Abloy Key Manager – Version 7.14301.0.0

March 7th, 2019.

Description: This is a review of Abloy Key Manager (version 7.14301.0.0). The software has suspicious files that can allow adversaries to launch attacks that can allow privilege escalation, load malicious files (hooking[1]), among others.

In this software three components were found compromised: KM7Setup.exe[2] sHJdnkvV.exe and ECOCIhtx.exe. These files were labeled as malicious. The main aspects explored included: the capacity to drop executable files, network weakness, and the elevation privilege[3] through weaknesses in the system security (SeChangeNotifyPrivilege).

The software open connections through Google and Amazon services, however one network connection seemed suspicious. The network analysis observed that multiple malicious artifacts were in transit through the software and those connections[4].

Another security risk is related to an expired certificate that prevents the validation of the software source[5].

[1] https://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf

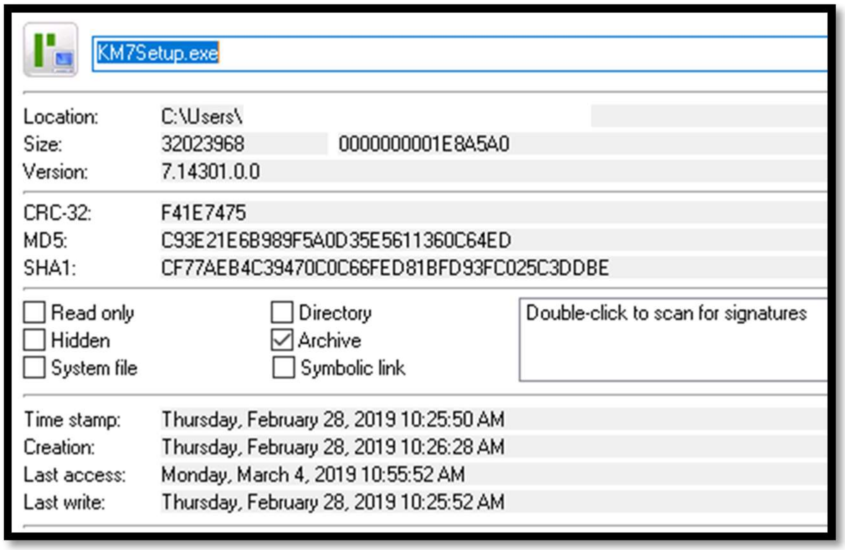
[2] https://www.virustotal.com/#/file/2c8d49b7ef16aec4c984664b87713b300d8a06bf82b8967499674397b1565029/details

[3] https://docs.microsoft.com/en-us/windows-hardware/drivers/ifs/elevation-of-privilege

[4] https://www.hybrid-analysis.com/sample/2c8d49b7ef16aec4c984664b87713b300d8a06bf82b8967499674397b1565029/5c7d416903883820949f1f1d

[5] https://comodosslstore.com/resources/how-to-avoid-code-signing-certificate-expired-issues/

File identification



KM7Setup.exe

Location: C:\Users\

Size: 32023968 0000000001E8A5A0

Version: 7.14301.0.0

CRC-32: F41E7475

MD5: C93E21E6B989F5A0D35E5611360C64ED

SHA1: CF77AEB4C39470C0C66FED81BFD93FC025C3DDBE

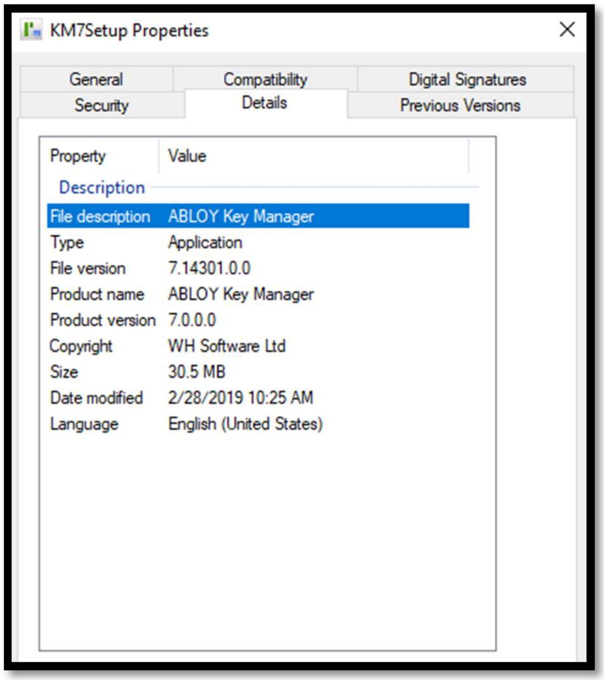
☐ Read only ☐ Directory Double-click to scan for signatures
☐ Hidden ☑ Archive
☐ System file ☐ Symbolic link

Time stamp: Thursday, February 28, 2019 10:25:50 AM

Creation: Thursday, February 28, 2019 10:26:28 AM

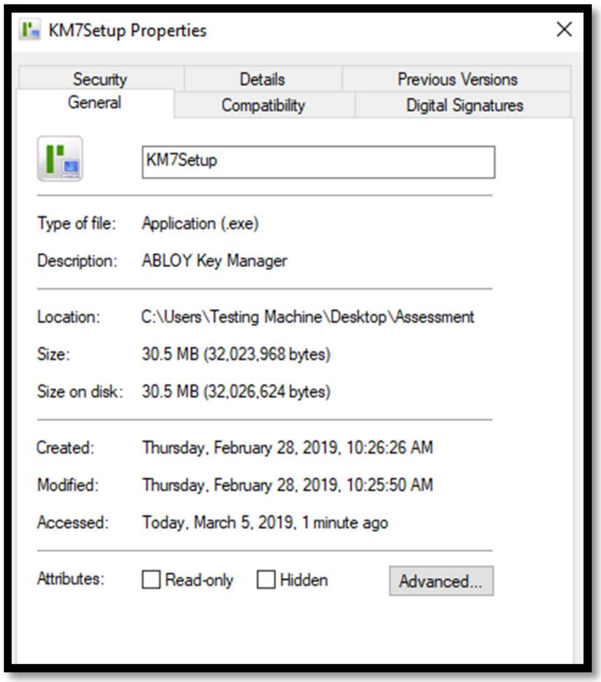
Last access: Monday, March 4, 2019 10:55:52 AM

Last write: Thursday, February 28, 2019 10:25:52 AM



KM7Setup Properties

Property	Value
Description	
File description	ABLOY Key Manager
Type	Application
File version	7.14301.0.0
Product name	ABLOY Key Manager
Product version	7.0.0.0
Copyright	WH Software Ltd
Size	30.5 MB
Date modified	2/28/2019 10:25 AM
Language	English (United States)



KM7Setup Properties

KM7Setup

Type of file: Application (.exe)

Description: ABLOY Key Manager

Location: C:\Users\Testing Machine\Desktop\Assessment

Size: 30.5 MB (32,023,968 bytes)

Size on disk: 30.5 MB (32,026,624 bytes)

Created: Thursday, February 28, 2019, 10:26:26 AM

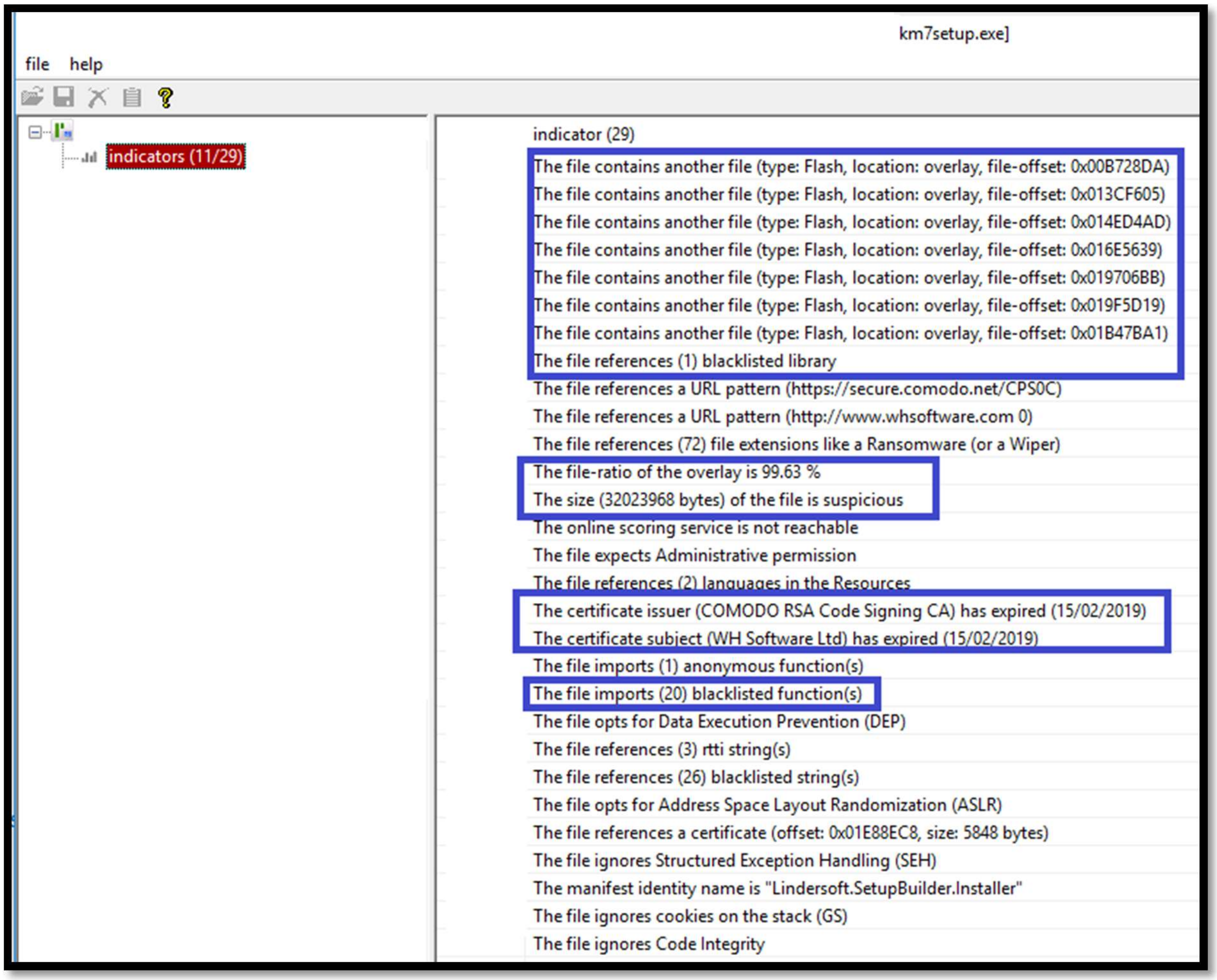
Modified: Thursday, February 28, 2019, 10:25:50 AM

Accessed: Today, March 5, 2019, 1 minute ago

Attributes: ☐ Read-only ☐ Hidden Advanced...

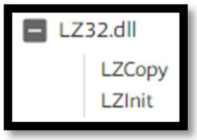
Initial security evaluation

First was identified some weakness such as the reference to another files compression (file-ratio), size, libraries and functions in use by the software.



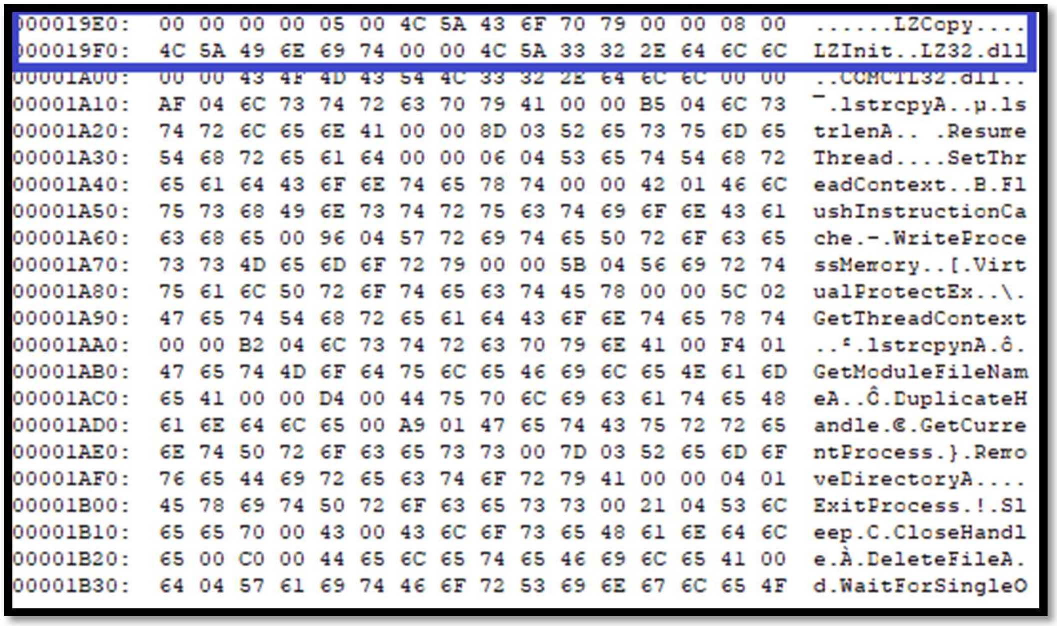
```
indicator (29)
The file contains another file (type: Flash, location: overlay, file-offset: 0x00B728DA)
The file contains another file (type: Flash, location: overlay, file-offset: 0x013CF605)
The file contains another file (type: Flash, location: overlay, file-offset: 0x014ED4AD)
The file contains another file (type: Flash, location: overlay, file-offset: 0x016E5639)
The file contains another file (type: Flash, location: overlay, file-offset: 0x019706BB)
The file contains another file (type: Flash, location: overlay, file-offset: 0x019F5D19)
The file contains another file (type: Flash, location: overlay, file-offset: 0x01B47BA1)
The file references (1) blacklisted library
The file references a URL pattern (https://secure.comodo.net/CPS0C)
The file references a URL pattern (http://www.whsoftware.com 0)
The file references (72) file extensions like a Ransomware (or a Wiper)
The file-ratio of the overlay is 99.63 %
The size (32023968 bytes) of the file is suspicious
The online scoring service is not reachable
The file expects Administrative permission
The file references (2) languages in the Resources
The certificate issuer (COMODO RSA Code Signing CA) has expired (15/02/2019)
The certificate subject (WH Software Ltd) has expired (15/02/2019)
The file imports (1) anonymous function(s)
The file imports (20) blacklisted function(s)
The file opts for Data Execution Prevention (DEP)
The file references (3) rtti string(s)
The file references (26) blacklisted string(s)
The file opts for Address Space Layout Randomization (ASLR)
The file references a certificate (offset: 0x01E88EC8, size: 5848 bytes)
The file ignores Structured Exception Handling (SEH)
The manifest identity name is "Lindersoft.SetupBuilder.Installer"
The file ignores cookies on the stack (GS)
The file ignores Code Integrity
```

Drop Files. The software relies in the use of a dynamic link library (*.dll) that could be used by malware for dropping compressed files (lz32.dll[6]) which bringing functions such as LZInit[7] and LZCopy[8] that allows decompressing, copying an initialize files.



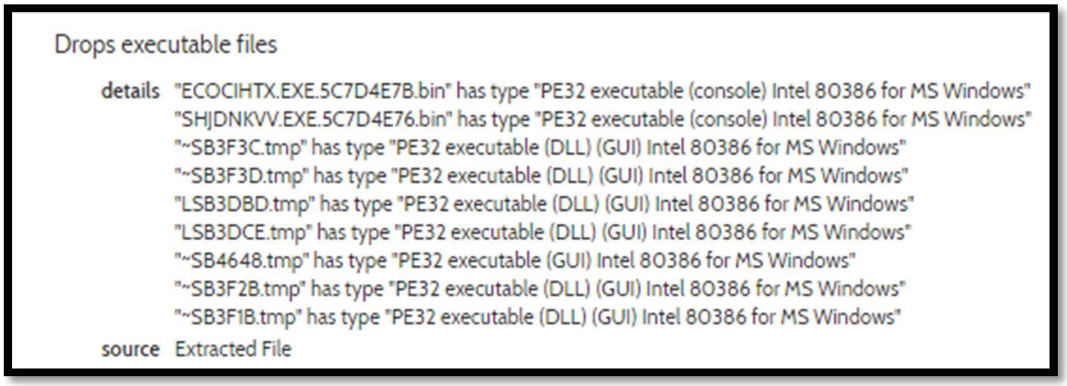
```
LZ32.dll
    LZCopy
    LZInit
```

[6] https://www.trendmicro.com/vinfo/us/threat-encyclopedia/search/lz32.dll
[7] https://docs.microsoft.com/en-us/windows/desktop/api/lzexpand/nf-lzexpand-lzinit
[8] https://docs.microsoft.com/en-us/windows/desktop/api/lzexpand/nf-lzexpand-lzcopy



```
000019E0:  00 00 00 00 05 00 4C 5A 43 6F 70 79 00 00 08 00  ......LZCopy....
000019F0:  4C 5A 49 6E 69 74 00 00 4C 5A 33 32 2E 64 6C 6C  LZInit..LZ32.dll
00001A00:  00 00 43 4F 4D 43 54 4C 33 32 2E 64 6C 6C 00 00  ..COMCTL32.dll..
00001A10:  AF 04 6C 73 74 72 63 70 79 41 00 00 B5 04 6C 73  ¯.lstrcpyA..µ.ls
00001A20:  74 72 6C 65 6E 41 00 00 8D 03 52 65 73 75 6D 65  trlenA.. .Resume
00001A30:  54 68 72 65 61 64 00 00 06 04 53 65 74 54 68 72  Thread....SetThr
00001A40:  65 61 64 43 6F 6E 74 65 78 74 00 00 42 01 46 6C  eadContext..B.Fl
00001A50:  75 73 68 49 6E 73 74 72 75 63 74 69 6F 6E 43 61  ushInstructionCa
00001A60:  63 68 65 00 96 04 57 72 69 74 65 50 72 6F 63 65  che.–.WriteProce
00001A70:  73 73 4D 65 6D 6F 72 79 00 00 5B 04 56 69 72 74  ssMemory..[.Virt
00001A80:  75 61 6C 50 72 6F 74 65 63 74 45 78 00 00 5C 02  ualProtectEx..\.
00001A90:  47 65 74 54 68 72 65 61 64 43 6F 6E 74 65 78 74  GetThreadContext
00001AA0:  00 00 B2 04 6C 73 74 72 63 70 79 6E 41 00 F4 01  ..².lstrcpynA.ô.
00001AB0:  47 65 74 4D 6F 64 75 6C 65 46 69 6C 65 4E 61 6D  GetModuleFileNam
00001AC0:  65 41 00 00 D4 00 44 75 70 6C 69 63 61 74 65 48  eA..Ô.DuplicateH
00001AD0:  61 6E 64 6C 65 00 A9 01 47 65 74 43 75 72 72 65  andle.©.GetCurre
00001AE0:  6E 74 50 72 6F 63 65 73 73 00 7D 03 52 65 6D 6F  ntProcess.}.Remo
00001AF0:  76 65 44 69 72 65 63 74 6F 72 79 41 00 00 04 01  veDirectoryA....
00001B00:  45 78 69 74 50 72 6F 63 65 73 73 00 21 04 53 6C  ExitProcess.!.Sl
00001B10:  65 65 70 00 43 00 43 6C 6F 73 65 48 61 6E 64 6C  eep.C.CloseHandl
00001B20:  65 00 C0 00 44 65 6C 65 74 65 46 69 6C 65 41 00  e.À.DeleteFileA.
00001B30:  64 04 57 61 69 74 46 6F 72 53 69 6E 67 6C 65 4F  d.WaitForSingleO
```

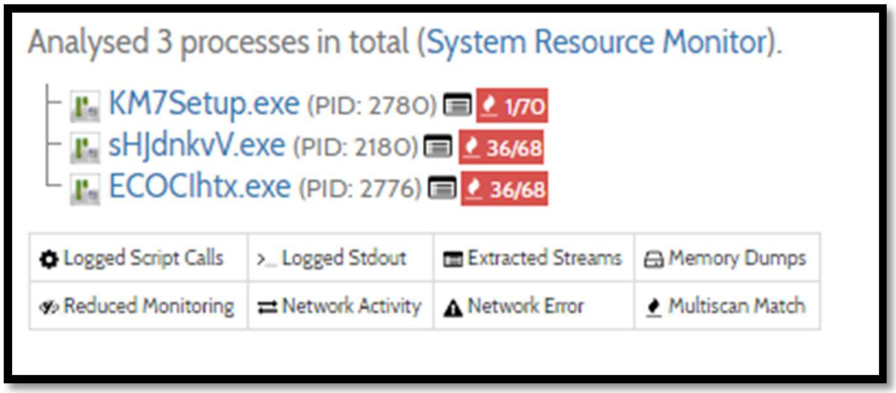
The software can drop malicious executable files:



Drops executable files

details "ECOCIHTX.EXE.5C7D4E7B.bin" has type "PE32 executable (console) Intel 80386 for MS Windows"
"SHJDNKVV.EXE.5C7D4E76.bin" has type "PE32 executable (console) Intel 80386 for MS Windows"
"~SB3F3C.tmp" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
"~SB3F3D.tmp" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
"LSB3DBD.tmp" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
"LSB3DCE.tmp" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
"~SB4648.tmp" has type "PE32 executable (GUI) Intel 80386 for MS Windows"
"~SB3F2B.tmp" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
"~SB3F1B.tmp" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"

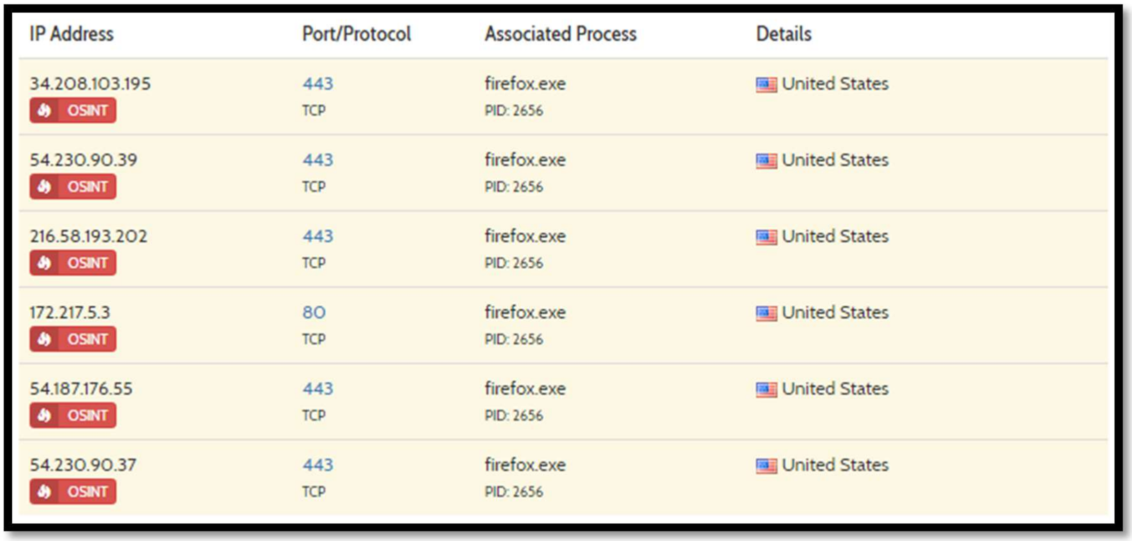
source Extracted File



Analysed 3 processes in total (System Resource Monitor).

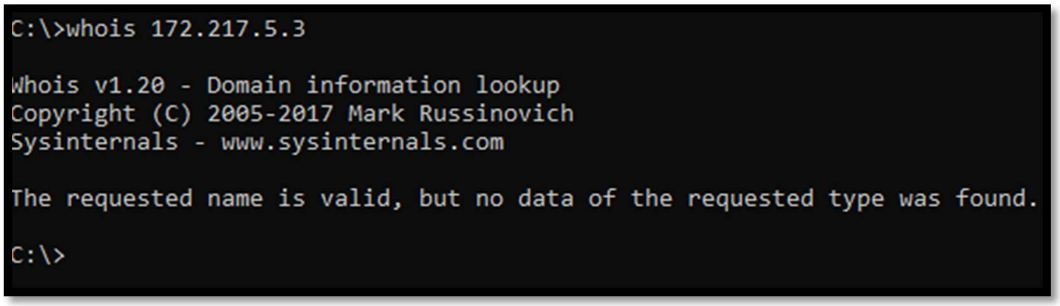
- KM7Setup.exe (PID: 2780) 1/70
- sHJdnkvV.exe (PID: 2180) 36/68
- ECOCIhtx.exe (PID: 2776) 36/68

Network. And establish network Connections:

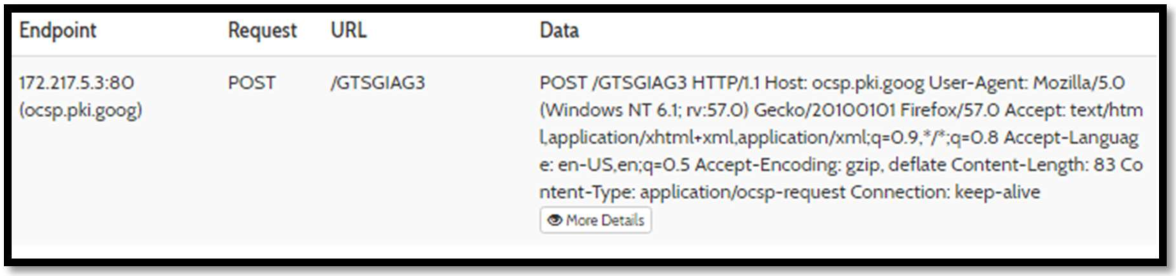


IP Address	Port/Protocol	Associated Process	Details
34.208.103.195 OSINT	443 TCP	firefox.exe PID: 2656	United States
54.230.90.39 OSINT	443 TCP	firefox.exe PID: 2656	United States
216.58.193.202 OSINT	443 TCP	firefox.exe PID: 2656	United States
172.217.5.3 OSINT	80 TCP	firefox.exe PID: 2656	United States
54.187.176.55 OSINT	443 TCP	firefox.exe PID: 2656	United States
54.230.90.37 OSINT	443 TCP	firefox.exe PID: 2656	United States

Some of these connections refer to Amazon and Google websites, but the IP address 172.217.5.3 is associated with the address at "ocsp.pki.goog[9]".



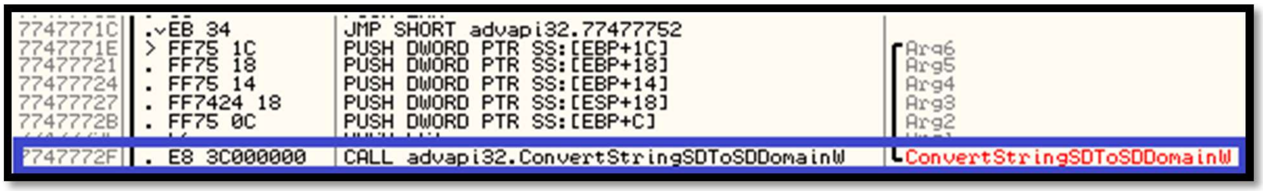
```
C:\>whois 172.217.5.3

Whois v1.20 - Domain information lookup
Copyright (C) 2005-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

The requested name is valid, but no data of the requested type was found.

C:\>
```



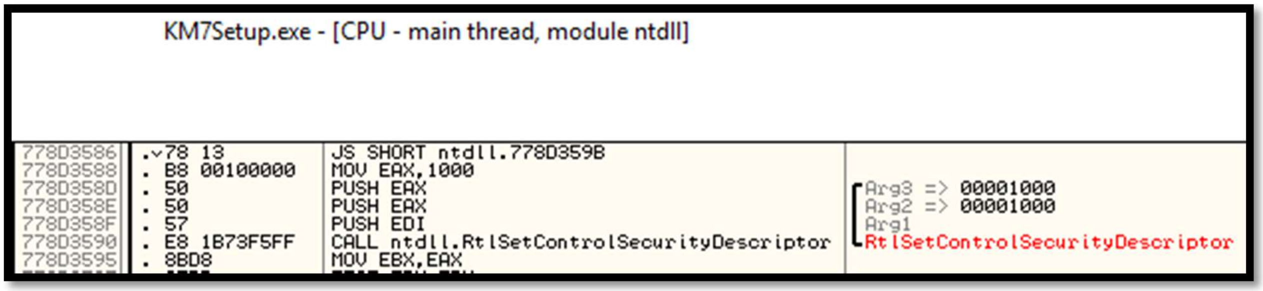
Endpoint	Request	URL	Data
172.217.5.3:80 (ocsp.pki.goog)	POST	/GTSGIAG3	POST /GTSGIAG3 HTTP/1.1 Host: ocsp.pki.goog User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:57.0) Gecko/20100101 Firefox/57.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Length: 83 Content-Type: application/ocsp-request Connection: keep-alive More Details

[9] https://www.malwares.com/report/host?host=ocsp.pki.goog

Security. Several functions were found related to the security[10] configuration that can be related to privilege[11] escalation in the advapi32.dll.

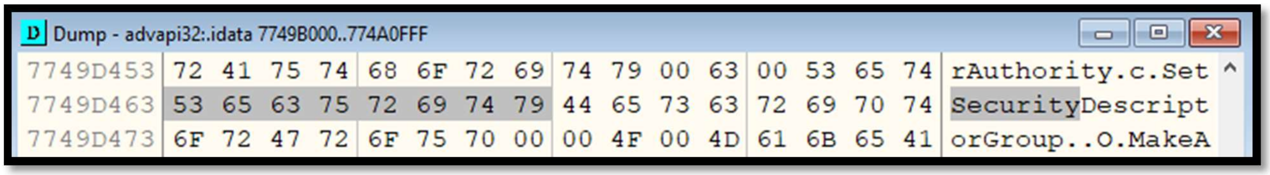


```
7747771C  .vEB 34          JMP SHORT advapi32.77477752
7747771E  > FF75 1C        PUSH DWORD PTR SS:[EBP+1C]                ┌Arg6
77477721  . FF75 18        PUSH DWORD PTR SS:[EBP+18]                │Arg5
77477724  . FF75 14        PUSH DWORD PTR SS:[EBP+14]                │Arg4
77477727  . FF7424 18      PUSH DWORD PTR SS:[ESP+18]                │Arg3
7747772B  . FF75 0C        PUSH DWORD PTR SS:[EBP+C]                 │Arg2
7747772F  . E8 3C000000    CALL advapi32.ConvertStringSDToSDDomainW  └ConvertStringSDToSDDomainW
```



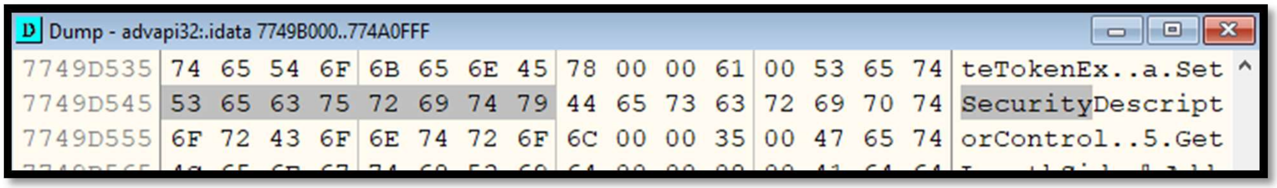
KM7Setup.exe - [CPU - main thread, module ntdll]

```
778D3586  .v78 13          JS SHORT ntdll.778D359B
778D3588  . B8 00100000    MOV EAX,1000
778D358D  . 50             PUSH EAX                                   ┌Arg3 => 00001000
778D358E  . 50             PUSH EAX                                   │Arg2 => 00001000
778D358F  . 57             PUSH EDI                                   │Arg1
778D3590  . E8 1B73F5FF    CALL ntdll.RtlSetControlSecurityDescriptor └RtlSetControlSecurityDescriptor
778D3595  . 8BD8           MOV EBX,EAX
```



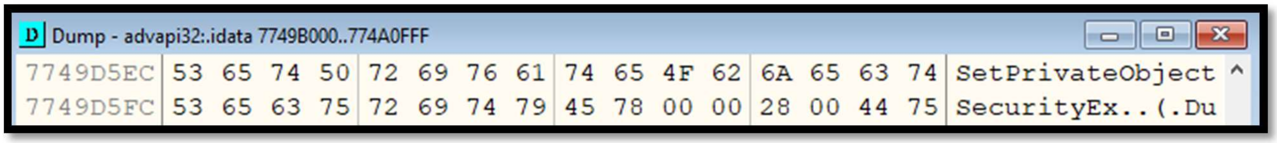
Dump - advapi32:.idata 7749B000..774A0FFF

```
7749D453 72 41 75 74 68 6F 72 69 74 79 00 63 00 53 65 74 rAuthority.c.Set
7749D463 53 65 63 75 72 69 74 79 44 65 73 63 72 69 70 74 SecurityDescript
7749D473 6F 72 47 72 6F 75 70 00 00 4F 00 4D 61 6B 65 41 orGroup..O.MakeA
```



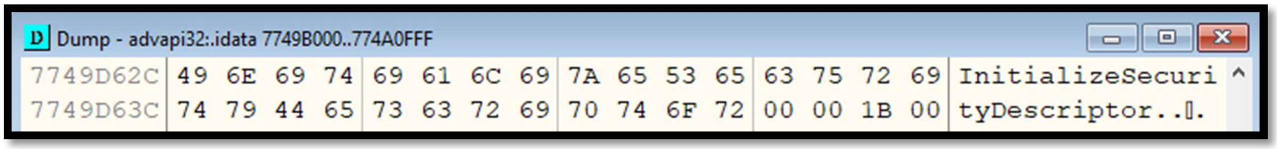
Dump - advapi32:.idata 7749B000..774A0FFF

```
7749D535 74 65 54 6F 6B 65 6E 45 78 00 00 61 00 53 65 74 teTokenEx..a.Set
7749D545 53 65 63 75 72 69 74 79 44 65 73 63 72 69 70 74 SecurityDescript
7749D555 6F 72 43 6F 6E 74 72 6F 6C 00 00 35 00 47 65 74 orControl..5.Get
```



Dump - advapi32:.idata 7749B000..774A0FFF

```
7749D5EC 53 65 74 50 72 69 76 61 74 65 4F 62 6A 65 63 74 SetPrivateObject
7749D5FC 53 65 63 75 72 69 74 79 45 78 00 00 28 00 44 75 SecurityEx..(.Du
```

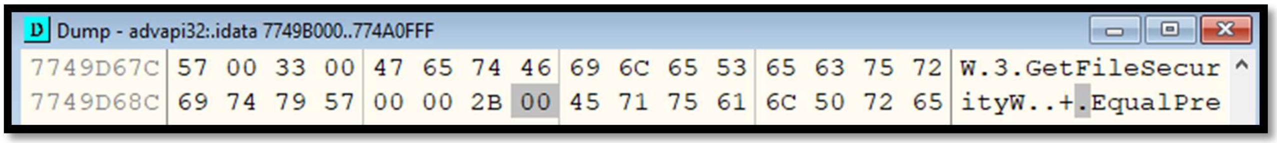


Dump - advapi32:.idata 7749B000..774A0FFF

```
7749D62C 49 6E 69 74 69 61 6C 69 7A 65 53 65 63 75 72 69 InitializeSecuri
7749D63C 74 79 44 65 73 63 72 69 70 74 6F 72 00 00 1B 00 tyDescriptor...
```

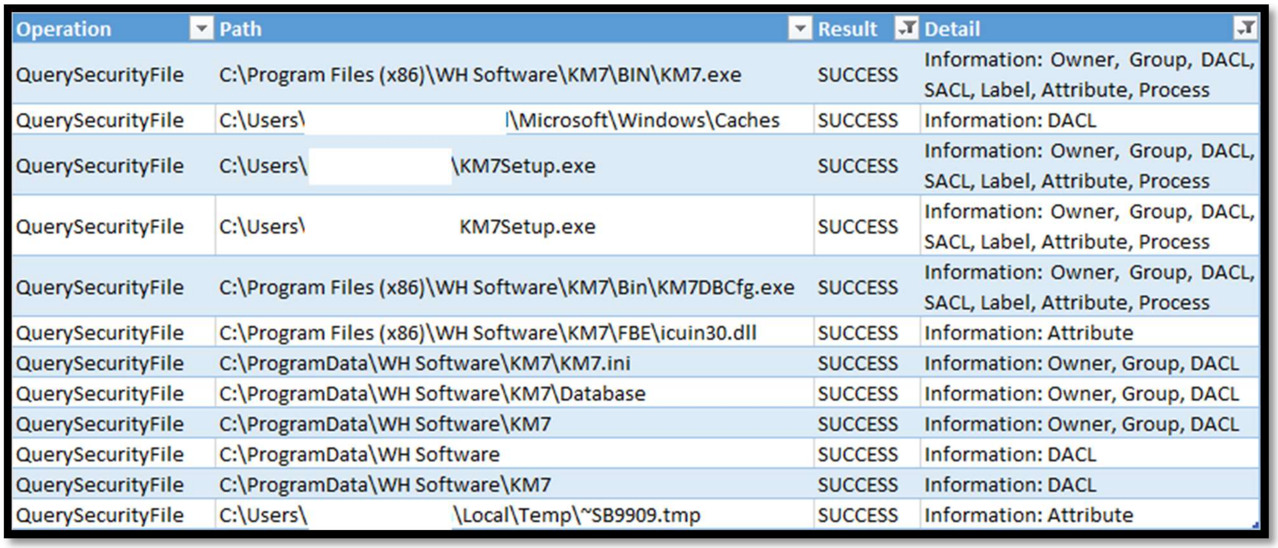
[10] https://docs.microsoft.com/en-us/previous-versions/windows/desktop/secrcw32prov/setsecuritydescriptor-method-in-class-win32-logicalfilesecuritysetting

[11] https://docs.microsoft.com/en-us/windows/desktop/WmiSdk/executing-privileged-operations

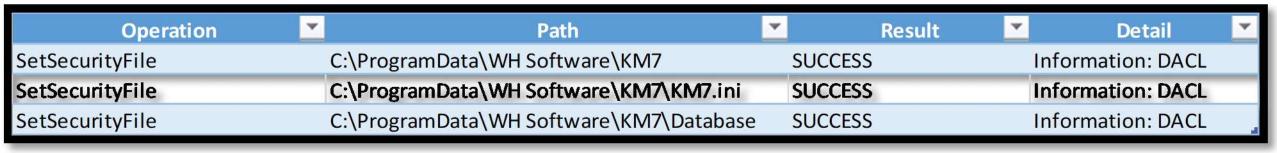


```
7749D67C 57 00 33 00 47 65 74 46 69 6C 65 53 65 63 75 72 W.3.GetFileSecur
7749D68C 69 74 79 57 00 00 2B 00 45 71 75 61 6C 50 72 65 ityW..+.EqualPre
```

Security operations launched by the software includes:

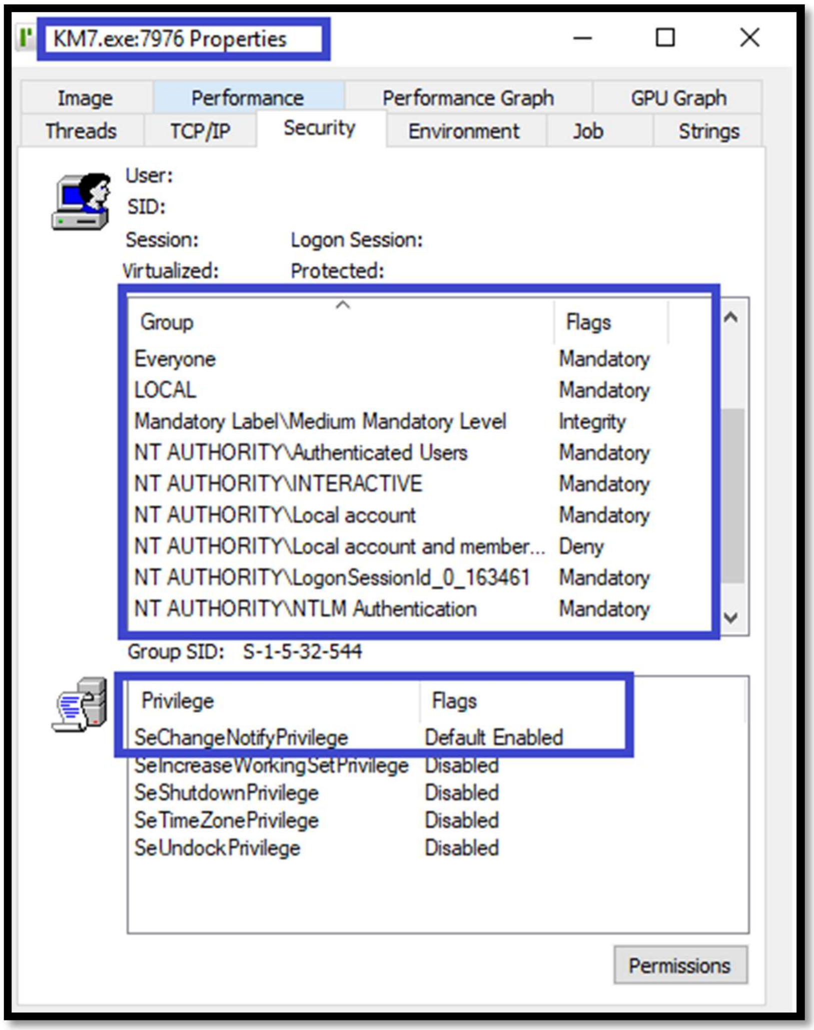


Operation	Path	Result	Detail
QuerySecurityFile	C:\Program Files (x86)\WH Software\KM7\BIN\KM7.exe	SUCCESS	Information: Owner, Group, DACL, SACL, Label, Attribute, Process
QuerySecurityFile	C:\Users\ l\Microsoft\Windows\Caches	SUCCESS	Information: DACL
QuerySecurityFile	C:\Users\ \KM7Setup.exe	SUCCESS	Information: Owner, Group, DACL, SACL, Label, Attribute, Process
QuerySecurityFile	C:\Users\ KM7Setup.exe	SUCCESS	Information: Owner, Group, DACL, SACL, Label, Attribute, Process
QuerySecurityFile	C:\Program Files (x86)\WH Software\KM7\Bin\KM7DBCfg.exe	SUCCESS	Information: Owner, Group, DACL, SACL, Label, Attribute, Process
QuerySecurityFile	C:\Program Files (x86)\WH Software\KM7\FBE\icuin30.dll	SUCCESS	Information: Attribute
QuerySecurityFile	C:\ProgramData\WH Software\KM7\KM7.ini	SUCCESS	Information: Owner, Group, DACL
QuerySecurityFile	C:\ProgramData\WH Software\KM7\Database	SUCCESS	Information: Owner, Group, DACL
QuerySecurityFile	C:\ProgramData\WH Software\KM7	SUCCESS	Information: Owner, Group, DACL
QuerySecurityFile	C:\ProgramData\WH Software	SUCCESS	Information: DACL
QuerySecurityFile	C:\ProgramData\WH Software\KM7	SUCCESS	Information: DACL
QuerySecurityFile	C:\Users\ \Local\Temp\~SB9909.tmp	SUCCESS	Information: Attribute



Operation	Path	Result	Detail
SetSecurityFile	C:\ProgramData\WH Software\KM7	SUCCESS	Information: DACL
SetSecurityFile	**C:\ProgramData\WH Software\KM7\KM7.ini**	**SUCCESS**	**Information: DACL**
SetSecurityFile	C:\ProgramData\WH Software\KM7\Database	SUCCESS	Information: DACL

SeChangeNotifyPrivilege[12]. This privilege controls whether users are allowed to bypass traverse checking.



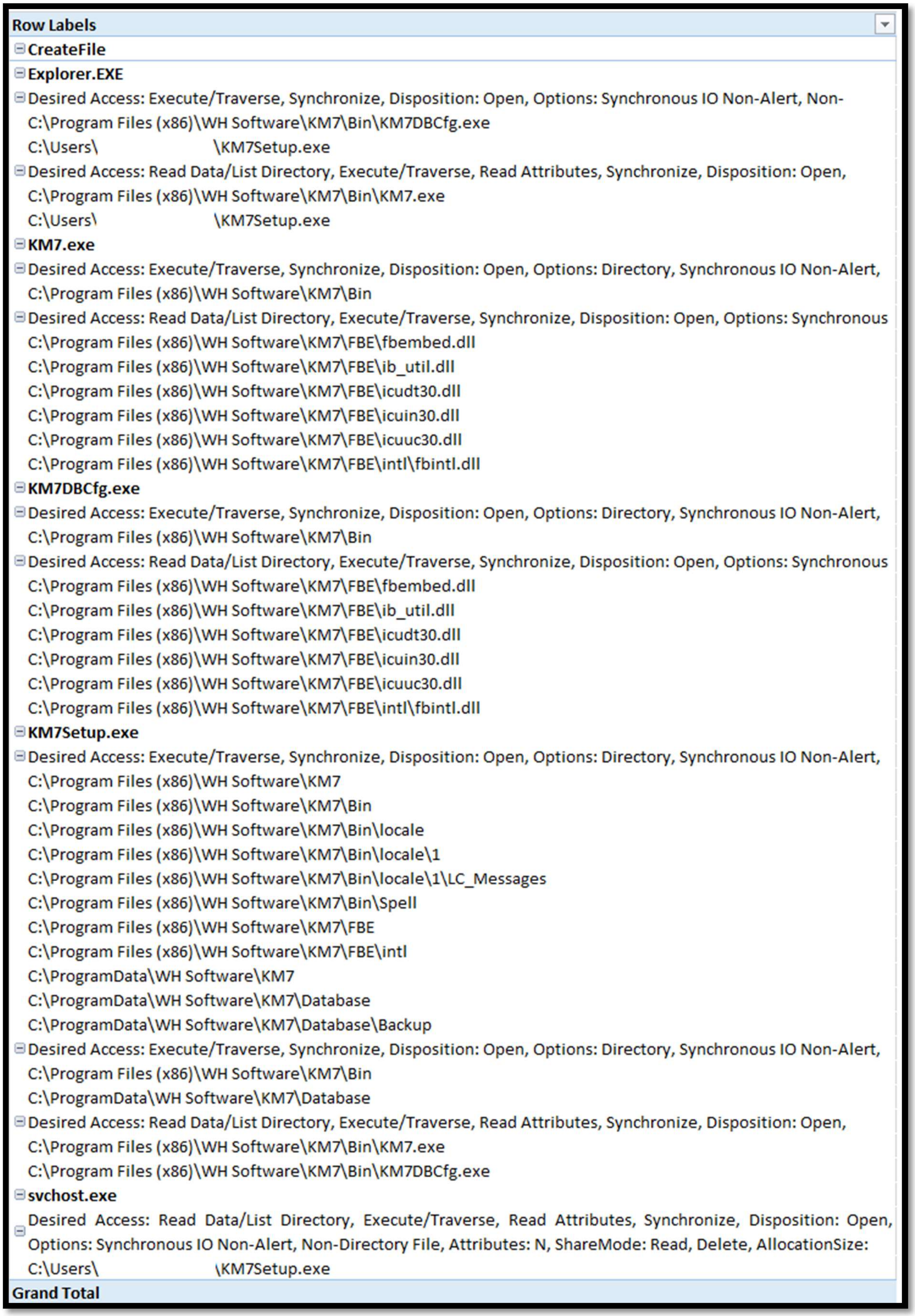
User:
SID:
Session: Logon Session:
Virtualized: Protected:

Group	Flags
Everyone	Mandatory
LOCAL	Mandatory
Mandatory Label\Medium Mandatory Level	Integrity
NT AUTHORITY\Authenticated Users	Mandatory
NT AUTHORITY\INTERACTIVE	Mandatory
NT AUTHORITY\Local account	Mandatory
NT AUTHORITY\Local account and member...	Deny
NT AUTHORITY\LogonSessionId_0_163461	Mandatory
NT AUTHORITY\NTLM Authentication	Mandatory

Group SID: S-1-5-32-544

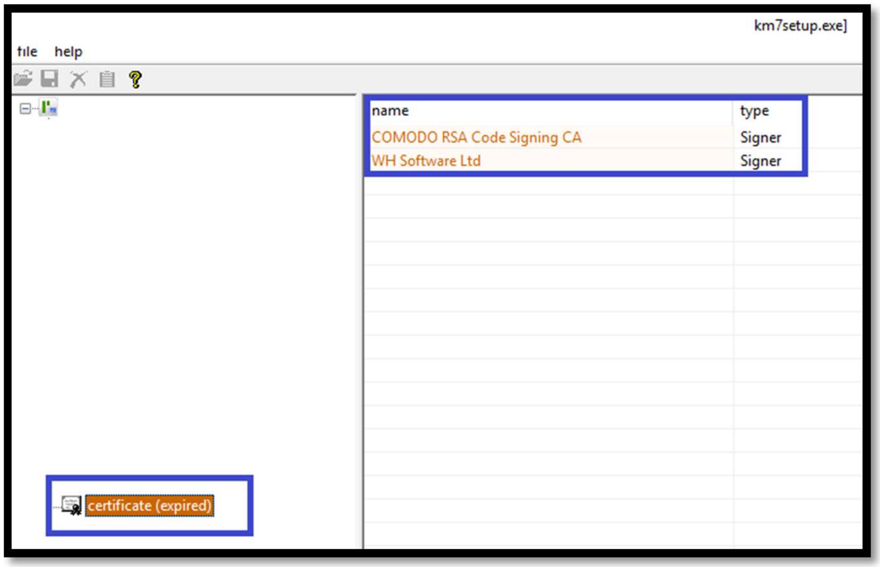
Privilege	Flags
SeChangeNotifyPrivilege	Default Enabled
SeIncreaseWorkingSetPrivilege	Disabled
SeShutdownPrivilege	Disabled
SeTimeZonePrivilege	Disabled
SeUndockPrivilege	Disabled

[12] https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.cdot-famg-cifs%2FGUID-B188F6D1-253B-49C5-925F-53488BF1A31B.html

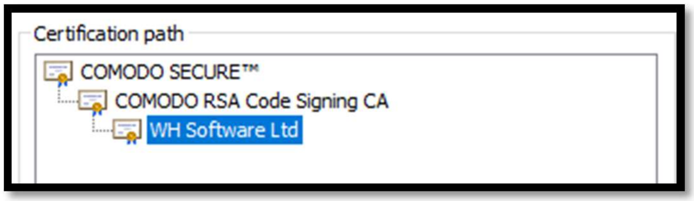


```
Row Labels
⊟CreateFile
⊟Explorer.EXE
⊟Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-
  C:\Program Files (x86)\WH Software\KM7\Bin\KM7DBCfg.exe
  C:\Users\                    \KM7Setup.exe
⊟Desired Access: Read Data/List Directory, Execute/Traverse, Read Attributes, Synchronize, Disposition: Open,
  C:\Program Files (x86)\WH Software\KM7\Bin\KM7.exe
  C:\Users\                    \KM7Setup.exe
⊟KM7.exe
⊟Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert,
  C:\Program Files (x86)\WH Software\KM7\Bin
⊟Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous
  C:\Program Files (x86)\WH Software\KM7\FBE\fbembed.dll
  C:\Program Files (x86)\WH Software\KM7\FBE\ib_util.dll
  C:\Program Files (x86)\WH Software\KM7\FBE\icudt30.dll
  C:\Program Files (x86)\WH Software\KM7\FBE\icuin30.dll
  C:\Program Files (x86)\WH Software\KM7\FBE\icuuc30.dll
  C:\Program Files (x86)\WH Software\KM7\FBE\intl\fbintl.dll
⊟KM7DBCfg.exe
⊟Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert,
  C:\Program Files (x86)\WH Software\KM7\Bin
⊟Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous
  C:\Program Files (x86)\WH Software\KM7\FBE\fbembed.dll
  C:\Program Files (x86)\WH Software\KM7\FBE\ib_util.dll
  C:\Program Files (x86)\WH Software\KM7\FBE\icudt30.dll
  C:\Program Files (x86)\WH Software\KM7\FBE\icuin30.dll
  C:\Program Files (x86)\WH Software\KM7\FBE\icuuc30.dll
  C:\Program Files (x86)\WH Software\KM7\FBE\intl\fbintl.dll
⊟KM7Setup.exe
⊟Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert,
  C:\Program Files (x86)\WH Software\KM7
  C:\Program Files (x86)\WH Software\KM7\Bin
  C:\Program Files (x86)\WH Software\KM7\Bin\locale
  C:\Program Files (x86)\WH Software\KM7\Bin\locale\1
  C:\Program Files (x86)\WH Software\KM7\Bin\locale\1\LC_Messages
  C:\Program Files (x86)\WH Software\KM7\Bin\Spell
  C:\Program Files (x86)\WH Software\KM7\FBE
  C:\Program Files (x86)\WH Software\KM7\FBE\intl
  C:\ProgramData\WH Software\KM7
  C:\ProgramData\WH Software\KM7\Database
  C:\ProgramData\WH Software\KM7\Database\Backup
⊟Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert,
  C:\Program Files (x86)\WH Software\KM7\Bin
  C:\ProgramData\WH Software\KM7\Database
⊟Desired Access: Read Data/List Directory, Execute/Traverse, Read Attributes, Synchronize, Disposition: Open,
  C:\Program Files (x86)\WH Software\KM7\Bin\KM7.exe
  C:\Program Files (x86)\WH Software\KM7\Bin\KM7DBCfg.exe
⊟svchost.exe
 Desired Access: Read Data/List Directory, Execute/Traverse, Read Attributes, Synchronize, Disposition: Open,
⊟Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, Delete, AllocationSize:
  C:\Users\                    \KM7Setup.exe
Grand Total
```

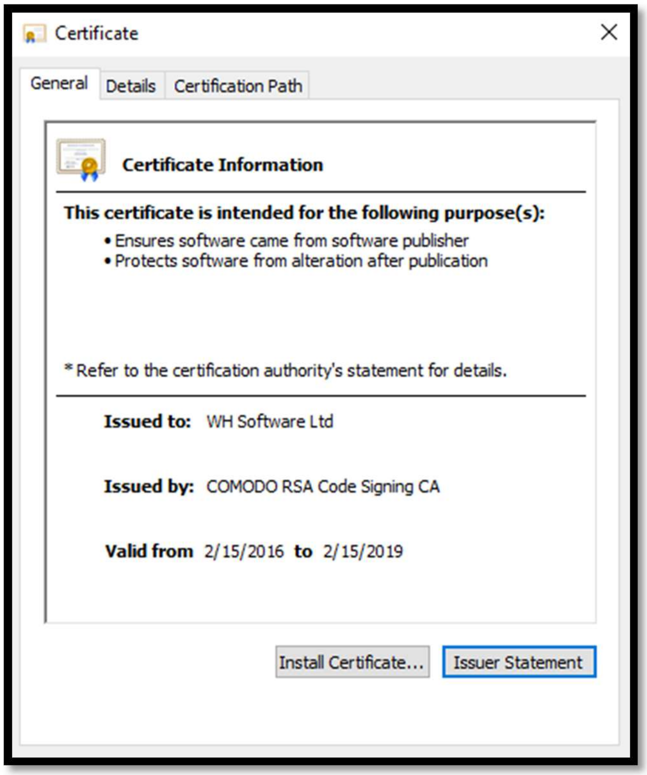
Certificate. The certificate is expired:



name	type
COMODO RSA Code Signing CA	Signer
WH Software Ltd	Signer


Certification path

COMODO SECURE™
COMODO RSA Code Signing CA
WH Software Ltd



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

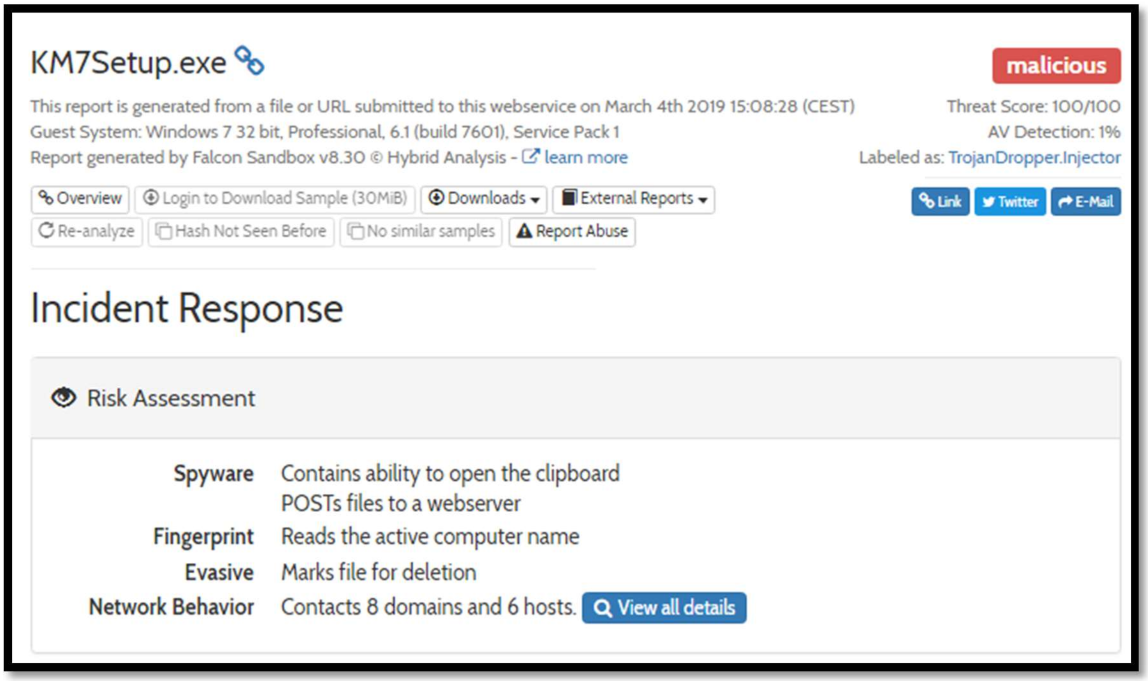
* Refer to the certification authority's statement for details.

Issued to: WH Software Ltd

Issued by: COMODO RSA Code Signing CA

Valid from 2/15/2016 **to** 2/15/2019

Behaviour Analysis. These are the results of the Anti-virus tools:



KM7Setup.exe

malicious

This report is generated from a file or URL submitted to this webservice on March 4th 2019 15:08:28 (CEST)
Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v8.30 © Hybrid Analysis - learn more

Threat Score: 100/100
AV Detection: 1%
Labeled as: TrojanDropper.Injector

Incident Response

Risk Assessment

Spyware	Contains ability to open the clipboard POSTs files to a webserver
Fingerprint	Reads the active computer name
Evasive	Marks file for deletion
Network Behavior	Contacts 8 domains and 6 hosts. View all details