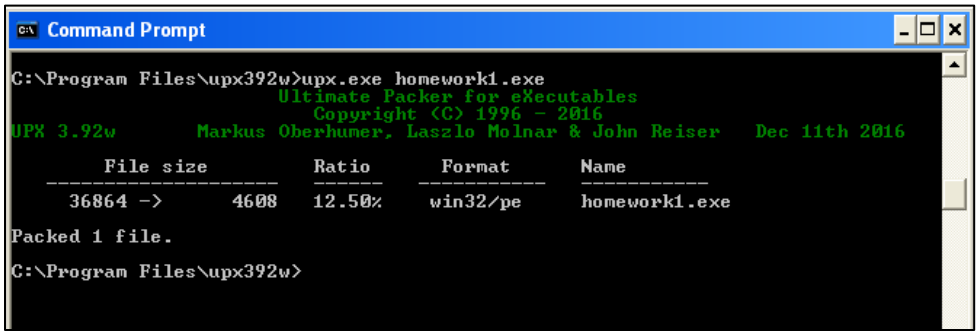
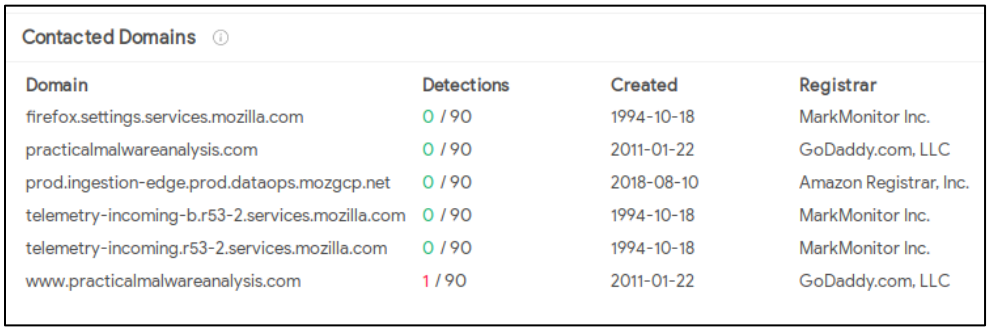
1. Is it packed or not? Support your answer with a screenshot of the tool that you used.

Ans. The homework1.exe is not a packed file. With the help of upx.exe tool, when run in the command line it gave the following output- “Packed 1 file” which means the file was not already packed before running the upx.exe tool. Below is the screenshot for reference:



2. Does this malware sample contact any host on the Internet? If so, what is the name of the host? Support your answer with a screenshot of the tool that you used.

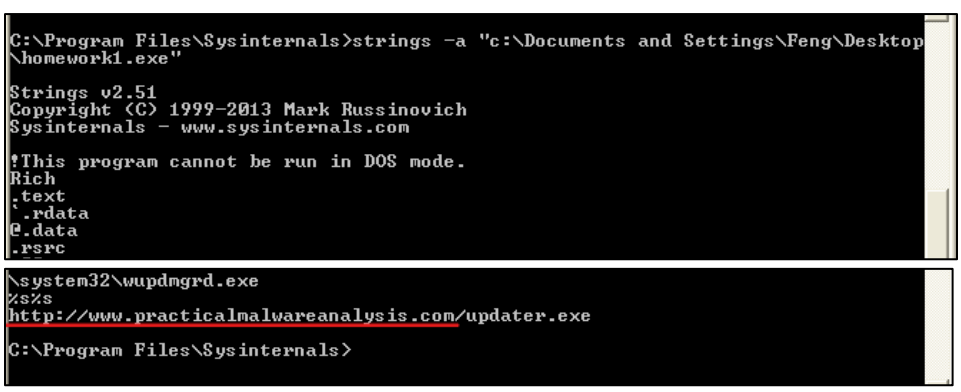
Ans: Below is the list of hosts on Internet contacted by malware sample. Virustotal.com tool was used to find it.



Contacted Domains

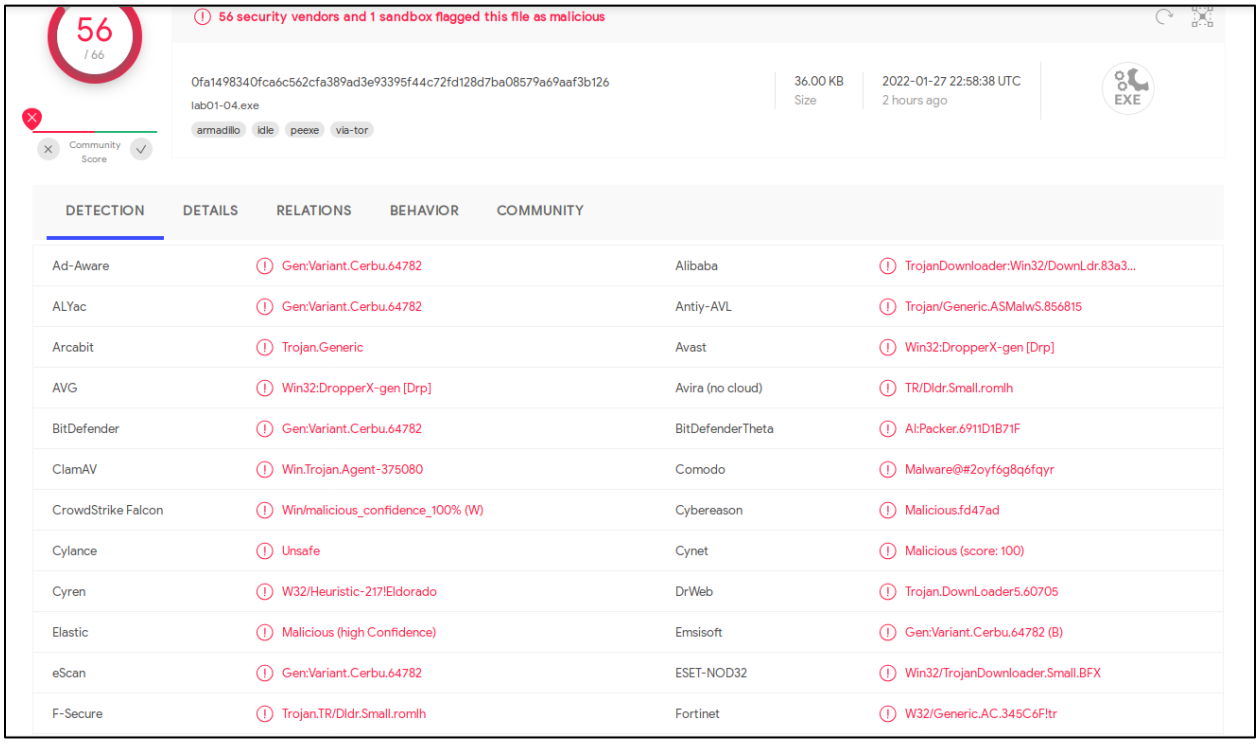
Domain	Detections	Created	Registrar
firefox.settings.services.mozilla.com	0 / 90	1994-10-18	MarkMonitor Inc.
practicalmalwareanalysis.com	0 / 90	2011-01-22	GoDaddy.com, LLC
prod.ingestion-edge.prod.dataops.mozgcp.net	0 / 90	2018-08-10	Amazon Registrar, Inc.
telemetry-incoming-b.r53-2.services.mozilla.com	0 / 90	1994-10-18	MarkMonitor Inc.
telemetry-incoming.r53-2.services.mozilla.com	0 / 90	1994-10-18	MarkMonitor Inc.
www.practicalmalwareanalysis.com	1 / 90	2011-01-22	GoDaddy.com, LLC

We can also find the name of the host on the internet contacted by the malware sample using Sysinternals tool called ‘Strings’. Upon execution of the command, it was found that **www.practicalmalwareanalysis.com** is the host contacted by malware sample. Below is the screenshot for reference:



3. Upload this file to VirusTotal.com and summarize the findings of VirusTotal, include the report from VirusTotal as an appendix in your submission.

Ans: Upon uploading the file on virustotal.com, it can be seen that the file is detected to be malicious by 56 Antivirus engines. The file is a malicious code that downloads and/or drops additional malware onto a system.



56 security vendors and 1 sandbox flagged this file as malicious

56 / 66

Community Score

0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126

lab01-04.exe

armadillo idle peexe via-tor

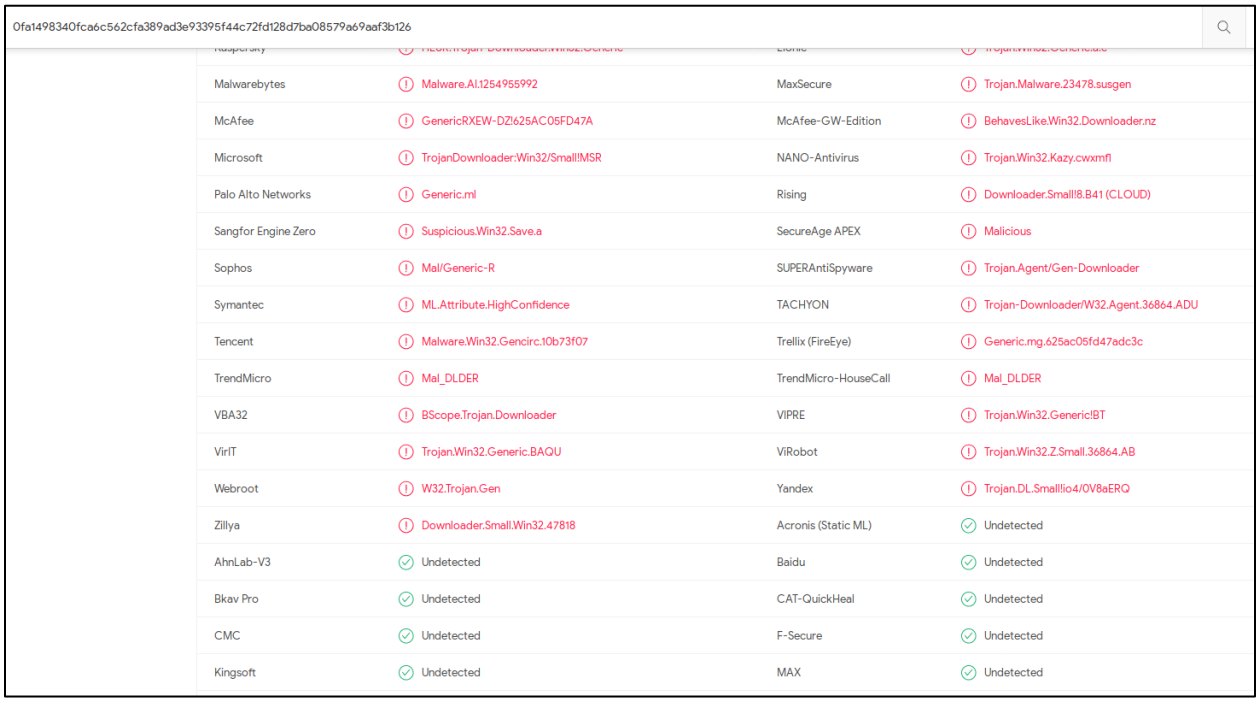
36.00 KB Size

2022-01-27 22:58:38 UTC 2 hours ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Ad-Aware	Gen:Variant.Cerbu.64782	Alibaba	TrojanDownloader:Win32/DownLdr.83a3...
ALYac	Gen:Variant.Cerbu.64782	Antiy-AVL	Trojan/Generic.ASMalwS.856815
Arcabit	Trojan.Generic	Avast	Win32:DropperX-gen [Drp]
AVG	Win32:DropperX-gen [Drp]	Avira (no cloud)	TR/Dldr.Small.romlh
BitDefender	Gen:Variant.Cerbu.64782	BitDefenderTheta	AI:Packer.6911D1B71F
ClamAV	Win.Trojan.Agent-375080	Comodo	Malware@#2oyf6g8q6fqyr
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.fd47ad
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W32/Heuristic-217!Eldorado	DrWeb	Trojan.DownLoader5.60705
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Cerbu.64782 (B)
eScan	Gen:Variant.Cerbu.64782	ESET-NOD32	Win32/TrojanDownloader.Small.BFX
F-Secure	Trojan.TR/Dldr.Small.romlh	Fortinet	W32/Generic.AC.345C6F!tr



0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126

Malwarebytes	Malware.AI.1254955992	MaxSecure	Trojan.Malware.23478.susgen
McAfee	GenericRXEW-DZ!625AC05FD47A	McAfee-GW-Edition	BehavesLike.Win32.Downloader.nz
Microsoft	TrojanDownloader:Win32/Small!MSR	NANO-Antivirus	Trojan.Win32.Kazy.cwxmfl
Palo Alto Networks	Generic.ml	Rising	Downloader.Small!8.B41 (CLOUD)
Sangfor Engine Zero	Suspicious.Win32.Save.a	SecureAge APEX	Malicious
Sophos	Mal/Generic-R	SUPERAntiSpyware	Trojan.Agent/Gen-Downloader
Symantec	ML.Attribute.HighConfidence	TACHYON	Trojan-Downloader/W32.Agent.36864.ADU
Tencent	Malware.Win32.Gencirc.10b73f07	Trellix (FireEye)	Generic.mg.625ac05fd47adc3c
TrendMicro	Mal_DLDER	TrendMicro-HouseCall	Mal_DLDER
VBA32	BScope.Trojan.Downloader	VIPRE	Trojan.Win32.Generic!BT
VirIT	Trojan.Win32.Generic.BAQU	ViRobot	Trojan.Win32.Z.Small.36864.AB
Webroot	W32.Trojan.Gen	Yandex	Trojan.DL.Small!io4/0V8aERQ
Zillya	Downloader.Small.Win32.47818	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Baidu	Undetected
Bkav Pro	Undetected	CAT-QuickHeal	Undetected
CMC	Undetected	F-Secure	Undetected
Kingsoft	Undetected	MAX	Undetected

Under the 'Details' tab, we get the hash value of files, the file type which says it's a PE32 executable for MS Windows and also its creation time and other details as seen in below screenshot.

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Basic Properties

MD5	625ac05fd47adc3c63700c3b30de79ab
SHA-1	9369d80106dd245938996e245340a3c6f17587fe
SHA-256	0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126
Vhash	034046151d151038z100f=z
Authentihash	e4d9d8ea008b5521c4b4273b8a276cf618db3f8af0bdd2f17d50f6c09e5bc150
Imphash	aade0ea6fbdcd9b8e96fe999cae6f603
Rich PE header hash	a9ce8adbba583f6837fc888ad6f8789e
SSDEEP	96:TF0MgAr71nxY9AAIvqZ2ZNHHsP4oynLKcm5OzG38U6p2WL4P4oyn:iJaPLjC2ZNHMP4oynLKL38jp2VP4oyn
TLSH	T14EF2A7476B14D432D7884176262F82E68713697213B941CF9BF7568C85B6CE3923EF07
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Microsoft Visual C++ compiled executable (generic) (40.3%)
TrID	Win32 Dynamic Link Library (generic) (16%)
TrID	Win16 NE executable (generic) (12.3%)
TrID	Win32 Executable (generic) (11%)
TrID	Win32 Executable MS Visual FoxPro 7 (5.4%)
File size	36.00 KB (36864 bytes)
PEiD packer	Microsoft Visual C++
Cyren packer	rsrc

History

Creation Time	2019-08-30 22:26:59 UTC
First Seen In The Wild	2011-07-05 18:16:16 UTC
First Submission	2011-07-06 00:05:42 UTC
Last Submission	2022-01-27 22:17:20 UTC
Last Analysis	2022-02-02 03:35:00 UTC

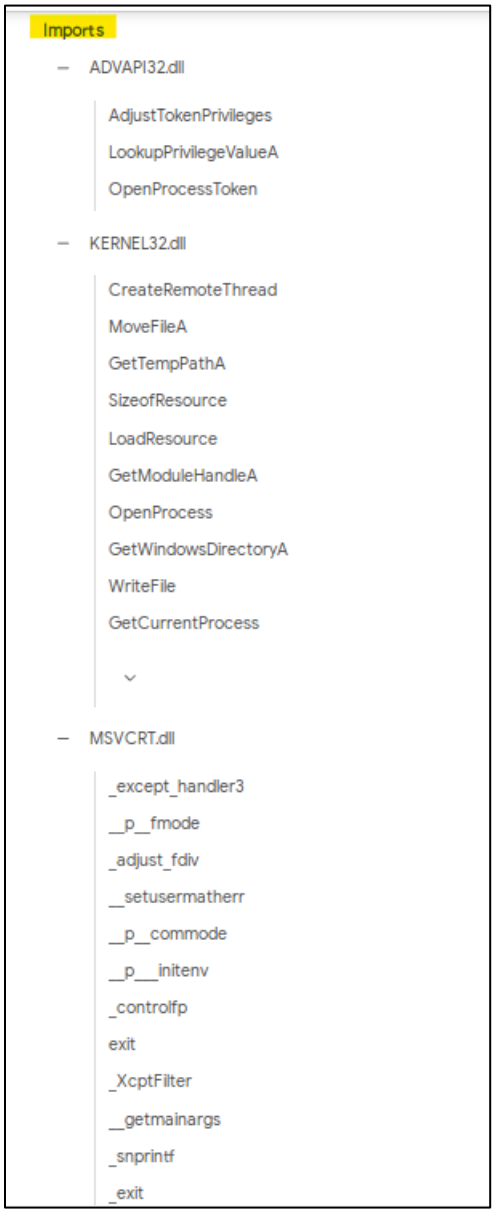
Apart from this, it also gives us details of the compilation date and the imported functions as seen below:

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2019-08-30 22:26:59 UTC
Entry Point	5583
Contained Sections	4

Based on the imports from Kernel32 we can see that this will load resources from the file's resource section and write files to disk. Based on the 'GetWindowsDirectory' function we can assume this will write files to the system directory, and will then execute them due to the 'WinExec' function.

The imports from Advapi32 indicate that this is attempting to modify or change the token assigned to the execution of this process, presumably to elevate privileges or give extended access rights.



The 'Details' tab also gives us information about the sections present in the malware sample file. These sections contain either code or data.

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	1824	4096	3.12	77df9f7ebc4a2bc4bdf2b454d7635aee	419793.88
.rdata	8192	978	4096	1.59	d630e1eb49ed821e38202aefef911a39	729061.13
.data	12288	332	4096	0.51	d9a3822a7733a76776d8b6e64e364b9d	946649.25
.rsrc	16384	16480	20480	0.71	398569177d4d82090d3e1747be560f9a	4618603

Under the 'Relations' tab, we get information about the other domains and IP address that are contacted by the malware sample file. It also shows the detection scores of these domains and IPs indicating them to be malicious or not:

Contacted Domains

Domain	Detections	Created	Registrar
firefox.settings.services.mozilla.com	0 / 90	1994-10-18	MarkMonitor Inc.
practicalmalwareanalysis.com	1 / 90	2011-01-22	GoDaddy.com, LLC
prod.ingestion-edge.prod.dataops.mozgcp.net	0 / 90	2018-08-10	Amazon Registrar, Inc.
telemetry-incoming-b.r53-2.services.mozilla.com	0 / 90	1994-10-18	MarkMonitor Inc.
telemetry-incoming.r53-2.services.mozilla.com	0 / 90	1994-10-18	MarkMonitor Inc.
www.practicalmalwareanalysis.com	1 / 90	2011-01-22	GoDaddy.com, LLC

Contacted IP Addresses

IP	Detections	Autonomous System	Country
114.114.114.114	1 / 90	174	CN
13.107.4.50	0 / 90	8068	US
13.224.247.103	0 / 91	16509	US
13.224.247.119	0 / 91	16509	US
13.224.247.16	0 / 89	16509	US
13.224.247.21	0 / 89	16509	US
192.0.78.24	1 / 90	2635	US
192.0.78.25	1 / 90	2635	US
192.168.0.21	0 / 90	-	-
192.168.0.38	0 / 90	-	-

• • •

Details regarding the Execution Parents can also be seen under the 'Relations' tab. This shows other malicious files that execute the malware sample we uploaded on virustotal.

Execution Parents

Scanned	Detections	Type	Name
2021-01-02	51 / 71	Win32 EXE	Software.exe
2020-12-20	51 / 64	ZIP	Practical-Malware-Analysis-Labs.zip
2020-05-27	51 / 64	ZIP	Lab 1 documents-20200212.zip
2021-11-01	50 / 58	RAR	Chapter_1L.rar
2020-10-15	41 / 61	RAR	Chapter_1L.rar
2021-11-07	45 / 59	RAR	46CF898558FF66B83D919962DD7D088D.mlw
2021-11-15	34 / 56	RAR	恶意代码静态分析工具.rar
2022-02-02	58 / 65	Win32 EXE	practicalmalwareanalysis-labs.exe
2021-02-07	49 / 64	ZIP	Assignment1.zip
2021-11-08	50 / 58	RAR	Lab01.rar

Under the 'Relations' tab, it is also seen that malware sample drops another malicious executable file with the name 'wupdmgr.exe'.

Dropped Files

Scanned	Detections	File type	Name	
2022-01-28	56 / 67	?	Win32 EXE	wupdmgr.exe
2022-01-19	0 / 55	?	Text	PowerPlan.log
2022-01-30	0 / 57	?	JavaScript	ConDrv
?	?	?	file	ec5526b24e9bd32e2d03ac182d0ff27372ef2dcda72844de1e4ad7d13c9e6167

Below is the screenshot of URLs that are contacted by the malware. It seen that malicious executable named 'updater.exe' possibly is being downloaded from this website.

Contacted URLs

Scanned	Detections	Status	URL
2021-10-19	1 / 91	404	http://practicalmalwareanalysis.com/updater.exe
2021-09-27	4 / 90	404	http://www.practicalmalwareanalysis.com/updater.exe

Under the 'Behavior' tab, we get information about what processes and service actions were done by the malware sample upon executing the file in sandbox environment, the modules that were loaded and made use of, actions taken on filesystem and registry, HTTP requests and DNS resolutions. Below are the screenshots for reference:

File System Actions

Files With Modified Attributes

C:\Documents and Settings\Miller\Local Settings\Temporary Internet Files\Content.IE5

C:\Documents and Settings\Miller\Local Settings\Temporary Internet Files\Content.IE5\index.dat

C:\Documents and Settings\Miller\Cookies\index.dat

C:\Documents and Settings\Miller\Local Settings\History\History.IE5\index.dat

C:\Documents and Settings\Miller\Local Settings\History\History.IE5

C:\Documents and Settings\Miller\Cookies

C:\Documents and Settings\Miller\Local Settings\History

C:\Documents and Settings\Miller\Local Settings\Temporary Internet Files

Registry Actions

Registry Keys Set

+ HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\SESSION MANAGER\SFC
+ HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\SESSION MANAGER\SFC
+ HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS
+ HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP
+ HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS
+ HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
+ HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\CONNECTIONS
+ HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP
+ HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS
+ HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS

Registry Keys Deleted

HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS

Modules Loaded

Runtime Modules

c:\windows\system32\apphelp.dll

c:\windows\system32\user32.dll

c:\windows\system32\imm32.dll

c:\windows\system32\rpcrt4.dll

c:\windows\system32\psapi.dll

c:\windows\system32\secur32.dll

c:\windows\system32\wintrust.dll

c:\windows\system32\advapi32.dll

c:\windows\system32\gdi32.dll

c:\windows\system32\msvcrt.dll

Process And Service Actions

Processes Created

C:\DOCUME~1\Miller\LOCALS~1\Temp\Lab01-04.exe

C:\WINDOWS\system32\winlogon.exe

C:\WINDOWS\system32\wupdmgr.exe

C:\DOCUME~1\Miller\LOCALS~1\Temp\winup.exe

Shell Commands

C:\DOCUME~1\Miller\LOCALS~1\Temp\Lab01-04.exe

winlogon.exe

C:\WINDOWS\system32\wupdmgr.exe

C:\DOCUME~1\Miller\LOCALS~1\Temp\winup.exe

Processes Tree

↳ 1316 - C:\DOCUME~1\Miller\LOCALS~1\Temp\Lab01-04.exe

↳ 496 - C:\WINDOWS\system32\winlogon.exe

↳ 460 - C:\WINDOWS\system32\wupdmgr.exe

↳ 904 - C:\DOCUME~1\Miller\LOCALS~1\Temp\winup.exe

Network Communication

HTTP Requests

– http://practicalmalwareanalysis.com/updater.exe

HTTP Method	GET
Response code	404

– http://www.practicalmalwareanalysis.com/updater.exe

HTTP Method	GET
Response code	301

DNS Resolutions

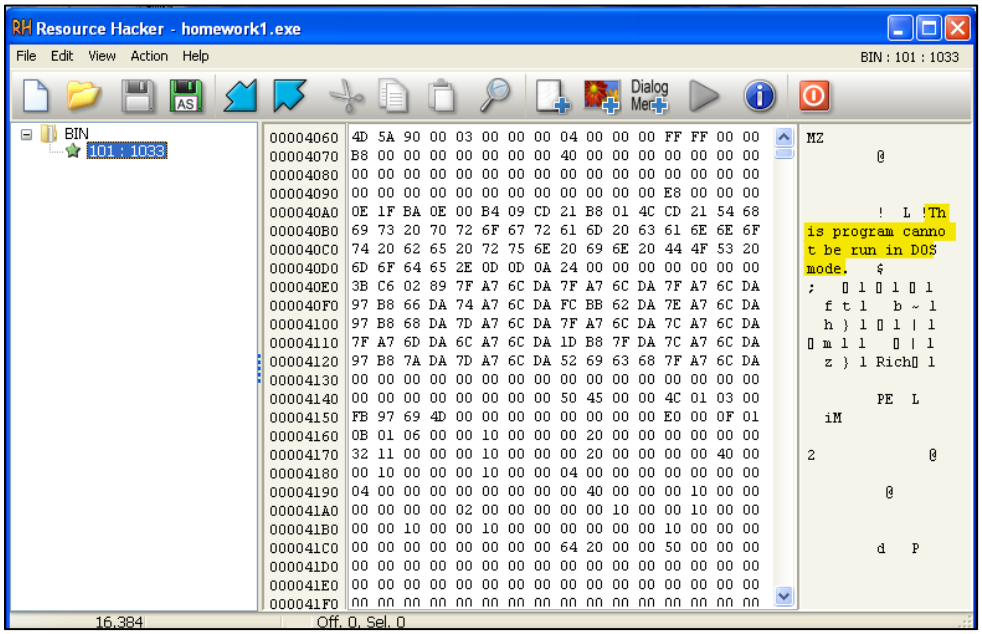
– www.practicalmalwareanalysis.com

192.0.78.25

192.0.78.24

4. This malware sample has another executable in its resource section. Extract it with Resource Hacker, analyze it, and write down the names of its imported APIs grouped by the DLLs.

Ans. When the malware sample was opened in Resource Hacker, we can see the string 'This program cannot be run in DOS mode.' This string is the error message included in the DOS header at the beginning of all PE files. Hence, we can conclude that this resource is an additional executable file stored in the resource section of the malware sample. The executable file is a downloader program that downloads additional malware. The resource was saved as a binary file and analyzed further using PEview tool. It calls URLDownloadToFileA, a function commonly used by malicious downloaders. It also calls WinExec, which probably executes the downloaded file.



In the below screenshot, under the 'Value' column is the names of imported APIs grouped by DLLs.