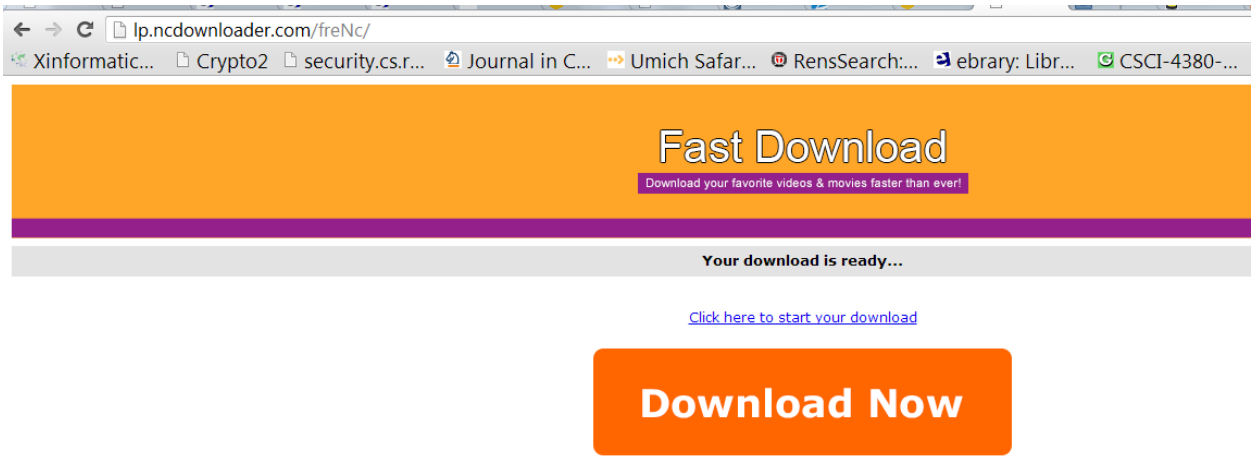
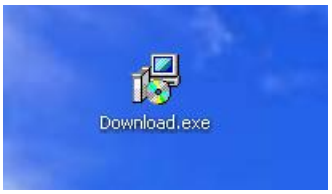
Consider the purpose of this report to find host-based and network-based indicators, and to establish a general purpose/functionality of the program.

Jeremy White
2/1/2013
Sample Malware Analysis 1

I found malware by typing “free movies” into google.

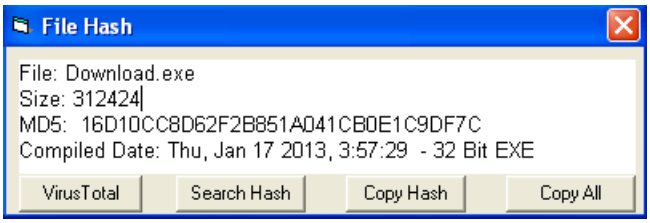


I clicked the download button which was the address http://storebox1.info/v686 and downloaded Download.exe.



Static Analysis

1) **File Hash:**



2) Virus Total:

virustotal

SHA256: 6cfaedc32559f4add9105f39167d2488ac2caa43545007dee942bf8e179cbb81

File name: Download.exe

Detection ratio: 8 / 46

Analysis date: 2013-02-02 02:45:51 UTC (30 minutes ago)

More details

Analysis | Comments | Votes | Additional information

Antivirus	Result	Update
Agnitum	-	20130201
AhnLab-V3	-	20130201
AntiVir	Adware/InstallRex.A	20130201
Antiy-AVL	-	20130201
Avast	-	20130201
AVG	Suspicion: unknown virus	20130202
BitDefender	-	20130202
ByteHero	-	20130131
CAT-QuickHeal	-	20130201
ClamAV	-	20130202
Commtouch	-	20130202
Comodo	-	20130202
DrWeb	Adware.Downware.836	20130202
Emsisoft	-	20130202
eSafe	-	20130131
ESET-NOD32	Win32/InstalleRex.E.Gen	20130201
F-Prot	-	20130201

F-Secure	-	20130202
Fortinet	-	20130202
GData	-	20130202
Ikarus	-	20130201
Jiangmin	-	20121221
K7AntiVirus	Trojan	20130201
Kaspersky	-	20130201
Kingsoft	-	20130131
Malwarebytes	PUP.Offerware	20130201
McAfee	-	20130202
McAfee-GW-Edition	Heuristic.LooksLike.Win32.Suspicious.B	20130202
Microsoft	-	20130201
MicroWorld-eScan	-	20130202
NANO-Antivirus	-	20130202
Norman	-	20130201
nProtect	-	20130201
Panda	-	20130201
PCTools	-	20130202
Rising	-	20130201
Sophos	-	20130202
SUPERAntiSpyware	-	20130202
Symantec	-	20130202
TheHacker	-	20130131
TotalDefense	-	20130201
TrendMicro	-	20130202
TrendMicro-HouseCall	-	20130201
VBA32	-	20130201
VIPRE	Artua Vladislav (fs)	20130202
ViRobot	-	20130201

Some AV scanners detect, some don't. This could indicate that it is not outright malware, as in a virus or botnet, but still malicious/annoying enough that is it classified as malware. It could possibly be adware or spyware. Looking up the malware names listed in virus total, I do not find any readily available reports on this malware.

3) Strings

File: Download.exe MD5: 16d10cc8d62f2b851a041cb0e1c9df7c Size: 312424	
Ascii Strings: ---------- 0000004D !This program cannot be run in DOS mode. 000000C8 Rich 000001D8 .text 000001FF `.rdata 00000227 @.data 00000250 .rsrc 00000277 @.reloc 0000029F B.tsustub 000002C7 B.tsuarch	
.rdata:004030CC TSU Loader .rdata:00403154 Executable has no valid MZ signature .rdata:00403190 Error %u while retrieving entry point from %ls .rdata:004031C0 _TsuMainW@8 .rdata:004031CC Error %u while loading TSU.DLL %ls .rdata:004031F0 Error %u while extracting TSU.DLL to %ls .rdata:00403238 GetTempPath() failed => %u .rdata:00403254 Executable has no .tsustub section .rdata:00403278 .tsustub .rdata:00403284 GetModuleFileName() failed => %u .rdata:004032A8 This installer is for Windows 2000 and later .rdata:004033E2 HeapAlloc .rdata:004033EE HeapFree .rdata:004033FA OutputDebugStringA .rdata:00403410 lstrcpynW .rdata:0040341C UnmapViewOfFile .rdata:0040342E MultiByteToWideChar .rdata:00403444 MapViewOfFile .rdata:00403454 CloseHandle .rdata:00403462 CreateFileMappingW .rdata:00403478 GetFileSize .rdata:00403486 CreateFileW .rdata:00403494 lstrlenW .rdata:004034A0 GetCommandLineW .rdata:004034B2 ExitProcess .rdata:004034C0 Sleep .rdata:004034C8 DeleteFileW .rdata:004034D6 SetFileAttributesW	

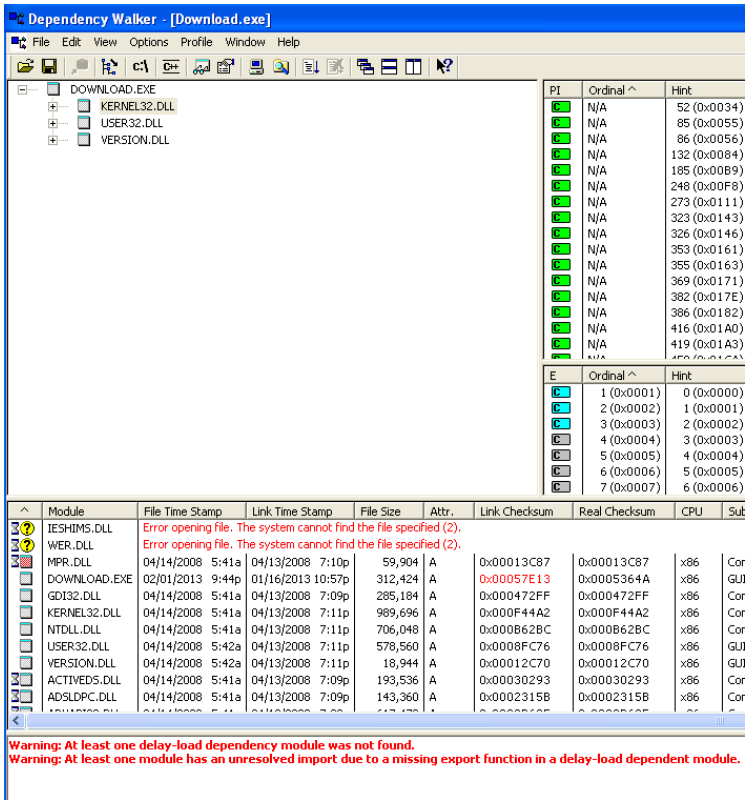
.rdata:004034EC GetFileAttributesW .rdata:00403502 FreeLibrary .rdata:00403510 GetProcAddress .rdata:00403522 LoadLibraryW .rdata:00403532 GetTempPathW .rdata:00403542 GetModuleHandleW .rdata:00403556 GetLastError .rdata:00403566 GetModuleFileNameW .rdata:0040357C GetTickCount .rdata:0040358C GetCurrentThreadId .rdata:004035A2 GetSystemTimeAsFileTime .rdata:004035BC GetCurrentProcessId .rdata:004035D2 GetProcessHeap .rdata:004035E4 ReadFile .rdata:004035F0 WriteFile .rdata:004035FC SetFileTime .rdata:0040360A SetFilePointer .rdata:0040361A KERNEL32.dll .rdata:0040362A MessageBoxA .rdata:00403638 wvsprintfA .rdata:00403646 wsprintfW .rdata:00403652 PostMessageW .rdata:00403660 USER32.dll .rdata:0040366E VerQueryValueW .rdata:00403680 GetFileVersionInfoW .rdata:00403696 GetFileVersionInfoSizeW .rdata:004036AE VERSION.dll .rdata:004036BC RSDS .rdata:004036D4 D:\Dev\Tin7\InstallDir\vc80-win32u\Loader.pdb .rsrc:0040525D xxxp .rsrc:004052FF wwwwwwwxp .rsrc:00405328 wwwwp .rsrc:00405340 """"/ .rsrc:004053D0 """"/ .rsrc:004053EF wwwwwwww .rsrc:00406C8F <?xml version="1.0" encoding="UTF-8" standalone="yes"?> .rsrc:00406CC8 <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0"> .rsrc:00406D14 <assemblyIdentity .rsrc:00406D29 name="Tarma.InstallMate7.Loader" .rsrc:00406D4D version="7.2.0.0" .rsrc:00406D62 type="win32" .rsrc:00406D72 processorArchitecture="*" .rsrc:00406D93 <description>Tarma InstallMate v7 Setup Loader</description> .rsrc:00406DD2 <dependency> .rsrc:00406DE2 <dependentAssembly>	-definitely look up this

.rsrc:00406DFA <assemblyIdentity .rsrc:00406E11 name="Microsoft.Windows.Common-Controls" .rsrc:00406E3F publicKeyToken="6595b64144ccf1df" .rsrc:00406E66 version="6.0.0.0" .rsrc:00406E7D type="win32" .rsrc:00406E8F processorArchitecture="*" .rsrc:00406EAE language="*" .rsrc:00406EC5 </dependentAssembly> .rsrc:00406EDC </dependency> .rsrc:00406EEC <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2"> .rsrc:00406F24 <security> .rsrc:00406F33 <requestedPrivileges> .rsrc:00406F4E <requestedExecutionLevel level="requireAdministrator"/> .rsrc:00406F8A </requestedPrivileges> .rsrc:00406FA4 </security> .rsrc:00406FB2 </trustInfo> .rsrc:00406FC0 </assembly> .rsrc:00406FCD PADPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDING	
0004B43E >0<0 0004B4D7 Salt Lake City1 0004B4F0 The USERTRUST Network1!0 0004B510 http://www.usertrust.com1 0004B533 UTN-USERFirst-Object0 0004B54B 110824000000Z 0004B55A 200530104838Z0{1 0004B581 Greater Manchester1 0004B59E Salford1 0004B5B0 COMODO CA Limited1!0 0004B5CC COMODO Code Signing CA 20 0004B661 "%jl 0004B6B8 O1[P! 0004B6FE w#*OY 0004B7A6 ;0907 0004B7B0 1http://crl.usertrust.com/UTN-USERFirst-Object.crl0t 0004B7EF h0f0= 0004B7FF 1http://crt.usertrust.com/UTNAddTrustObject_CA.crt0% 0004B83F http://ocsp.usertrust.com0 0004B879]ZB^ 0004B892 Y.yI 0004B89B mP5\ 0004B8D6 =q/; 0004B960 <a~^I 0004B9B4 Greater Manchester1 0004B9D1 Salford1 0004B9E3 COMODO CA Limited1!0	

0004B9FF COMODO Code Signing CA 20 0004BA1B 121115000000Z 0004BA2A 13111523595 9Z0 0004BA52 522331 0004BA62 center1 0004BA73 Ramat Gan1 0004BA87 Nahum 191 0004BA9A Moshe Karaso1 0004BAB1 Moshe Karaso0 0004BAE6 `~5z 0004BC79 ?0=0; 0004BC8C 0+0) 0004BC9C https://secure.comodo.net/CPS0A 0004BCC1 :0806 0004BCCB 0http://crl.comodoca.com/COMODOCodeSigningCA2.crl0r 0004BD09 f0d0< 0004BD19 0http://crt.comodoca.com/COMODOCodeSigningCA2.crt0$ 0004BD58 http://ocsp.comodoca.com0# 0004BD7D admin@starinstaller.info0 0004BED1 Greater Manchester1 0004BEEE Salford1 0004BF00 COMODO CA Limited1!0 0004BF1C COMODO Code Signing CA 2 0004BFF2 x'y, 0004C036 k~LX 0004C061 ~**.~ 0004C087 3eRS 0004C0B7 u:+f	
0004C0D8 <$ InstallerID="27275924" DownloadID="1627954648" ExternalID="0" PublisherID="686" SourceID="0" PageID="0" MutexID="" RegistryMutexID="" PayloadOffset="311512" PayloadSize="0" ExtractPayload="0" CountryCode="US" Language="EN" AffiliateID="" ServerName="BOX1" ServerUrl="http://i1.installbox1.info" ServerUrl1="http://i2.monitorbox1.info" ServerCfgUrl="http://c1.installbox1.info" ServerCfgUrl1="http://c2.monitorbox1.info" ServerReportUrl="http://r1.reportbox1.info" ServerReportUrl1="http://r2.monitorbox1.info" BrowserID="4" BrowserVersionID="3941311253" DomainID="159187051" RefererDomainID="2015894365" InstallerDate="2013/02/02" InstallerTime="1:48:37" ShowInTaskbar="1" InstallerMode="" QueryString="" ConfigQuery="installer_id=27275924&publisher_id=686&source_id=0&page_id=0&country_code=US&locale=EN&browser_id=4&download_id=1627954648&external_id=0" UserAgentID="1337450450" QueryStringID="0" $>	Network-based indicator

Unicode Strings: ---------- .rdata:004030D8 \StringFileInfo\%04x%04x\Arguments .rdata:00403120 \Var .rdata:0040312A ileInfo\Translation .rdata:0040317C /d:"%s" .rdata:0040321C Tsu%08lX.dll .rsrc:004056BC 333f3 .rsrc:00405748 f3fff .rsrc:0040647E VS_VERSION_INFO .rsrc:004064DA StringFileInfo .rsrc:004064FE 000004b0 .rsrc:00406516 ProductCode .rsrc:00406530 {C7FF08EC-CA52-4870-8A74-26E5A99CBA36} .rsrc:00406586 ProductName .rsrc:004065A0 RightClick .rsrc:0040662A ProductVersion .rsrc:004066D2 FileDescription .rsrc:004066F4 Installer .rsrc:0040670E FileVersion .rsrc:00406728 2013.1.31.1826 .rsrc:00406752 InternalName .rsrc:0040676C TSULoader .rsrc:00406786 OriginalFilename .rsrc:004067A8 TSULoader.exe - .rsrc:004067CA PackageCode .rsrc:004067E4 {7279D116-7CB6-47B0-A55B-3494A99AF3E0} .rsrc:0040683A Arguments .rsrc:004068DA SpecialBuild .rsrc:0040697E Comments .rsrc:00406990 WinNT (x86) Unicode Lib Rel .rsrc:004069CE CompanyName .rsrc:004069E8 RightClick .rsrc:00406A72 LegalCopyright .rsrc:00406A90 Copyright .rsrc:00406AA6 2012 RightClick .rsrc:00406B1A Email .rsrc:00406BB2 WebSite .rsrc:00406C52 rFileInfo .rsrc:00406C6E Translation	Possible host-based indicator Possible host-based indicator

4) Dependency Walker



a) Dependency walker offers warning of delay-load modules, could indicate run-time unpacking.

b) Two DLL's are reported missing: 1) IESHIMS.DLL 2) WER.DLL

These DLLs missing seem to be a common problem according to google search results.

Taken from a Microsoft forum:

"Ieshims.dll and wer.dll are only used on Vista and above machines for IE8, they are not needed in XP and thats why you can't find them. They can, however, be downloaded here:

http://www.dll-files.com/pop.php?dll=wer

http://www.dll-files.com/pop.php?dll=ieshims"

source: http://social.technet.microsoft.com/Forums/en-US/w7itproinstall/thread/8a751f65-ade9-4b8b-a3d3-c720ccbd3d2c/

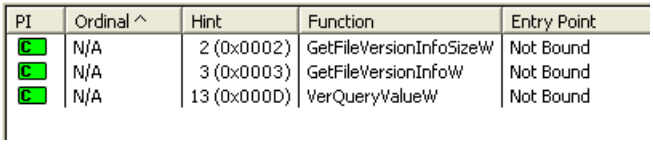
Kernel32.dll Exports:

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	52 (0x0034)	CloseHandle	Not Bound
C	N/A	85 (0x0055)	CreateFileMappingW	Not Bound
C	N/A	86 (0x0056)	CreateFileW	Not Bound
C	N/A	132 (0x0084)	DeleteFileW	Not Bound
C	N/A	185 (0x00B9)	ExitProcess	Not Bound
C	N/A	248 (0x00F8)	FreeLibrary	Not Bound
C	N/A	273 (0x0111)	GetCommandLineW	Not Bound
C	N/A	323 (0x0143)	GetCurrentProcessId	Not Bound
C	N/A	326 (0x0146)	GetCurrentThreadId	Not Bound
C	N/A	353 (0x0161)	GetFileAttributesW	Not Bound
C	N/A	355 (0x0163)	GetFileSize	Not Bound
C	N/A	369 (0x0171)	GetLastError	Not Bound
C	N/A	382 (0x017E)	GetModuleFileNameW	Not Bound
C	N/A	386 (0x0182)	GetModuleHandleW	Not Bound
C	N/A	416 (0x01A0)	GetProcAddress	Not Bound
C	N/A	419 (0x01A3)	GetProcessHeap	Not Bound
C	N/A	458 (0x01CA)	GetSystemTimeAsFileTime	Not Bound
C	N/A	470 (0x01D6)	GetTempPathW	Not Bound
C	N/A	479 (0x01DF)	GetTickCount	Not Bound
C	N/A	528 (0x0210)	HeapAlloc	Not Bound
C	N/A	534 (0x0216)	HeapFree	Not Bound
C	N/A	597 (0x0255)	LoadLibraryW	Not Bound
C	N/A	616 (0x0268)	MapViewOfFile	Not Bound
C	N/A	629 (0x0275)	MultiByteToWideChar	Not Bound
C	N/A	653 (0x028D)	OutputDebugStringA	Not Bound
C	N/A	693 (0x02B5)	ReadFile	Not Bound
C	N/A	794 (0x031A)	SetFileAttributesW	Not Bound
C	N/A	795 (0x031B)	SetFilePointer	Not Bound
C	N/A	799 (0x031F)	SetFileTime	Not Bound
C	N/A	854 (0x0356)	Sleep	Not Bound
C	N/A	881 (0x0371)	UnmapViewOfFile	Not Bound
C	N/A	932 (0x03A4)	WriteFile	Not Bound
C	N/A	970 (0x03CA)	lstrcpynW	Not Bound
C	N/A	973 (0x03CD)	lstrlenW	Not Bound

User32.dll Exports:

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	479 (0x01DF)	MessageBoxA	Not Bound
C	N/A	515 (0x0203)	PostMessageW	Not Bound
C	N/A	728 (0x02D8)	wsprintfW	Not Bound
C	N/A	729 (0x02D9)	wvsprintfA	Not Bound

Version.dll Exports:



PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	2 (0x0002)	GetFileVersionInfoSizeW	Not Bound
C	N/A	3 (0x0003)	GetFileVersionInfoW	Not Bound
C	N/A	13 (0x000D)	VerQueryValueW	Not Bound

No network functionality indicated in DLL imports. This contradicts strings found that indicate network connections. There is probably a dll that is loaded surreptitiously during run-time.

5) **Peid**
6) **PE View**
7) **….**
8) **…**

Cover all static tools that have been shown in the book up to this point. No need to use tools with redundant purposes.

Dynamic Analysis

1) **Process Explorer**
2) **ApateDNS**
3) **Wireshark**
4) **Procmon**
5) **Regshot**
6) **….**
7) **….**
8) **….**
9)

Cover all dynamic tools that have been shown in the book up to this point. No need to use tools with redundant purposes.

Do not include tools not covered in the book up to this point, i.e. IDA Pro, OllyDBG, or any disassembly. You will not receive more credit for including these. If you would

like to do additional analysis, I encourage you to do so, but do not include it in your report or presentation.