
14,0x0008608F	VirtualProtect
19,0x00086BF4	RtlAddFunctionTable
18,0x000881FF	GetCurrentThreadId

Basic Dynamic Analysis

Regshot Results



Keys Deleted	1
Keys Added	63
Values Added	68
Values Modified	47
Files/(Attrib) Modified	11

Sample Values Added

HKU\S-1-5-21-4083756768-584771330-1588837462-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000020030C\VirtualDesktop: 10 00 00 00 30 30 44 56 22 1A 67 40 BA 3F 0A 44 AE 37 A5 45 5E 46 58 AA

HKU\S-1-5-21-4083756768-584771330-1588837462-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\55\Shell\SniffedFolderType: "Generic"

HKU\S-1-5-21-4083756768-584771330-1588837462-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\55\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByKey:FMTID: "{00000000-0000-0000-0000-000000000000}"

HKU\S-1-5-21-4083756768-584771330-1588837462-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\55\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByKey:PID: 0x00000000

HKU\S-1-5-21-4083756768-584771330-1588837462-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\55\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByDirection: 0x00000001

HKU\S-1-5-21-4083756768-584771330-1588837462-1001_Classes\Local Settings

\Software\Microsoft\Windows\Shell\Bags\55\Shell\SniffedFolderType: "Generic"

Sample Values Modified

HKU\S-1-5-21-4083756768-584771330-1588837462-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count\HRZR_PGYFRFFVBA:

HKU\S-1-5-21-4083756768-584771330-1588837462-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\CebtenzQngn\pubpbyngrl\yvo\ertfubg.syner\gbbyf\Ertfubg-k64-Havpbqr.rkr: 00 00 00 00 01 00 00 00 02 00 00 00 72 01 01 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 90 CB 4D FA E6 36 D8 01 00 00 00 00

HKU\S-1-5-21-4083756768-584771330-1588837462-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\CebtenzQngn\pubpbyngrl\yvo\ertfubg.syner\gbbyf\Ertfubg-k64-Havpbqr.rkr: 00 00 00 00 01 00 00 00 04 00 00 00 D2 B8 03 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 90 CB 4D FA E6 36 D8 01 00 00 00 00

HKU\S-1-5-21-4083756768-584771330-1588837462-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count\HRZR_PGYFRFFVBA:

Sample File / File Attributes Modified

C:\Windows\Logs\CBS\CBS.log
2022-03-14 14:46:48, 0x00000820, 11977577
2022-03-14 14:48:53, 0x00000820, 12166307

C:\Windows\Prefetch\DLLHOST.EXE-5E46FA0D.pf
2022-03-14 14:45:37, 0x00002020, 4044
2022-03-14 14:48:45, 0x00002020, 4040

C:\Windows\Prefetch\SEARCHAPP.EXE-0651CA85.pf
2022-03-03 19:55:41, 0x00002020, 37673
2022-03-14 14:53:05, 0x00002020, 39421

C:\Windows\ServiceState\EventLog\Data\lastalive0.dat
2022-03-14 14:47:43, 0x00000026, 2048
2022-03-14 14:53:43, 0x00000026, 2048

C:\Windows\ServiceState\EventLog\Data\lastalive1.dat
2022-03-14 14:46:43, 0x00000026, 2048
2022-03-14 14:52:43, 0x00000026, 2048

INetSim Log Information
Our first DNS request is to time.windows.com,
Second is to update.ec12-4-109-278-3-ubuntu20-04.local
Third (below) is to cdn.altimiter.local

2022-02-17 19:12:08 DNS connection, type: A, class: IN, requested name: time.windows.com

2022-02-17 19:14:46 DNS connection, type: A, class: IN, requested name: update.ec12-4-109-278-3-ubuntu20-04.local

2022-02-17 19:14:46 HTTP connection, method: GET, URL: http://update.ec12-4-109-278-3-ubuntu20-04.local/, file name: /var/lib/inetsim/http/fakefiles/sample.html

2022-02-17 19:14:47 DNS connection, type: A, class: IN, requested name: cdn.altimiter.local

2022-02-17 19:14:47 HTTP connection, method: GET, URL: http://cdn.altimiter.local/feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C4AC2A617437ECCBBA9, file name: /var/lib/inetsim/http/fakefiles/sample.html

2022-02-17 19:14:48 HTTP connection, method: GET, URL: http://cdn.altimiter.local/feed?post=B69A1CF6853645A440A0337BA0FB38291DE0B01A07FC129199658DDD4C1286BE45FEA8851D9BC6BC34220A6466D404C49A988BD6895AF291136076CCAFA9, file name: /var/lib/inetsim/http/fakefiles/sample.html

2022-02-17 19:14:49 HTTP connection, method: GET, URL: http://cdn.altimiter.local/feed?post=B69C1CF58536758272963755A8FB34291DEBB01907FC28919D7789E440128EBE45FDA88C199BC6BC08240E5C72D40CC49A9B8BC2895AC6B7666571CEBBA9, file name: /var/lib/inetsim/http/fakefiles/sample.html

2022-02-17 19:14:50 HTTP connection, method: GET, URL: http://cdn.altimiter.local/feed?post=A69C1CF68535758244B2337BAFFE38290DEBB01A07FF20919D758DDD480786BE49FDA8851998C6BC34020A6C57E504C48A9B8BD68959C6B7174302E29D84, file name: /var/lib/inetsim/http/fakefiles/sample.html

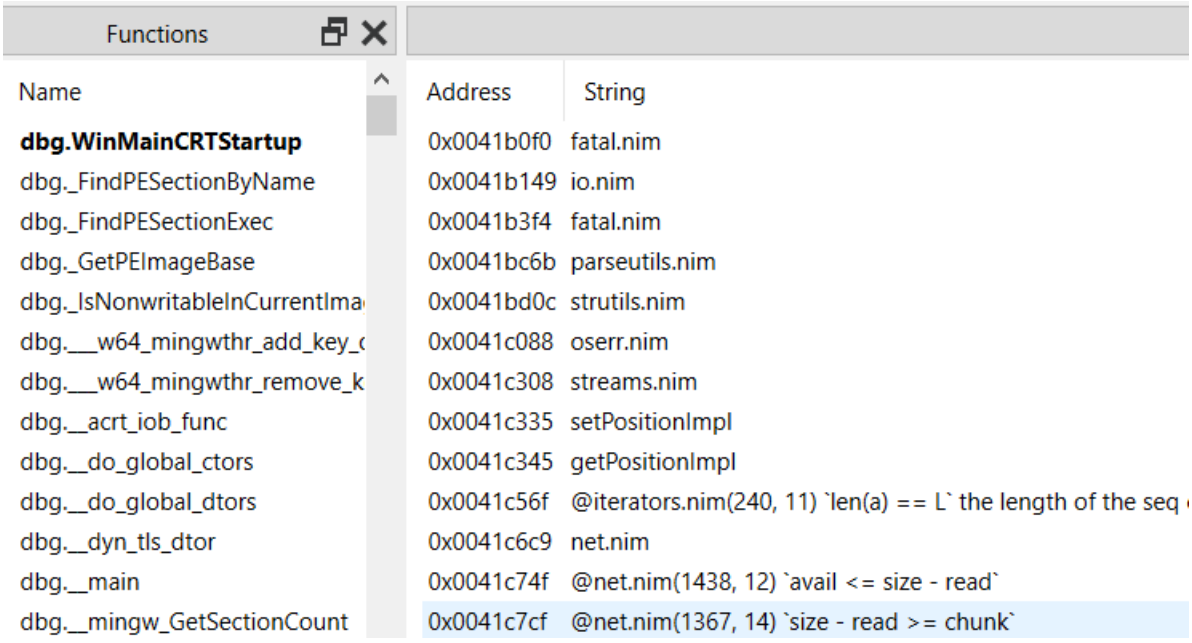
This process above repeated once per second This appears to be the exfiltration taking place as it is continuously repeating with a different string attached each time

Advanced Analysis

Strings from X64dbg (partial) Referencing NIM

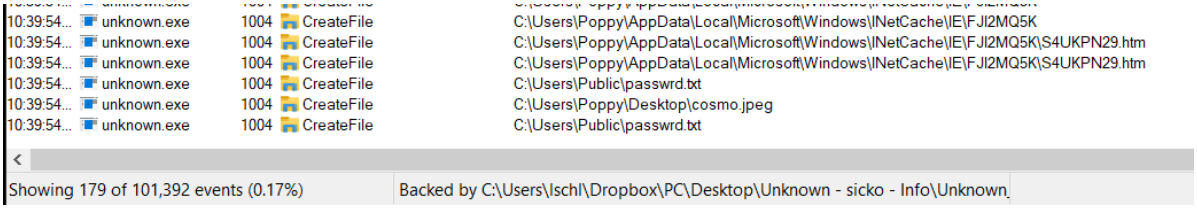
```
0000000000407F0E | lea r9,qword ptr ds:[41B3F4]          | "fatal.nim"
00000000004085CD | lea r9,qword ptr ds:[41BC6B]          | "parseutils.nim"
0000000000409056 | lea r9,qword ptr ds:[41BD0C]          | "strutils.nim"
000000000040B33C | lea r9,qword ptr ds:[41C088]          | "oserr.nim"
000000000040C3C6 | lea r9,qword ptr ds:[41C308]          | "streams.nim"
000000000040C7A9 | lea rcx,qword ptr ds:[41C335]         | "setPositionImpl"
000000000040C8B0 | lea rcx,qword ptr ds:[41C345]         | "getPositionImpl"
000000000040DFB2 | lea r9,qword ptr ds:[41C6C9]          | "net.nim"
000000000040E358 | lea r9,qword ptr ds:[41C6C9]          | "net.nim"
000000000040E465 | lea r9,qword ptr ds:[41C6C9]          | "net.nim"
0000000000411131 | lea r9,qword ptr ds:[41CC89]          | "tables.nim"
0000000000412BB4 | lea r9,qword ptr ds:[41CE91]          | "httpclient.nim"
0000000000412CAA | lea r9,qword ptr ds:[41CE91]          | "httpclient.nim"
0000000000413B88 | lea r9,qword ptr ds:[41CE91]          | "httpclient.nim"
```

Strings from Cutter (partial referencing NIM)



Functions		
Name	Address	String
dbg.WinMainCRTStartup	0x0041b0f0	fatal.nim
dbg._FindPESectionByName	0x0041b149	io.nim
dbg._FindPESectionExec	0x0041b3f4	fatal.nim
dbg._GetPEImageBase	0x0041bc6b	parseutils.nim
dbg._IsNonwritableInCurrentIma	0x0041bd0c	strutils.nim
dbg.__w64_mingwthr_add_key_(	0x0041c088	oserr.nim
dbg.__w64_mingwthr_remove_k	0x0041c308	streams.nim
dbg.__acrt_iob_func	0x0041c335	setPositionImpl
dbg.__do_global_ctors	0x0041c345	getPositionImpl
dbg.__do_global_dtors	0x0041c56f	@iterators.nim(240, 11) `len(a) == L` the length of the seq
dbg.__dyn_tls_dtor	0x0041c6c9	net.nim
dbg.__main	0x0041c74f	@net.nim(1438, 12) `avail <= size - read`
dbg.__mingw_GetSectionCount	0x0041c7cf	@net.nim(1367, 14) `size - read >= chunk`

Processes from ProcMon showing possible encryption key and target?



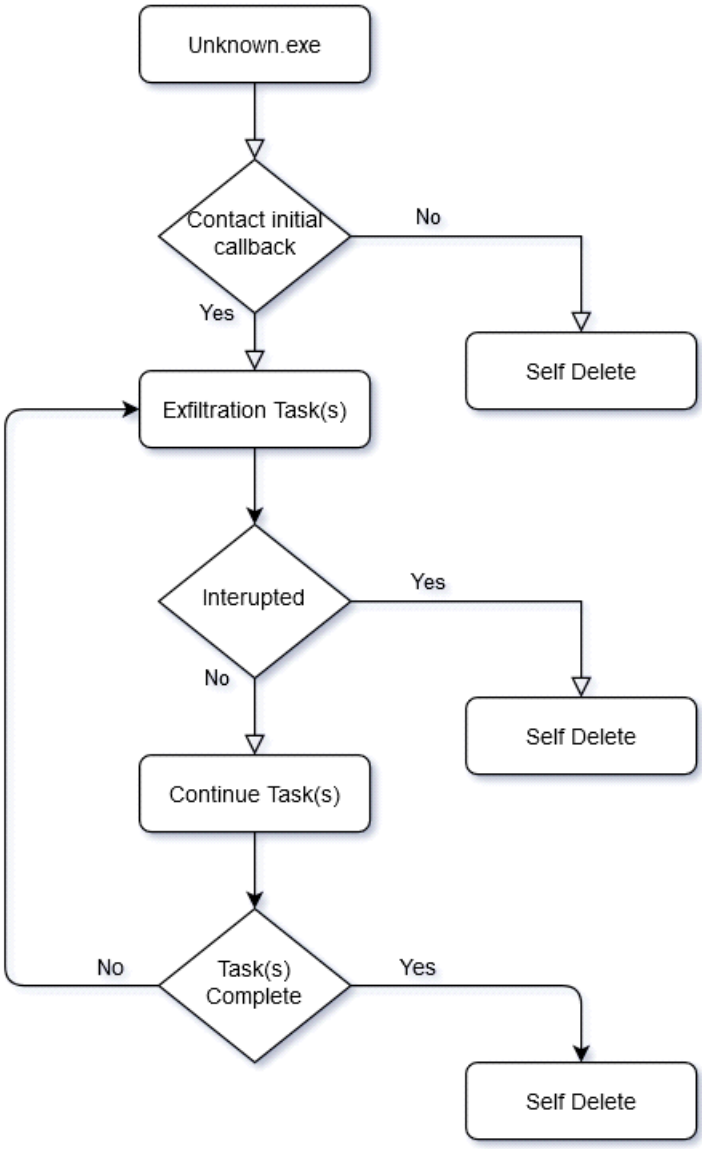
10:39:54...	unknown.exe	1004	CreateFile	C:\Users\Poppy\AppData\Local\Microsoft\Windows\INetCache\IE\FJI2MQ5K
10:39:54...	unknown.exe	1004	CreateFile	C:\Users\Poppy\AppData\Local\Microsoft\Windows\INetCache\IE\FJI2MQ5K\S4UKPN29.htm
10:39:54...	unknown.exe	1004	CreateFile	C:\Users\Poppy\AppData\Local\Microsoft\Windows\INetCache\IE\FJI2MQ5K\S4UKPN29.htm
10:39:54...	unknown.exe	1004	CreateFile	C:\Users\Public\passwrd.txt
10:39:54...	unknown.exe	1004	CreateFile	C:\Users\Poppy\Desktop\cosmo.jpeg
10:39:54...	unknown.exe	1004	CreateFile	C:\Users\Public\passwrd.txt

Showing 179 of 101,392 events (0.17%) | Backed by C:\Users\Ischl\Dropbox\PC\Desktop\Unknown - sicko - Info\Unknown

Additional references to encryption methodOperation: CreateFile from Thread 1068 (last item in screenshot above), C:\Users\Public\passwrd.txt

bcryptprimitives.dll 0x7ffd02d40000 0x83000 C:\Windows\System32\bcryptprimitives.dll
Microsoft Corporation 10.0.19041.1202 (WinBuild.160101.0800) 12/8/2012 10:40:38 PM

bcrypt.dll 0x7ffd02dd0000 0x27000 C:\Windows\System32\bcrypt.dll
Microsoft Corporation 10.0.19041.1 (WinBuild.160101.0800) 5/26/2020 5:18:52 AM


Unknown.exe
Contact initial callback
No
Yes
Self Delete
Exfiltration Task(s)
Interupted
Yes
No
Self Delete
Continue Task(s)
Task(s) Complete
No
Yes
Self Delete