CPSC 458 Assignment 1 Answers

by Carla Jacobsen

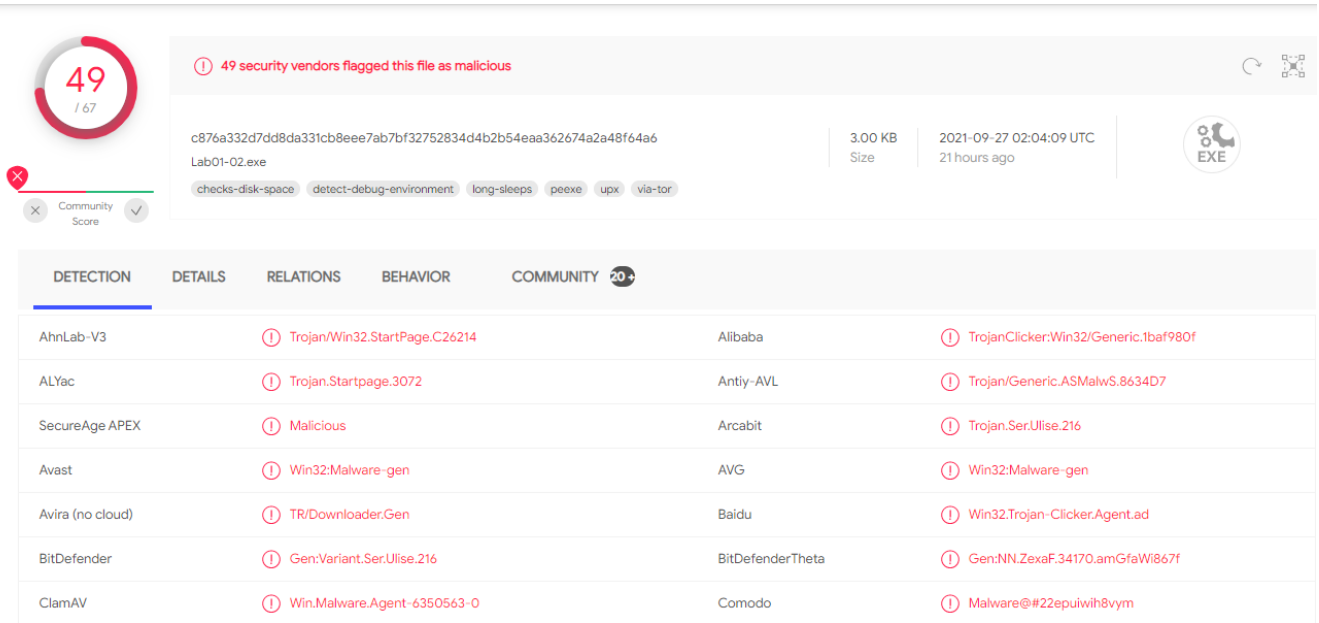
Question 2: Use the static analysis techniques learned in class in order to analyze 1.exe.

Does it match any existing antivirus definitions? Explain which ones and what do the different anti-viruses detect?

EditViewInsertFormatToolsTable
12pt
Paragraph

Yes:
c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6
Lab01-02.exe

Trojan
Downloader



==========

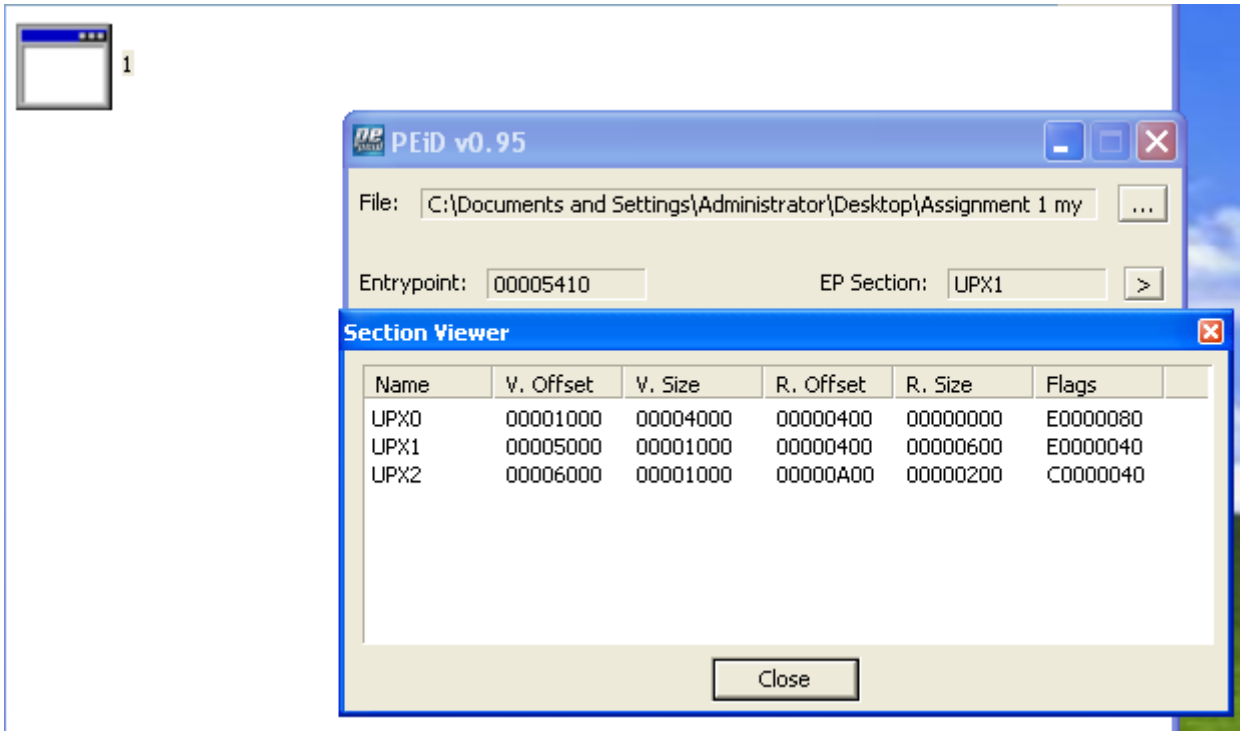
Question 3: Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

In Peid in the EP Section it says that it uses UPX0, UPX1, UPX2. So it probably is packed.

Unpacking: upx -d 1.exe

```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "C:\Documents and Settings\Administra
tor\Desktop\Assignment 1 my work\1 exe\q3 screenshot\unpacking"

C:\Documents and Settings\Administrator\Desktop\Assignment 1 my work\1 exe\q3 sc
reenshot\unpacking>upx -d 1.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95d       Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     16384 <-      3072   18.75%    win32/pe     1.exe

Unpacked 1 file.

C:\DOCUME~1\ADMINI~1\Desktop\ASSIGN~2\1EXE~1\Q3SCRE~1\UNPACK~1>
```

==========
==========



==========

==========
==========
==========

Question 4: Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?

CsrCaptureMessageMultiUnicodeStringsInPlace: uses unicode text

CsrClientConnectToServer: connects to a server

NtAdjustPrivilegesToken: seems to adjust privileges (http://undocumented.ntinternals.net/index.html?page=UserMode%2FUndocumented%20Functions%2FNT%20Objects%2FToken%2FNtAdjustPrivilegesToken.html says it changes privileges of tokens)

NtAllocateUserPhysicalPages: (http://www.codewarrior.cn/ntdoc/win2k/mm/NtAllocateUserPhysicalPages.htm says deals with pages and a user array)

NtCancelDeviceWakeupRequest: (http://www.codewarrior.cn/ntdoc/winxp/po/NtCancelDeviceWakeupRequest.htm seems to be able to prevent the device from being woken up)

DeviceIoControl function (ioapiset.h)
[4:48 PM] Sends a control code directly to a specified device driver, causing the corresponding device to perform the corresponding operation.

InternetOpenUrlA: seems to access the internet (https://docs.microsoft.com/en-us/windows/win32/api/wininet/nf-wininet-internetopenurla connects to a url)

CreateServiceA: (https://docs.microsoft.com/en-us/windows/win32/api/winsvc/nf-winsvc-createservicea starts a service and puts it into a database)

advapi32.dll: (https://www.file.net/process/advapi32.dll.html can shutdown or restart the machine, has access to the windows registry, has access to user accounts, can start and stop windows services)

NTDLL.DLL: (from lecture: not normally imported by windows programs, deals with the kernel)

RPCRT4.DLL: (https://www.processlibrary.com/en/directory/files/rpcrt4/23580/ used for networks and the internet; might connect to the internet or a network)

CRYPT32.DLL: (https://docs.microsoft.com/en-us/windows/win32/seccrypto/crypt32-dll-versions#:~:text=In%20this%20article-,Crypt32.,this%20DLL%20provide%20different%20capabilities. Deals with cryptography; there might be encryption or decryption)

MSASN1.DLL: (https://www.file.net/process/msasn1.dll.html also deals with cryptography)

MSIMG32.DLL: (https://itstillworks.com/msimg32dll-6633013.html creates transparent images and gradients; possibly deals with graphics; maybe there is a GUI)

NETAPI32.DLL (https://www.processlibrary.com/en/directory/files/netapi32/21334/ deals with networks; might try to connect to a network)

WS2_32.DLL (from lecture: deals with networks; in dependency walker, most of the functions from here are showing up as N/A)

WLDAP32.DLL: (https://www.processlibrary.com/en/directory/files/wldap32/21856/: deals with internet directories; might connect to the internet; the functions here display as N/A in the dependency walker)

IMAGEHLP.DLL: (https://www.processlibrary.com/en/directory/files/imagehlp/25269/ if this isn't in C:\Windows\System32 then it is a potential security risk)

GetDesktopWindow: (https://docs.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-getdesktopwindow deals with the desktop window)

WinVerifyTrust: (https://docs.microsoft.com/en-us/windows/win32/api/wintrust/nf-wintrust-winverifytrust ; https://docs.microsoft.com/en-us/windows/win32/secgloss/t-gly deals with whether a file is trusted or not)

WININET.DLL: (from lecture: deals with networks)

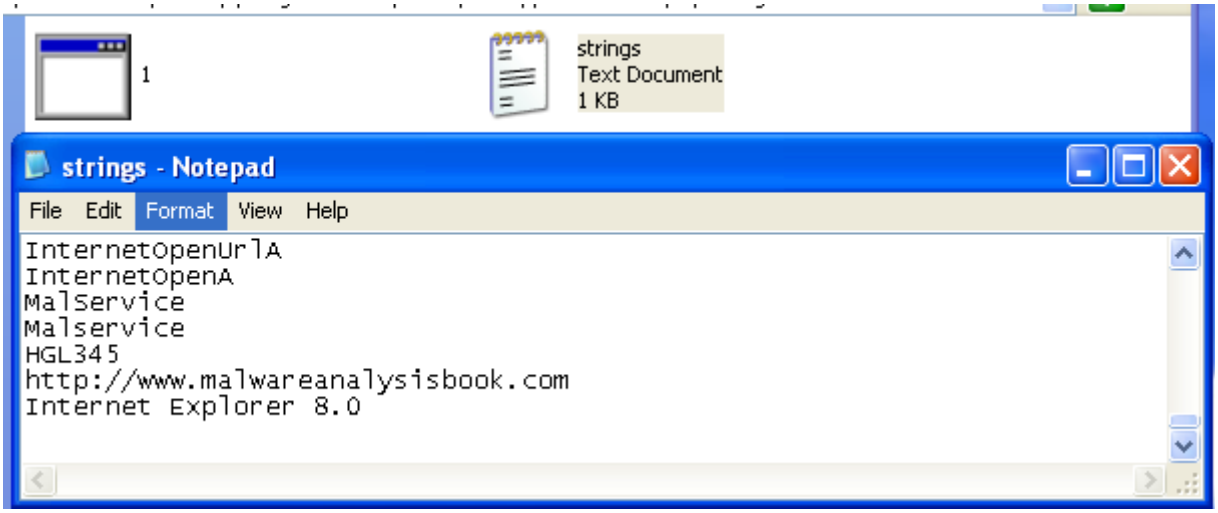
GDI32.DLL: (from lecture: deals with graphics, might have a GUI)

USER32.DLL: (from lecture: deals with user-interface; might have a GUI)
==========
==========
==========
==========
==========
==========

Question 5: What host- or network-based indicators could be used to identify this malware on infected machines?

Network based: http:// www.malwareanalysisbook. Com, Internet Explorer 8.0

Host-based: MalService, Malservice, HGL345



==========

Question 6: Are there any indications that this program attempts to access the internet? Explain.

InternetOpenUrlA: seems to access the internet (https://docs.microsoft.com/en-us/windows/win32/api/wininet/nf-wininet-internetopenurla connects to a url)

RPCRT4.DLL: (https://www.processlibrary.com/en/directory/files/rpcrt4/23580/ used for networks and the internet; might connect to the internet or a network)

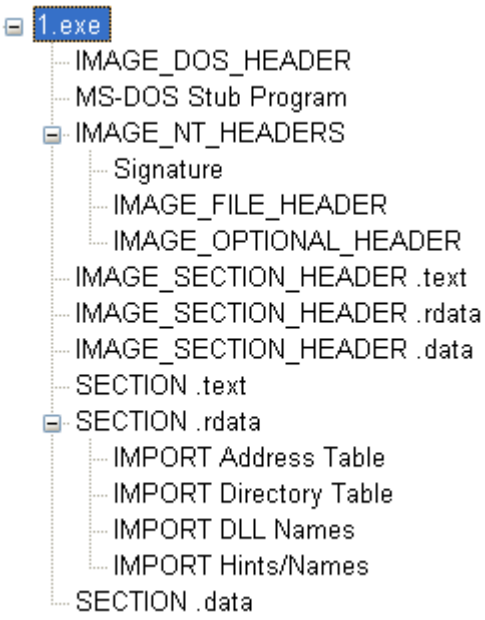
Strings seems to indicate that it may connect to http ://www.malwareanalysisbook .com

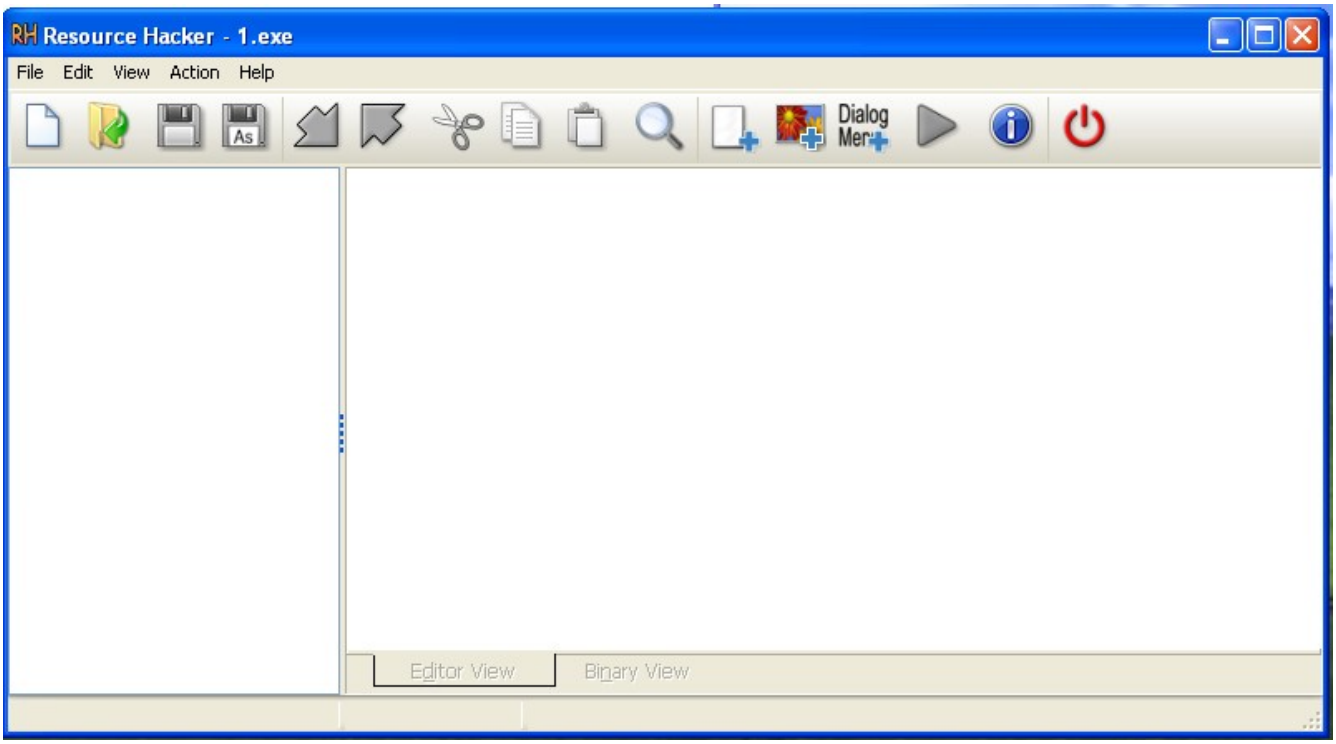
WLDAP32.DLL: (https://www.processlibrary.com/en/directory/files/wldap32/21856/: deals with internet directories; might connect to the internet; the functions here display as N/A in the dependency walker)

==========

Question 7: Is this likely a graphical program? Justify your answer with evidence from analysis.

There is no .rsrc section in the PeView for this program, and attempting to open it in Resource Hacker results in nothing happening. Therefore it is implied that this is probably not a graphical program.





~~GDI32.DLL: (from lecture: deals with graphics, might have a GUI)~~

~~USER32.DLL: (from lecture: deals with user-interface; might have a GUI)~~

~~There might be graphics in this program.~~

==========

==========

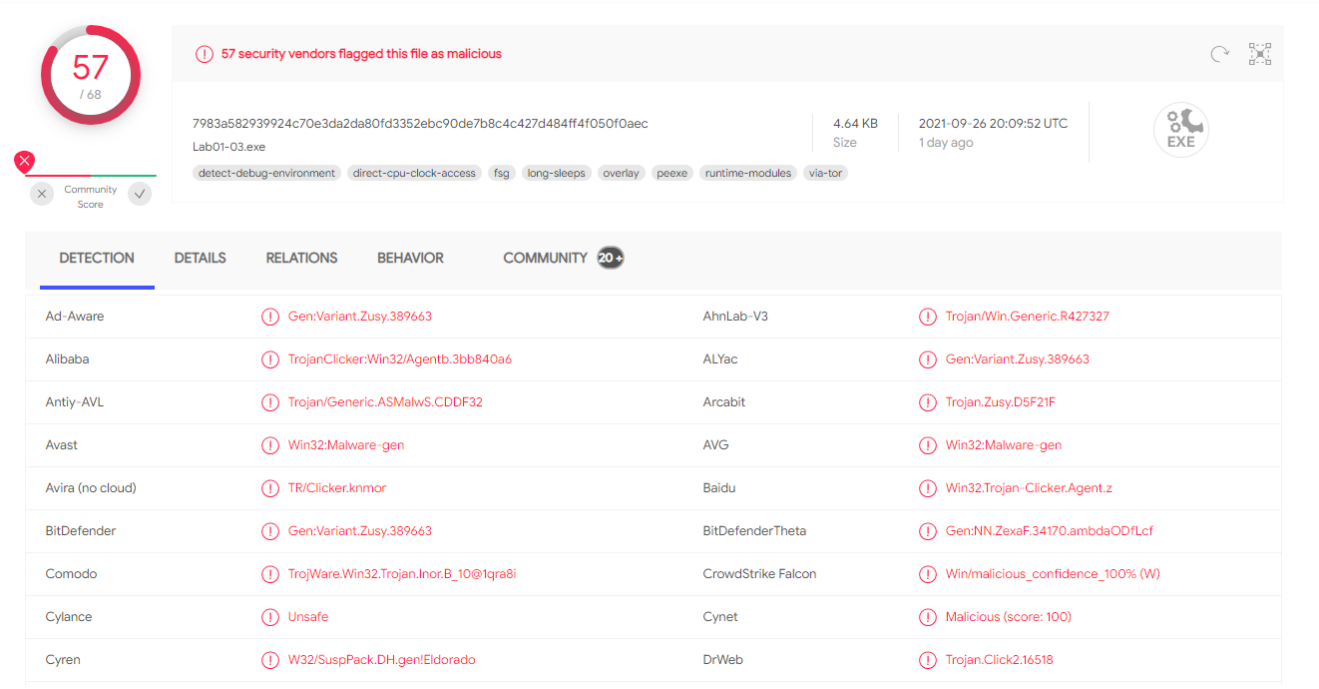
Question 8: Use the basic static analysis techniques covered in class in order to analyze 2.exe .com/. Does it match any existing antivirus definitions? Explain which antiviruses detect it and what they detect?

(Links to an external site.)

7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec

Lab01-03.exe

K7GW says Spyware
Microsoft says Trojan
SentinelOne (Static ML) says malicious PE



Microsoft	Trojan:Win32/Tnega!MSR
SentinelOne (Static ML)	Static AI - Malicious PE

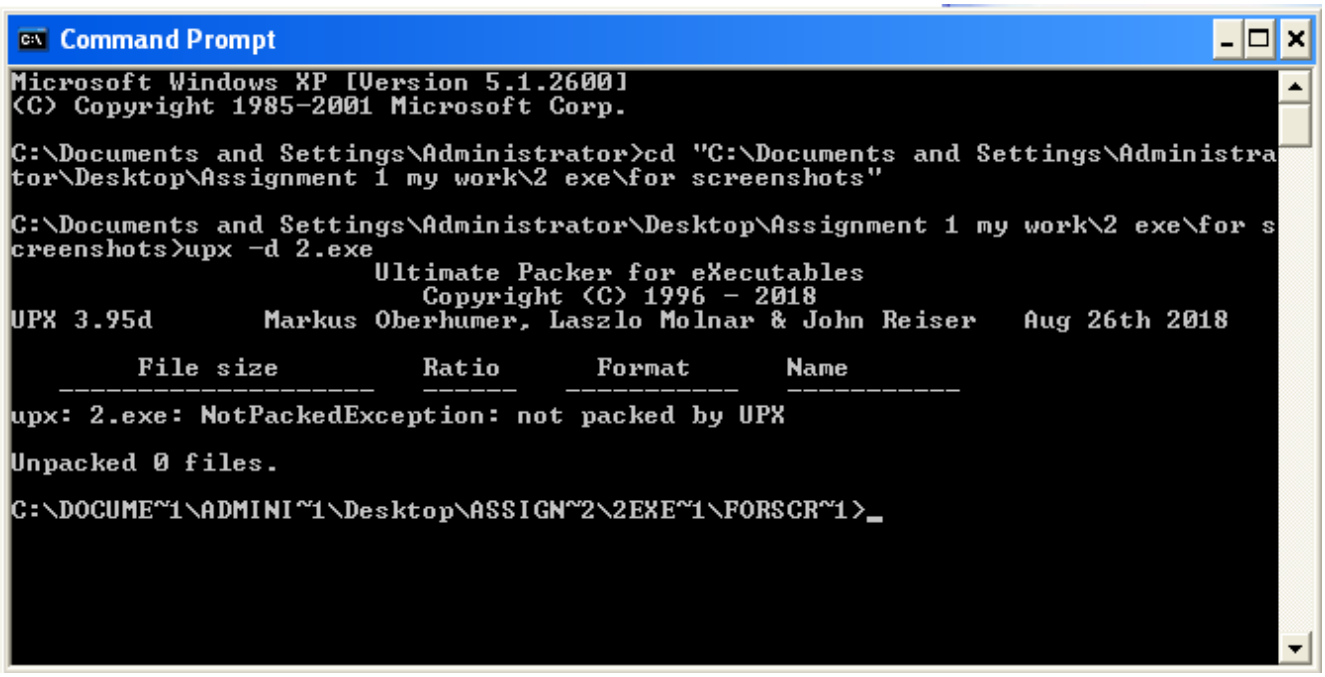
==========

Question 9: Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

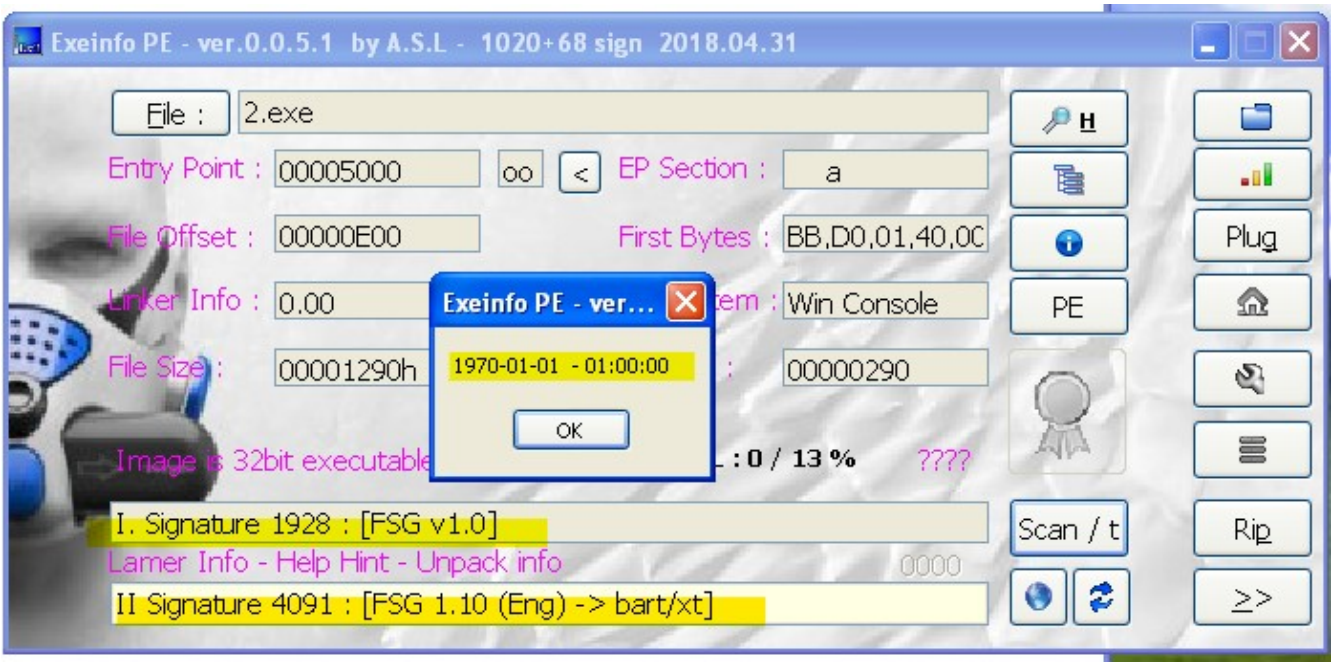
This file does not seem to be packed by UPX. Attempting to unpack it results in a message saying that it isn't packed by UPX.

The file seems to be packed by FSG which is a packer we have not yet learned about.

The file also has a timestamp of 1970-01-01 – 01:00:00 which is a sign of obfuscation.



```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "C:\Documents and Settings\Administra
tor\Desktop\Assignment 1 my work\2 exe\for screenshots"

C:\Documents and Settings\Administrator\Desktop\Assignment 1 my work\2 exe\for s
creenshots>upx -d 2.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95d       Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
upx: 2.exe: NotPackedException: not packed by UPX

Unpacked 0 files.

C:\DOCUME~1\ADMINI~1\Desktop\ASSIGN~2\2EXE~1\FORSCR~1>_
```



==========

Question 10: When was this program compiled? What was the compiler? Can you tell?

This information is hidden due to being packed by FSG.

pFile	Data	Description	Value
00000064	014C	Machine	IMAGE_FILE_MACHINE_I386
00000066	0003	Number of Sections	
00000068	00000000	Time Date Stamp	
0000006C	00000000	Pointer to Symbol Table	
00000070	00000000	Number of Symbols	
00000074	00E0	Size of Optional Header	
00000076	010F	Characteristics	
		0001	IMAGE_FILE_RELOCS_STRIPPED
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPED
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
		0100	IMAGE_FILE_32BIT_MACHINE

==========
==========
==========

==========
==========
==========

Question 11: Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?

CsrCaptureMessageMultiUnicodeStringsInPlace: probably does something related to messages, there are no helpful google results when searching for this

CsrClientConnectToServer: probably connects to a server (https://www.geoffchappell.com/studies/windows/win32/ntdll/api/csrutil/clientcallserver.htm connects to a specific kind of server)

NtAdjustPrivilegesToken: seems to adjust privileges (http://undocumented.ntinternals.net/index.html?page=UserMode%2FUndocumented%20Functions%2FNT%20Objects%2FToken%2FNtAdjustPrivilegesToken.html says it changes privileges of tokens)

NtAllocateUserPhysicalPages: (http://www.codewarrior.cn/ntdoc/win2k/mm/NtAllocateUserPhysicalPages.htm says deals with pages and a user array)

NtCancelDeviceWakeupRequest: (http://www.codewarrior.cn/ntdoc/winxp/po/NtCancelDeviceWakeupRequest.htm seems to be able to prevent the device from being woken up)

NtQuerySystemInformation: (https://docs.microsoft.com/en-us/windows/win32/api/winternl/nf-winternl-ntquerysysteminformation collects some information about the operating system)

NtReadFile: (https://docs.microsoft.com/en-us/windows/win32/devnotes/ntreadfile reads from a file)

NtSetSystemEnvironmentValueEx: (can't find any information that says what it does but some of the google search results seem to indicate that it might be related to malware [I did not visit any of these search results pages but saw that in the names of some results were malware related] and the name seems to imply that it changes parts of the operating system)

AdjustTokenPrivileges: (https://docs.microsoft.com/en-us/windows/win32/api/securitybaseapi/nf-securitybaseapi-adjusttokenprivileges changes privileges of a token)

NTCreateFile - Creates a new file or directory, or opens an existing file, device, directory, or volume.
https://docs.microsoft.com/en-us/windows/win32/api/winternl/nf-winternl-ntcreatefile

fmod (gets the remainder from a division operation https://www.cplusplus.com/reference/cmath/fmod/ more advanced analysis is needed to determine what this function is used for in the program)

MSVCRT (https://docs.python.org/3/library/msvcrt.html used in some windows services, there might be a service involved)

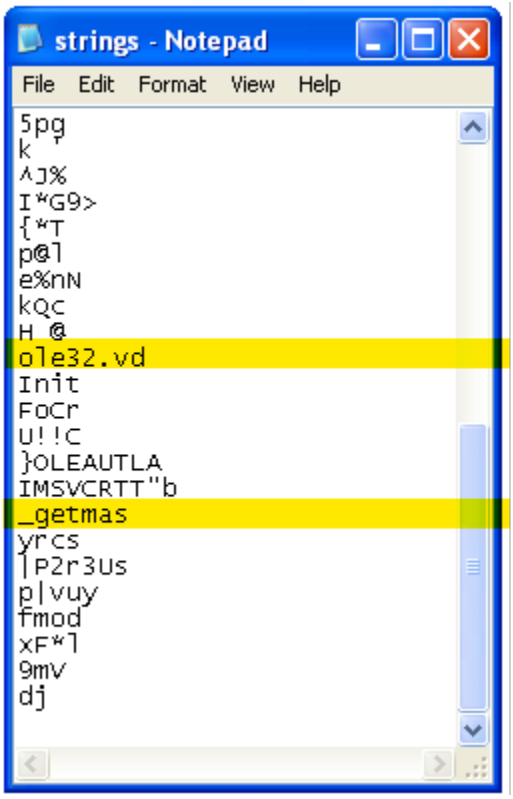
KERNEL32.dll (from lecture, might have access to memory, files, and hardware)

==========
==========
==========
==========
==========
==========

Question 12: What host- or network-based indicators could be used to identify this malware on infected machines?

Host based: ole32.vd (seems to be related to ole32.dll https://www.processlibrary.com/en/directory/files/ole32/23128/ , might be a file related to the dll), _getmas (searched online and found only 1 result but couldn't use it because it seemed like it would have homework answers, need to use more advanced analysis to find out what this is)

Network based: none found, more advanced analysis is needed



==========

Question 13: Are there indications that this program connects to the internet? Justify your answer with evidence from analysis.

CsrClientConnectToServer: probably connects to a server (https://www.geoffchappell.com/studies/windows/win32/ntdll/api/csrutil/clientcallserver.htm connects to a specific kind of server)

It might be able to connect to the internet but no network-based indicators were found. More advanced analysis is needed.

==========

Question 14: Is this likely a graphical program? Justify your answer using evidence from analysis.

There is no evidence that this is a graphical program so far.

The program is packed, which means that if it is a graphical program, then evidence of this is hidden and more advanced analysis techniques are needed.

==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========

Question 15: Analyze 3.exe using basic static analysis techniques described in class.

Upload the 3.exe file to http://www.VirusTotal.com/. Does it match any existing antivirus definitions? What antivirus systems detect it? What do they detect?

K7AntiVirus says trojan downloader

Ikarus says backdoor

Avast says dropper

56 / 67

Community Score

56 security vendors and 1 sandbox flagged this file as malicious

0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126
Lab01-04.exe
armadillo peexe via-tor

36.00 KB Size | 2021-09-27 06:30:07 UTC 17 hours ago | EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 20+

Ad-Aware	Gen:Variant.Cerbu.64782	Alibaba	TrojanDownloader:Win32/DownLdr.83a3e...
ALYac	Gen:Variant.Cerbu.64782	Antiy-AVL	Trojan/Generic.ASMalwS.856815
SecureAge APEX	Malicious	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)
Cylance	Unsafe	Cynet	Malicious (score: 100)

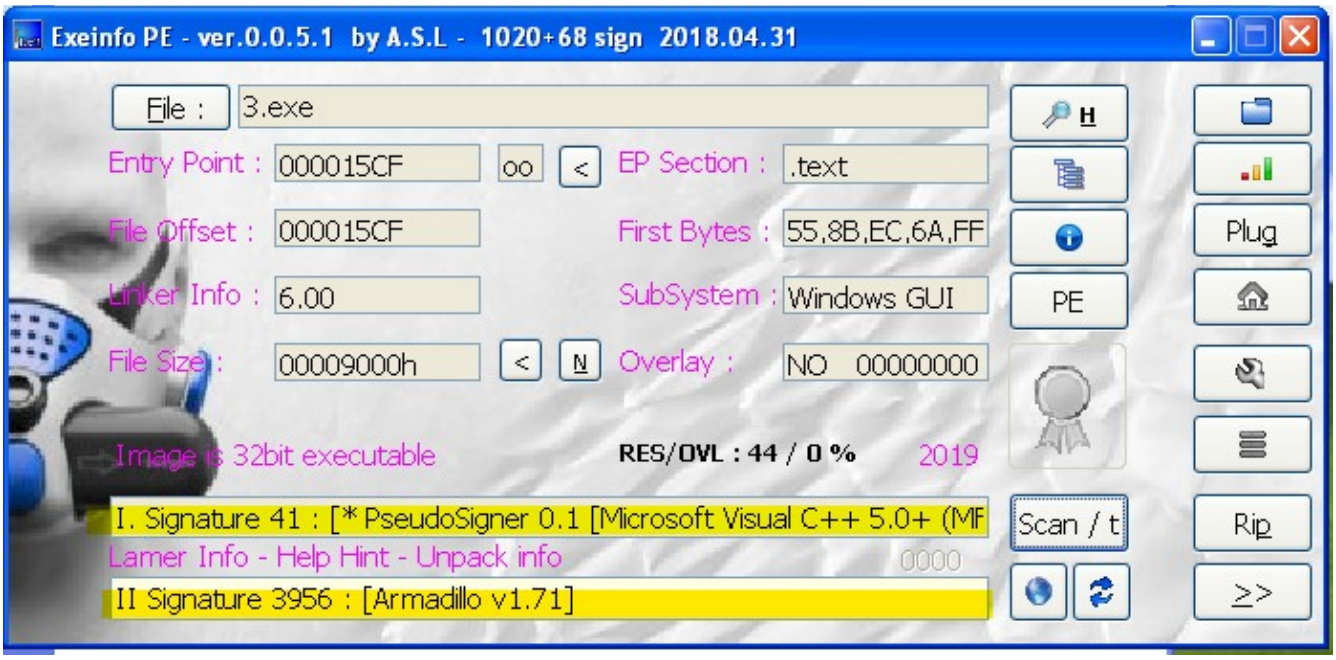
K7AntiVirus	Trojan-Downloader (0055e3da1)
Ikarus	Backdoor.Win32.SuspectCRC

==========

Q16: Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

This file does not seem to be packed by UPX. Attempting to unpack it results in a message saying that it isn't packed by UPX. The static analysis tools do not give any indications that the file is packed.

```
C:\Documents and Settings\Administrator\Desktop\Assignment 1 my work\3 exe\for s
creenshots>upx -d 3.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95d       Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
upx: 3.exe: NotPackedException: not packed by UPX

Unpacked 0 files.
```



==========

Question 17: When was this program compiled? What was the compiler? Can you tell?

Compiled on 2019-08-31 – 00:26:59 by Microsoft Visual C++ 5.0+ (MFC).

pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0004	Number of Sections	
000000F0	5D69A2B3	Time Date Stamp	2019/08/30 Fri 22:26:59 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	010F	Characteristics	
		0001	IMAGE_FILE_RELOCS_STRIPPED
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPED
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
		0100	IMAGE_FILE_32BIT_MACHINE

==========
==========
==========
==========
==========
==========

Question 18: Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?

CreateFileA: creates a file

GetWindowsDirectoryA: (https://docs.microsoft.com/en-us/windows/win32/api/sysinfoapi/nf-sysinfoapi-getwindowsdirectorya gets the path of a directory)

LoadLibraryA: (https://docs.microsoft.com/en-us/windows/win32/api/libloaderapi/nf-libloaderapi-loadlibrarya loads a library)

MoveFileA: (https://docs.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-movefilea moves files)

WinExec: (https://docs.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-winexec runs an application)

WriteFile: (https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-writefile writes to a file)

advapi32.dll: (https://www.file.net/process/advapi32.dll.html can shutdown or restart the machine, has access to the windows registry, has access to user accounts, can start and stop windows services)

KERNEL32.dll (from lecture, might have access to memory, files, and hardware)

AdjustTokenPrivileges: (https://docs.microsoft.com/en-us/windows/win32/api/securitybaseapi/nf-securitybaseapi-adjusttokenprivileges changes privileges of a token)

MSVCRT.dll (https://docs.python.org/3/library/msvcrt.html used in some windows services, there might be a service involved)

_snprintf: (https://docs.microsoft.com/en-us/cpp/c-runtime-library/reference/snprintf-snprintf-snprintf-l-snwprintf-snwprintf-l?view=msvc-160 used in text outputs, might have a GUI or text display)

_exit (https://man7.org/linux/man-pages/man2/exit.2.html the program might self-terminate)

sfc_os.dll (https://www.file.net/process/sfc_os.dll.html says that some malware pretends to be sfc_os.dll, https://www.exefiles.com/en/dll/sfc-os-dll/#:~:text=Read%3A%204.7%20minutes%5D-,Sfc_os.,DLL%20(Executable%20application)%20file. Deals with files, might do something with files)

psapi.dll (https://docs.microsoft.com/en-us/windows/win32/psapi/process-status-helper might monitor processes and device drivers, advanced analysis techniques are needed to determine if this is the case)

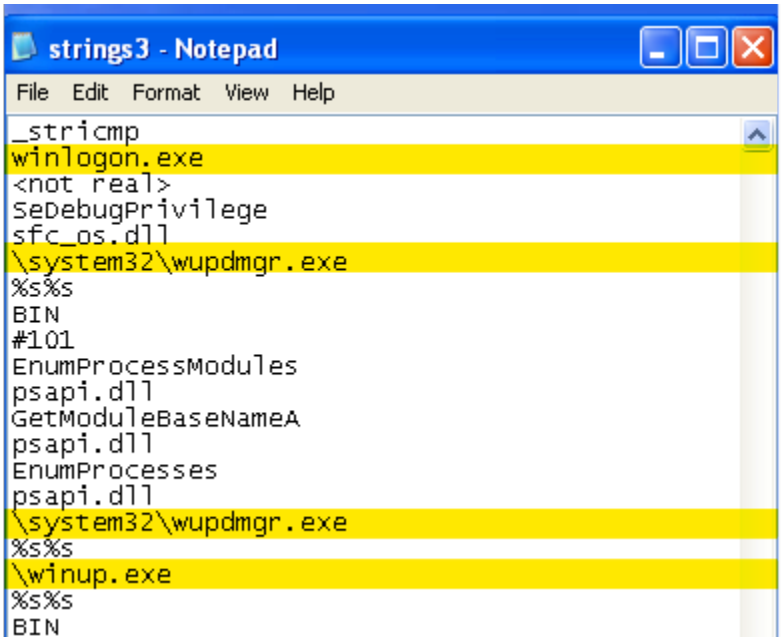
URLDownloadToFileA (https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms775123(v=vs.85) used to download files from the internet)

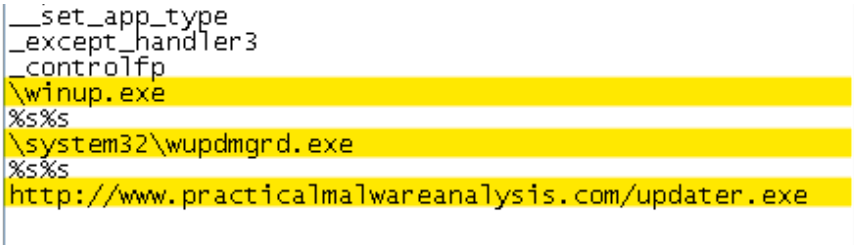
==========
==========
==========
==========
==========
==========

Question 19: What host- or network-based indicators could be used to identify this malware on infected machines?

Host-based: winlogon.exe, \system32\wupdmgr.exe, \system32\wupdmgr.exe, \winup.exe, \winup.exe, \system32\wupdmgrd.exe

Network-based: http ://www .practicalmalwareanalysis.com/updater.exe





==========

Question 20: This file has one resource in the resource section. Use Resource Hacker to examine that resource, and then use it to extract the resource. What can you learn from the resource?

VirusTotal says that the extracted resource is a trojan downloader.

11 / 60

Community Score

11 security vendors flagged this file as malicious

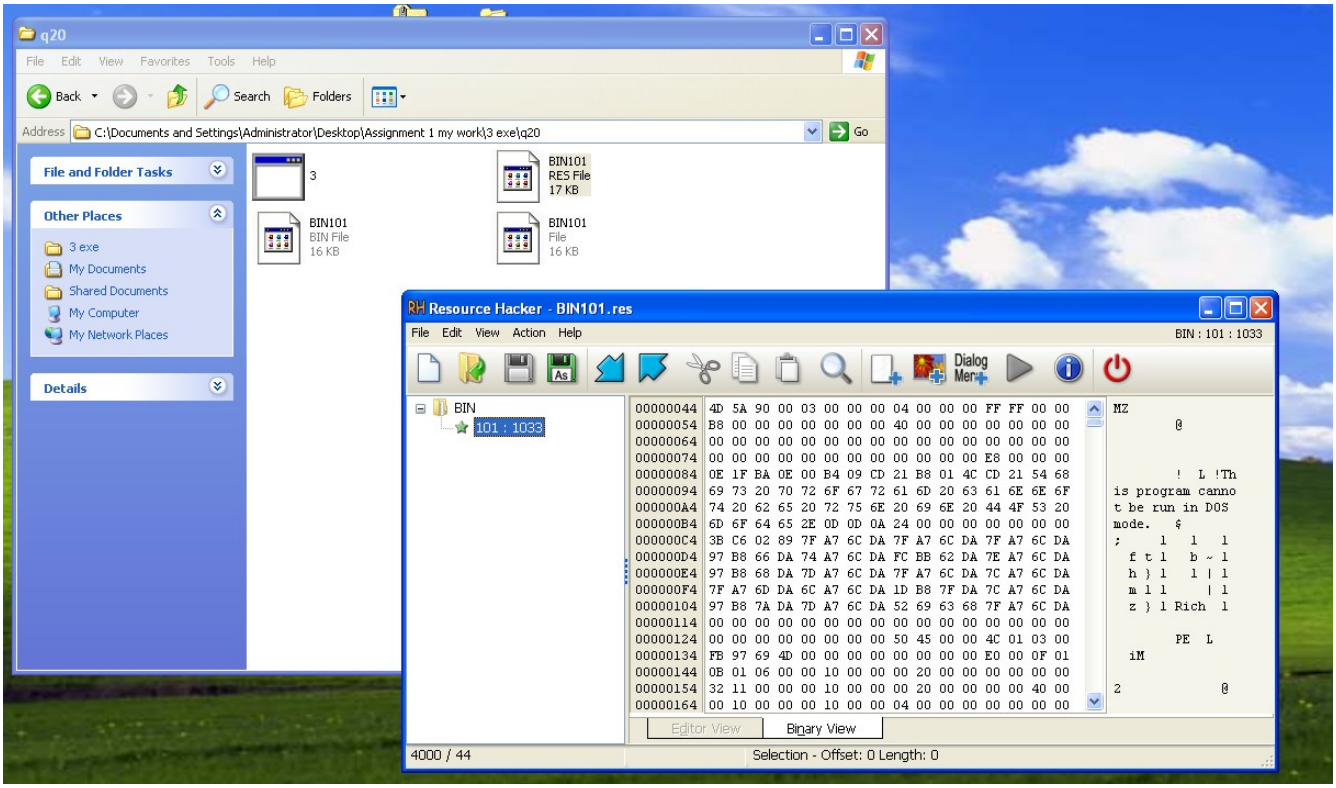
666c872b5caacf919d53c7d3dd346a556a9f9361da5b52941ee0ce8f8d817ab9
extracted.res

16.07 KB
Size

2020-05-22 10:33:49 UTC
1 year ago

DETECTION | DETAILS | COMMUNITY 1

Arcabit	Trojan.Downloader.JTGZ	BitDefender	Trojan.Downloader.JTGZ
BitDefenderTheta	Gen:NN.ZexaF.34122.bmW@auxp1Nj	DrWeb	Trojan.DownLoader5.60705
Emsisoft	Trojan.Downloader.JTGZ (B)	FireEye	Trojan.Downloader.JTGZ
GData	Trojan.Downloader.JTGZ	Ikarus	Trojan.Downloader
MAX	Malware (ai Score=82)	NANO-Antivirus	Trojan.Win32.Small.dbqpbh
Qihoo-360	Generic/Trojan.Downloader.9d3	Ad-Aware	Undetected



==========
==========
==========
==========
==========
==========
==========
==========
==========

==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========