ID: 690704
Sample Name:
fdm_x64_setup.exe
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 08:38:21
Date: 26/08/2022
Version: 35.0.0 Citrine

Table of Contents

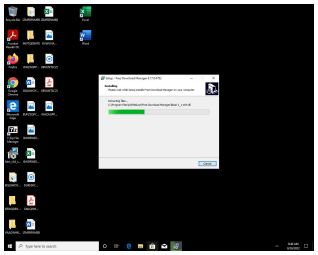
Windows Analysis Report

fdm_x64_setup.exe

Overview

General Information

Sample Name:	fdm_x64_setup.exe
Analysis ID:	690704
MD5:	31dd1d05a00ad4.
SHA1:	f8a33287bef3e72.
SHA256:	072ee364c81db9..
Infos:	



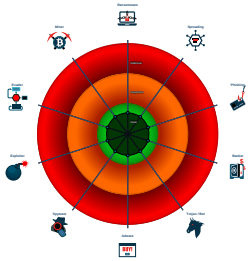
Detection

Score:	24
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Obfuscated command line found
- Uses schtasks.exe or at.exe to add…
- Uses 32bit PE files
- PE file contains strange resources
- Drops PE files
- PE file contains sections with non-s…
- Found dropped PE file which has no…

Classification



Process Tree

- **System is start**
- fdm_x64_setup.exe (PID: 184 cmdline: "C:\Users\alfredo\Desktop\fdm_x64_setup.exe" MD5: 31DD1D05A00AD4C3CBB94A8AF6726F98)
  - fdm_x64_setup.tmp (PID: 3892 cmdline: "C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp" /SL5="$2038C,34713263,780288,C:\Users\alfredo\Desktop\fdm_x64_setup.exe" MD5: 3C90C4DAABD5AFA78392EA879FA341A6)
    - schtasks.exe (PID: 3176 cmdline: "schtasks.exe" /end /tn FreeDownloadManagerHelperService MD5: 003D681048A63B9862C299F30492CFDF)
      - conhost.exe (PID: 2520 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: C5E9B1D1103EDCEA2E408E9497A5A88F)
- **cleanup**

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Data Obfuscation

Obfuscated command line found

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

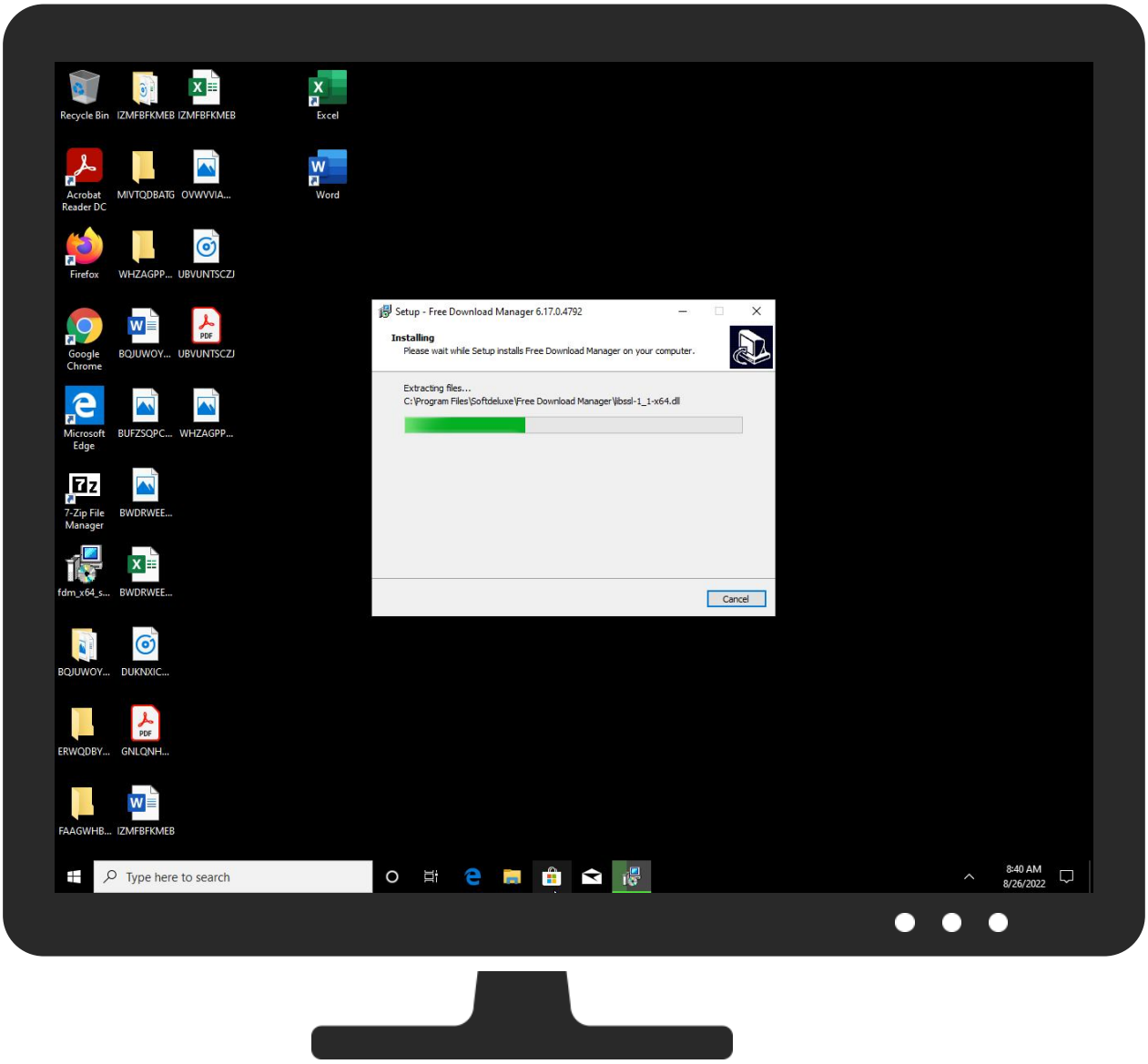
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Command and Scripting Interpreter	1 Scheduled Task/Job	1 Process Injection	3 Masquerading	OS Credential Dumping	2 System Owner/User Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Non-Application Layer Protocol	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Process Injection	LSASS Memory	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
fdm_x64_setup.exe	0%	Virustotal		Browse
fdm_x64_setup.exe	0%	Metadefender		Browse
fdm_x64_setup.exe	0%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp	0%	Virustotal		Browse
C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp	2%	ReversingLabs		
C:\Users\alfredo\AppData\Local\Temp\is-IHEBO.tmp_isetup_setup64.tmp	0%	Virustotal		Browse
C:\Users\alfredo\AppData\Local\Temp\is-IHEBO.tmp_isetup_setup64.tmp	0%	Metadefender		Browse
C:\Users\alfredo\AppData\Local\Temp\is-IHEBO.tmp_isetup_setup64.tmp	0%	ReversingLabs		
C:\Program Files\Softdeluxe\Free Download Manager\is-0BB6O.tmp	0%	Virustotal		Browse
C:\Program Files\Softdeluxe\Free Download Manager\is-0BB6O.tmp	0%	Metadefender		Browse
C:\Program Files\Softdeluxe\Free Download Manager\is-0BB6O.tmp	0%	ReversingLabs		
C:\Program Files\Softdeluxe\Free Download Manager\is-4DDA0.tmp	0%	Virustotal		Browse
C:\Program Files\Softdeluxe\Free Download Manager\is-4DDA0.tmp	0%	Metadefender		Browse
C:\Program Files\Softdeluxe\Free Download Manager\is-4DDA0.tmp	0%	ReversingLabs		
C:\Program Files\Softdeluxe\Free Download Manager\is-7CG1Q.tmp	0%	Virustotal		Browse
C:\Program Files\Softdeluxe\Free Download Manager\is-7CG1Q.tmp	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Program Files\Softdeluxe\Free Download Manager\is-7CG1Q.tmp	0%	ReversingLabs		
C:\Program Files\Softdeluxe\Free Download Manager\is-8OREA.tmp	0%	Virustotal		Browse
C:\Program Files\Softdeluxe\Free Download Manager\is-8OREA.tmp	0%	Metadefender		Browse
C:\Program Files\Softdeluxe\Free Download Manager\is-8OREA.tmp	0%	ReversingLabs		
C:\Program Files\Softdeluxe\Free Download Manager\is-AA7GK.tmp	0%	Metadefender		Browse
C:\Program Files\Softdeluxe\Free Download Manager\is-AA7GK.tmp	0%	ReversingLabs		
C:\Program Files\Softdeluxe\Free Download Manager\is-RG2KI.tmp	0%	Metadefender		Browse
C:\Program Files\Softdeluxe\Free Download Manager\is-RG2KI.tmp	0%	ReversingLabs		
C:\Program Files\Softdeluxe\Free Download Manager\is-VEVHM.tmp	0%	Metadefender		Browse
C:\Program Files\Softdeluxe\Free Download Manager\is-VEVHM.tmp	0%	ReversingLabs		
C:\Program Files\Softdeluxe\Free Download Manager\ffmpeg.exe (copy)	2%	ReversingLabs		
C:\Program Files\Softdeluxe\Free Download Manager\helperservice.exe (copy)	0%	ReversingLabs		
C:\Program Files\Softdeluxe\Free Download Manager\importwizard.exe (copy)	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.16.205	true	false		high
www.freedownloadmanager.org	199.101.132.243	true	false		high
clients.l.google.com	142.250.186.46	true	false		high
clients2.google.com	unknown	unknown	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	690704
Start date and time:	2022-08-26 08:38:21 +02:00
Joe Sandbox Product:	CloudBasic
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fdm_x64_setup.exe
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1

Technologies:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Detection:	SUS
Classification:	sus24.winEXE@6/26@3/0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 142.251.36.131, 34.104.35.123
- Excluded domains from analysis (whitelisted): fs.microsoft.com, login.live.com, slscr.update.microsoft.com, nexusrules.officeapps.live.com
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: C:\Program Files\Softdeluxe\Free Download Manager\is-AA7GK.tmp

Created / dropped Files

C:\Program Files\Softdeluxe\Free Download Manager\api-ms-win-crt-locale-l1-1-0.dll (copy)

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	19136
Entropy (8bit):	7.03021960345049
Encrypted:	false
SSDEEP:	
MD5:	1D821D741CFAF0D322F2483114D93188
SHA1:	AA6ECD604D207BBAE869225A1A7738433A4417D6
SHA-256:	9B299B18FE97191E3875D173B2D89295CFA8D006A0C9328FAE867B8DA9BDC23B
SHA-512:	3FF35106664FED3746DC00ED0BF85DB853B047F736708C9A2587D9550581642A6837F1FF4A0275C54A42F6033FBD7567B233D3F832F25A241B321820BFF8A971
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m2..)S..)S..)S....].(S....A.+S....^.(S....C.(S..Rich)S..... .....PE..d....3.V....." .....0.....C.....`.....`...e..... .....<.....8..... .....rdata..|.....@..@.rsrc..... .....@..@..... ....

C:\Program Files\Softdeluxe\Free Download Manager\api-ms-win-crt-math-l1-1-0.dll (copy)

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	27840
Entropy (8bit):	6.631308224366814
Encrypted:	false
SSDEEP:	
MD5:	79878844B0A1EB2B621286DAD20BC4AB
SHA1:	A64CFD5F9424BAD329E2578168EE58A11CE14F36
SHA-256:	177779FF31D2977EA5BB583D3FC50209EDB64BBCE8C40D6D14E34EA4446266E3
SHA-512:	960A8D1CF1C447A77EB90ECF1E8171C8E01D6933B04EC18ACB0F7BBFECEBDFF5CB3C972B9ACE75715D2DFCB5FAF4DE7ECFE56B059FF8E1255272257EF905E35D
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m2..)S..)S..)S....].(S....A.+S....^.(S....C.(S..Rich)S..... .....PE..d....2.V....." .....,.....P.....`.....`....%.....@.....0...<.....8..... .....rdata...&.....(.....@..@.rsrc.....@.....,.....@..@..... ....

C:\Program Files\Softdeluxe\Free Download Manager\api-ms-win-crt-multibyte-l1-1-0.dll (copy)

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	26816
Entropy (8bit):	6.638936609977177
Encrypted:	false
SSDEEP:	
MD5:	A00B5CCB162606D61FBDB843D6EC0253
SHA1:	31C9BF8A87921C0FFBEC8BB882A0F48C16F10870
SHA-256:	E4152A6D181F5EBBD79EBF0F441D95073AA0AAAC8F5A6C77D9AB4AB17CFC353E
SHA-512:	F24471575B26F5C7C9B0AF19370B7A602B9273A599782C6591B0D7F99559B66EF0DEB4958B33EA12E65E24CB1FEFE92CC96A9924EF22933002B523F507B69592
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m2..)S..)S..)S....].(S....A.+S....^.(S....C.(S..Rich)S..... .....PE..d....3.V....." .....(.....P.....2....`.....`... .....@.....,...<.....8..... .....rdata..`."....$.....@..@.rsrc.....@.....(.....@..@..... ....

C:\Program Files\Softdeluxe\Free Download Manager\api-ms-win-crt-private-l1-1-0.dll (copy)

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	70848
Entropy (8bit):	5.845606084443252
Encrypted:	false
SSDEEP:	
MD5:	A9208707FFA4DCF42EB46CF117B9B4A5
SHA1:	D94DCD936D8D67FC963F0982FBC3EC118DA678D2
SHA-256:	680FD6211BFA8F0B591307D883410CFC3240702399E3C86B72213593F0E52216
SHA-512:	29668847EB615067BAF74EC2561D8B93F8EA0EFB42B04186F51B550AF538002E391A3C21A9DD5B1C87AC59D328D13C0367841F7D58C1CBBB9F2145FF8CBA7E8B
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m2..)S..)S..)S....].(S....A.+S....^.(S....C.(S..Rich)S..... .....PE..d....3.V....." .....p....`.....`.....<.....8..... .....rdata.....@..@.rsrc.....@..@..... ....

C:\Program Files\Softdeluxe\Free Download Manager\api-ms-win-crt-process-l1-1-0.dll (copy)

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	19648
Entropy (8bit):	6.971375962852365
Encrypted:	false
SSDEEP:	
MD5:	3D03D568767B6CB87B64952A3D6186A2
SHA1:	C7BD25D3DD98EC2EA9775B05D01208F1097D7B42
SHA-256:	59752E277397617768DA4B76F3A839A7C9280C20AB3FE7BE30DE71399FC4440F
SHA-512:	39488BAEC9E08E851B26DF29146A04276CCDD4E246931CADE496C38EF14A39E6FE59F5F1CA75923EB24790277C955502B9FFEDBA6D77458C5145719E5EE2E617
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m2..)S..)S..)S....].(S....A.+S....^.(S....C.(S..Rich)S..... .....PE..d...E3.V....." .....0.....`.....`...x..... .....<.....8..... .....rdata.....@..@.rsrc..... .....@..@..... ....

C:\Program Files\Softdeluxe\Free Download Manager\api-ms-win-crt-runtime-l1-1-0.dll (copy)

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp

File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	23232
Entropy (8bit):	6.845632510878297
Encrypted:	false
SSDEEP:	
MD5:	3C2162F8F05B362DDA8814505C555312
SHA1:	2BBCBB984C909ADA3CE8CC37BD910375C2D806F4
SHA-256:	B5A3C4681FF8C09CCF32E0E0BF7D183293B5171BBB6512FDB90585D6D88FBD70
SHA-512:	CA268CC8DC39BF025AA7612C4CBECC18CB8FCE30855C76E46C6524243C52ED4DAA34BD75B99A65C2FA46EAA1AA302B33BDC84630A074D53B91153A89B4539ADE
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m2..)S..)S..)S....].(S....A.+S....^.(S....C.(S..Rich)S..... .....PE..d...a4.V....." .....@.....[.....`.....`...4.....0.....<.....8..... .....rdata..H.....@..@.rsrc.....0.....@..@.....

C:\Program Files\Softdeluxe\Free Download Manager\api-ms-win-crt-stdio-l1-1-0.dll (copy)

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	24768
Entropy (8bit):	6.787542966815604
Encrypted:	false
SSDEEP:	
MD5:	759606F25742C0D3252A3B6BCF7A0098
SHA1:	6F395025343BEB970FB06207101D01A4144133BF
SHA-256:	E3C4E66BE42BDBA47B3186F1935BF852620B9F6C507CF56321E21714814D1EA2
SHA-512:	0D5A35780098620E275AA82BB962F5C1B85CAAC1EEA2A52C83B6963B002FAAAF5D25F5EF78B93F530E75329D33CC6297059DF2ED00624EE9A6EAED856E2D3C70
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m2..)S..)S..)S....].(S....A.+S....^.(S....C.(S..Rich)S..... .....PE..d....3.V....." ....@.....(Y....`.....`...a.....0.....$...<.....8..... .....rdata..t.....@..@.rsrc.....0..... .....@..@.....

C:\Program Files\Softdeluxe\Free Download Manager\ffmpeg.exe (copy)

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	23535104
Entropy (8bit):	6.004593158735539
Encrypted:	false
SSDEEP:	
MD5:	2209A1213CA2DBC6DEA064C67204DB32
SHA1:	92427997C3578BB2B99A93AD68C6D2A1C9A971FA
SHA-256:	F659DA0CAB01498EF177B152271F4B708E257AF237B2B81DA8AB6BE0132554F6
SHA-512:	E258AC82F62E2418D476AFBCB10F74D118A05CBF87EF5210D5B958B8CEC89B17A4047871B3731DE304C601A27D2B42022B26C968A09CDEB834BE6C2336C8528
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....].....dZ..... ...m.....m.....Rich.....PE..d....56`....."....4.....-.....@.....0/.....`.....*.....#.....P,..N....F.8..... .....@.F.....*.....text..... ..`.rdata...t[.....v[.....@..@.data...i....pU.....LU.....@....pdata.....#.....([.....@..@.idata..4@....*..B....b.....@..@.gfids..,.....+.....*c.....@..@_RDATA..... +.....,c.....@..@.00cfg.....@,.....Bd.....@..@.reloc.....P,.....Dd.....@..B....

C:\Program Files\Softdeluxe\Free Download Manager\helperservice.exe (copy)

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	128000
Entropy (8bit):	6.057392627980159
Encrypted:	false
SSDEEP:	
MD5:	EB755F6B7C0799011E18B1B769DC0EBE
SHA1:	510E8E65DFFDDC491A280BCDCEE31D4BF4F4E689
SHA-256:	11426FFEEE740B20CF9837E5B23A7BB3918EB0DB70676392D9A798DF9DC138B0
SHA-512:	EDE8CC54B80F72914B15CB2F0008CCABE9C8D93C850F0BB49AA20400A9F71C19EF1E68D47AA726A547A52A6C00FF858B2E5B5BED7E3BDE9F13603F9D1381B 7F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....D..$..`w..`w..`w...w..`wR.dv..`wR.cv..`wR.ev..`wR.av..`w..av.. `w..av..`w..aw..`w..ev..`w...w..`w...w..`w..bv..`wRich..`w.....PE..d....A.b....."....:..... *.....@.....@.....`..... (...|.... .....$.....0.....j..T.....l..(...@k..8.....P.....text...$8....:..... ..`.rdata..|....P.....>.....@..@.data...h..... ..@....pdata..$.....@..@.rsrc..... .....@..@.reloc.....0.....@..B..... .....

C:\Program Files\Softdeluxe\Free Download Manager\importwizard.exe (copy)	
Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	727040
Entropy (8bit):	6.354851680841405
Encrypted:	false
SSDEEP:	
MD5:	413453B7CEB7A76ACA79121F9CB8CCF2
SHA1:	FDA4BF0D9EE5CF1B043A24FFAC154EBA1797F5DA
SHA-256:	4EE94E78AB0148EBD4CE623BC225D49E8DB85F363B976EBA4D8FF9AFAFC66120
SHA-512:	0BE51A1629EC4FC008E4CDF5649CBA66EAE746992D1D9A90EF4AA43A8E0DABD3793A25234A3A287A5EEA22117BC5097595538891A57CD084A7B550941A06ED CA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k-GS/L)./L)./L).&4..!L).}9-.%L).}9*.+L).}9,..L).}9(.)L)..%(.%L).;'(.!L). .9(.(L)./L(._O)..9,..L)..9...L)./L...L)..9+..L).Rich/L).....PE..d...<B.b....."....h.....@.....p.....`.....P.... .....U.....`.....Xw..T.....y..(....w..8.....@.....text...X..... ..`.rdata...o.....p.....@..@.data...0....P...x...<.....@....pda ta...U.....V.....@..@.rsrc.....P.....@..@.reloc.....`.....@..B..... .....

C:\Program Files\Softdeluxe\Free Download Manager\is-0BB6O.tmp	
Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	70848
Entropy (8bit):	5.845606084443252
Encrypted:	false
SSDEEP:	
MD5:	A9208707FFA4DCF42EB46CF117B9B4A5
SHA1:	D94DCD936D8D67FC963F0982FBC3EC118DA678D2
SHA-256:	680FD6211BFA8F0B591307D883410CFC3240702399E3C86B72213593F0E52216
SHA-512:	29668847EB615067BAF74EC2561D8B93F8EA0EFB42B04186F51B550AF538002E391A3C21A9DD5B1C87AC59D328D13C0367841F7D58C1CBBB9F2145FF8CBA7E8 B
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m2..)S..)S..)S....].(S....A.+S....^.(S....C.(S..Rich)S..... .....PE..d....3.V..... .....rdata.....@..@.rsrc.....@..@..... ....

C:\Program Files\Softdeluxe\Free Download Manager\is-2M2DR.tmp

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	727040
Entropy (8bit):	6.354851680841405
Encrypted:	false
SSDEEP:	
MD5:	413453B7CEB7A76ACA79121F9CB8CCF2
SHA1:	FDA4BF0D9EE5CF1B043A24FFAC154EBA1797F5DA
SHA-256:	4EE94E78AB0148EBD4CE623BC225D49E8DB85F363B976EBA4D8FF9AFAFC66120
SHA-512:	0BE51A1629EC4FC008E4CDF5649CBA66EAE746992D1D9A90EF4AA43A8E0DABD3793A25234A3A287A5EEA22117BC5097595538891A57CD084A7B550941A06EDCA
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k-GS/L)./L)./L).&4..!L).}9-.%L).}9*.+L).}9,..L).}9(.)L)..%(.%L).;'(.!L). .9(.(L)./L(._O)..9,..L)..9...L)./L...L)..9+..L).Rich/L).....PE..d...<B.b.....".....h.....@.....p.....`.....P.... .....U.....`.....Xw..T.....y..(....w..8.....@.....text...X..... ..`.rdata...o.....p.....@..@.data...0....P...x...<.....@....pdata...U.....V.....@..@.rsrc.....P.....@..@.reloc.....`.....@..B..... .....

C:\Program Files\Softdeluxe\Free Download Manager\is-4DDA0.tmp

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	26816
Entropy (8bit):	6.638936609977177
Encrypted:	false
SSDEEP:	
MD5:	A00B5CCB162606D61FBDB843D6EC0253
SHA1:	31C9BF8A87921C0FFBEC8BB882A0F48C16F10870
SHA-256:	E4152A6D181F5EBBD79EBF0F441D95073AA0AAAC8F5A6C77D9AB4AB17CFC353E
SHA-512:	F24471575B26F5C7C9B0AF19370B7A602B9273A599782C6591B0D7F99559B66EF0DEB4958B33EA12E65E24CB1FEFE92CC96A9924EF22933002B523F507B69592
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m2..)S..)S..)S....].(S....A.+S....^.(S....C.(S..Rich)S..... .....PE..d....3.V.....(.....P.....2....`.....`.... .....@.....,..<.....8..... .....rdata...".....$.....@..@.rsrc.....@.....(.....@..@..... ....

C:\Program Files\Softdeluxe\Free Download Manager\is-7CG1Q.tmp

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	19136
Entropy (8bit):	7.03021960345049
Encrypted:	false
SSDEEP:	
MD5:	1D821D741CFAF0D322F2483114D93188
SHA1:	AA6ECD604D207BBAE869225A1A7738433A4417D6
SHA-256:	9B299B18FE97191E3875D173B2D89295CFA8D006A0C9328FAE867B8DA9BDC23B
SHA-512:	3FF35106664FED3746DC00ED0BF85DB853B047F736708C9A2587D9550581642A6837F1FF4A0275C54A42F6033FBD7567B233D3F832F25A241B321820BFF8A971
Malicious:	false

Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m2..)S..)S..)S....].(S....A.+S....^.(S....C.(S..Rich)S..... .....PE..d....3.V....." .....0.....C.....`.....`...e..... .....<.....8..... .....rdata..|.....@..@.rsrc..... .....@..@..... ....

C:\Program Files\Softdeluxe\Free Download Manager\is-8OREA.tmp

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	27840
Entropy (8bit):	6.631308224366814
Encrypted:	false
SSDEEP:	
MD5:	79878844B0A1EB2B621286DAD20BC4AB
SHA1:	A64CFD5F9424BAD329E2578168EE58A11CE14F36
SHA-256:	177779FF31D2977EA5BB583D3FC50209EDB64BBCE8C40D6D14E34EA4446266E3
SHA-512:	960A8D1CF1C447A77EB90ECF1E8171C8E01D6933B04EC18ACB0F7BBFECEBDFF5CB3C972B9ACE75715D2DFCB5FAF4DE7ECFE56B059FF8E1255272257EF905E35D
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m2..)S..)S..)S....].(S....A.+S....^.(S....C.(S..Rich)S..... .....PE..d....2.V....." .....,.....P.....`.....`....%.....@.....0...<.....8..... .....rdata...&.....(.....@..@.rsrc.....@.....,.....@..@..... ....

C:\Program Files\Softdeluxe\Free Download Manager\is-9O60R.tmp

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2858496
Entropy (8bit):	5.901039372404442
Encrypted:	false
SSDEEP:	
MD5:	8BF7134FD7C7B9F79FBAA46A820565FD
SHA1:	C82732C10A0F03EF1868D2CA6A8C42EC430A8A02
SHA-256:	A8F38398B8E95919CE4F4EB4CE9E2DB432B5B8DA00B531E2F1633795B3FA622A
SHA-512:	9D48C50A08236DF337ACE9F7546D3DB392D980D6B86111DA0F1B72848D9A7E74AA05EC9EB83F35C4C0570334F5C3B8460E1864EB2AD9A7FF5DC67D0206616E1
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b.....@...@...@.{f@...@.v.A...@.v.A...@.v.A...@.v.A...@...@3. .@~q.A...@.v.A...@.v.A...@.v.A...@.v.@...@.v.A...@Rich...@.....PE..d...I.Gb....." ....8.....P,.....`..... &.mg...+.@.....+.|.....).....+.pN...Z$.8.....Z$.8.....+.....text...D6.....8..... ..`.rdata..=....P.....<.....@..@.data...Aw...@) ..*...).....@....pdata..L.....).....J).....@..@.idata..8#....+..$....*.....@..@.00cfg..Q.....+....."+.....@..@.rsrc...|.....+.....$+.....@..@.reloc...q....+..r...,+.. .....@..B.....

C:\Program Files\Softdeluxe\Free Download Manager\is-AA7GK.tmp

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	23232
Entropy (8bit):	6.845632510878297
Encrypted:	false
SSDEEP:	
MD5:	3C2162F8F05B362DDA8814505C555312

SHA1:	2BBCBB984C909ADA3CE8CC37BD910375C2D806F4
SHA-256:	B5A3C4681FF8C09CCF32E0E0BF7D183293B5171BBB6512FDB90585D6D88FBD70
SHA-512:	CA268CC8DC39BF025AA7612C4CBECC18CB8FCE30855C76E46C6524243C52ED4DAA34BD75B99A65C2FA46EAA1AA302B33BDC84630A074D53B91153A89B4539ADE
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m2..)S..)S..)S....].(S....A.+S....^.(S....C.(S..Rich)S..... .....PE..d...a4.V....." .....@.....[....`.....`...4.....0.....<.....8..... .....rdata..H.....@..@.rsrc.....0.....@..@..... ....

C:\Program Files\Softdeluxe\Free Download Manager\is-B3NPD.tmp	
Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	23535104
Entropy (8bit):	6.004593158735539
Encrypted:	false
SSDEEP:	
MD5:	2209A1213CA2DBC6DEA064C67204DB32
SHA1:	92427997C3578BB2B99A93AD68C6D2A1C9A971FA
SHA-256:	F659DA0CAB01498EF177B152271F4B708E257AF237B2B81DA8AB6BE0132554F6
SHA-512:	E258AC82F62E2418D476AFBCB10F74D118A05CBF87EF5210D5B958B8CEC89B17A4047871B3731DE304C601A27D2B42022B26C968A09CDEB834BE6C2336C8528
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....].....dZ..... ...m.....m.....Rich.....PE..d....56`....."....4.....-.....@.....0/.....`.....*.....#.....P,..N....F.8..... .....@.F.....*.....text..... ..`.rdata...t[.....v[.....@..@.data...i....pU.....LU.....@....pdata.....#.....([.....@..@.idata..4@....*..B....b.....@..@.gfids..,.....+.....*c.....@..@_RDATA..... +.....,c.....@..@.00cfg.....@,.....Bd.....@..@.reloc.....P,.....Dd.....@..B.... .....

C:\Program Files\Softdeluxe\Free Download Manager\is-G7439.tmp	
Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	128000
Entropy (8bit):	6.057392627980159
Encrypted:	false
SSDEEP:	
MD5:	EB755F6B7C0799011E18B1B769DC0EBE
SHA1:	510E8E65DFFDDC491A280BCDCEE31D4BF4F4E689
SHA-256:	11426FFEEE740B20CF9837E5B23A7BB3918EB0DB70676392D9A798DF9DC138B0
SHA-512:	EDE8CC54B80F72914B15CB2F0008CCABE9C8D93C850F0BB49AA20400A9F71C19EF1E68D47AA726A547A52A6C00FF858B2E5B5BED7E3BDE9F13603F9D1381B17F
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....D..$..`w..`w..`w...w..`wR.dv..`wR.cv..`wR.ev..`wR.av..`w..av.. `w..av..`w..aw..`w..ev..`w...w..`w...w..`w..bv..`wRich..`w.....PE..d....A.b....."....:..... *.....@.....@.....`..... (...|.... .....$.....0.....j..T.....l..(...@k..8.....P.....text...$8.....:..... ..`.rdata..|....P.....>.....@..@.data...h..... ..@....pdata..$.....@..@.rsrc..... .....@..@.reloc.....0.....@..B..... .....

C:\Program Files\Softdeluxe\Free Download Manager\is-GTRN5.tmp	
Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	27824
Entropy (8bit):	6.216402056909113
Encrypted:	false
SSDEEP:	

MD5:	185C660A9F1BEC716A5D8CEAA936AE9E
SHA1:	1C6AC11BD9803BF293B0115F32D17E6F3B2715A5
SHA-256:	D2A16238E769A4554FC2BCBB50521BDCC92E128B2F2C0B9AD2ED55104D79A3EF
SHA-512:	7F8E89CD866FFDF5BA8D8C7312B15296801FB60EEC94E5144128FE86344B019639B00DF3C786A9019EFC2CA851365767F9673F5BC5551D1BB8C5694B96FA7B8F
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S.nA2.=A2.=A2.=HJ~=C2.=.Z.<C2.=.Z.<C2.=.Z.<K2.=.Z.<F2.=.Z.<@2.=.[.<B2.=A2.=$2.=.[.<@2.=.[.<@2.=.[.=@2.=A2z=@2.=.[.<@2.=RichA2.=.....PE..d.....a....." .....0.....^....`.....8.....A..d.....H....p..h....F...&.....3..T.....3.....0.....text..... ..`.rdata...#...0...$.....@..@.data.....`.....:.....@....pdata..h....p.....<.....@..@.rsrc...H.....>.....@..@.reloc.....D.....@..B.....

C:\Program Files\Softdeluxe\Free Download Manager\is-RG2KI.tmp

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	24768
Entropy (8bit):	6.787542966815604
Encrypted:	false
SSDEEP:	
MD5:	759606F25742C0D3252A3B6BCF7A0098
SHA1:	6F395025343BEB970FB06207101D01A4144133BF
SHA-256:	E3C4E66BE42BDBA47B3186F1935BF852620B9F6C507CF56321E21714814D1EA2
SHA-512:	0D5A35780098620E275AA82BB962F5C1B85CAAC1EEA2A52C83B6963B002FAAAF5D25F5EF78B93F530E75329D33CC6297059DF2ED00624EE9A6EAED856E2D3C70
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m2..)S..)S..)S....].(S....A.+S....^.(S....C.(S..Rich)S.....PE..d....3.V....." ....@.....(Y....`.....`...a.....0.....$...<.....8.....rdata..t.....@..@.rsrc.....0..... .....@..@.....

C:\Program Files\Softdeluxe\Free Download Manager\is-VEVHM.tmp

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	19648
Entropy (8bit):	6.971375962852365
Encrypted:	false
SSDEEP:	
MD5:	3D03D568767B6CB87B64952A3D6186A2
SHA1:	C7BD25D3DD98EC2EA9775B05D01208F1097D7B42
SHA-256:	59752E277397617768DA4B76F3A839A7C9280C20AB3FE7BE30DE71399FC4440F
SHA-512:	39488BAEC9E08E851B26DF29146A04276CCDD4E246931CADE496C38EF14A39E6FE59F5F1CA75923EB24790277C955502B9FFEDBA6D77458C5145719E5EE2E617
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m2..)S..)S..)S....].(S....A.+S....^.(S....C.(S..Rich)S.....PE..d...E3.V....." .....0.....`.....`...x..... .....<.....8.....rdata.....@..@.rsrc..... .....@..@.....

C:\Program Files\Softdeluxe\Free Download Manager\libEGL.dll (copy)

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	27824
Entropy (8bit):	6.216402056909113

Encrypted:	false
SSDEEP:	
MD5:	185C660A9F1BEC716A5D8CEAA936AE9E
SHA1:	1C6AC11BD9803BF293B0115F32D17E6F3B2715A5
SHA-256:	D2A16238E769A4554FC2BCBB50521BDCC92E128B2F2C0B9AD2ED55104D79A3EF
SHA-512:	7F8E89CD866FFDF5BA8D8C7312B15296801FB60EEC94E5144128FE86344B019639B00DF3C786A9019EFC2CA851365767F9673F5BC5551D1BB8C5694B96FA7B8F
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S.nA2.=A2.=A2.=HJ~=C2.=.Z.<C2.=.Z.<C2.=.Z.<K2.=.Z.<F2.=.Z.<@2.=.[.<B2.=A2.=$2.=.[.<@2.=.[.<@2.=.[.=@2.=A2z=@2.=.[.<@2.=RichA2.=.....PE..d.....a....." .....0.....^.....`.....8.....A..d.....H....p..h....F...&.....3..T.....3.....0.....text..... ..`.rdata...#...0...$.....@..@.data.....`.....:.....@....pdata..h....p.....<.....@..@.rsrc...H.....>.....@..@.reloc.....D.....@..B.....

C:\Program Files\Softdeluxe\Free Download Manager\libcrypto-1_1-x64.dll (copy)

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2858496
Entropy (8bit):	5.901039372404442
Encrypted:	false
SSDEEP:	
MD5:	8BF7134FD7C7B9F79FBAA46A820565FD
SHA1:	C82732C10A0F03EF1868D2CA6A8C42EC430A8A02
SHA-256:	A8F38398B8E95919CE4F4EB4CE9E2DB432B5B8DA00B531E2F1633795B3FA622A
SHA-512:	9D48C50A08236DF337ACE9F7546D3DB392D980D6B86111DA0F1B72848D9A7E74AA05EC9EB83F35C4C0570334F5C3B8460E1864EB2AD9A7FF5DC67D0206616E 1
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b.....@...@...@.{f@...@.v.A...@.v.A...@.v.A...@.v.A...@...@3. .@~q.A...@.v.A...@.v.A...@.v.A...@.v.@...@.v.A...@Rich...@.....PE..d...I.Gb....." .....8.....P,.....`..... &.mg...+.@.....+.|.....).....+.pN...Z$.8.....Z$.8.....+.....text...D6.....8..... ..`.rdata..=....P.....<.....@..@.data...Aw...@) ..*...).....@....pdata..L.....).....J).....@..@.idata..8#....+..$....*.....@..@.00cfg..Q.....+.....'+.....@..@.rsrc...|.....+.....$+.....@..@.reloc...q....+..r...,+.. .....@..B.....

C:\Users\alfredo\AppData\Local\Temp\is-IHEBO.tmp_isetup_setup64.tmp

Process:	C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.720366600008286
Encrypted:	false
SSDEEP:	
MD5:	E4211D6D009757C078A9FAC7FF4F03D4
SHA1:	019CD56BA687D39D12D4B13991C9A42EA6BA03DA
SHA-256:	388A796580234EFC95F3B1C70AD4CB44BFDDC7BA0F9203BF4902B9929B136F95
SHA-512:	17257F15D843E88BB78ADCFB48184B8CE22109CC2C99E709432728A392AFAE7B808ED32289BA397207172DE990A354F15C2459B6797317DA8EA18B040C85787E
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^.....I.....=\.....=\.....=\.....Rich.....PE.. d.....R.....#.....@.....`.....<!.....P..H....@..0..... ..... .....text..... ..`.rdata..|.... .....@..@.data.....0.....@....pdata..0....@.....@..@.rsrc...H....P.....@..@..... ....

C:\Users\alfredo\AppData\Local\Temp\is-N1RHV.tmp\fdm_x64_setup.tmp

Process:	C:\Users\alfredo\Desktop\fdm_x64_setup.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2570752

Entropy (8bit):	6.387948436036898
Encrypted:	false
SSDEEP:	
MD5:	3C90C4DAABD5AFA78392EA879FA341A6
SHA1:	F45D424B3D9D859D3524AFFE5D2EDEB5FF2C81BC
SHA-256:	C9DCF0E3F679469EE4A35083A115C671C37BE19E7EC5721E1F2F3FF1F6E09B0C
SHA-512:	A6E33FBB48C80F8CACB23CCAD2BAC1C4EA27F665447F22A6E45F1135687BBDBA5752FCE4D33B9374E1E3C4AC793548B7C188A4B2DC10C88ABE3C3CE36B42 10A
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	low
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L.....m^.....%.....%.....%...@..... (.....@.....@.....'.....&..5...0'..... '..... ..L.&.H.....&.....text.....%.....%..... ..`.itext...&....%..(....%..... ..`.data...dZ....%..\....%.....@....bss.....x...0&.....idata...5....&..6....&... .....@....didata.....&.....@&.....@....edata.....'.....J&.....@..@.tls....D.....'.....rdata..]..... '.....L&.....@..@.rsrc.....0'.....N&.....@..@..... ..... (.....:'.....@..@.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.996840948426598
TrID:	• Win32 Executable (generic) a (10002005/4) 98.04% • Inno Setup installer (109748/4) 1.08% • InstallShield setup (43055/19) 0.42% • Win32 EXE PECompact compressed (generic) (41571/9) 0.41% • Win16/32 Executable Delphi generic (2074/23) 0.02%
File name:	fdm_x64_setup.exe
File size:	35460872
MD5:	31dd1d05a00ad4c3cbb94a8af6726f98
SHA1:	f8a33287bef3e721d52f6b8152822bbdc9a9c3a8
SHA256:	072ee364c81db95d8f45c8d06037cba332cd004d3b8290ee435b369f7becb829
SHA512:	05104bb79d18c4f948a471119dff470c9efdec4a3c15d2e40f34ab759d2cec2996a496a1219a9ca8294520f12e77230a614ad4bbb89055364340e5bd6fa91b99
SSDEEP:	786432:8AOLmwf+uW2YZGfabX6m0tXmx8iLpuB+jND3OL+PWj7BO:bImwG52Y4fa2mk5iL/NLAkW5O
TLSH:	CB77333FB649953EE9AE067345B3A6109DBB3A25641BCC1F0BF0051ECF365601E3963A
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	a2a0b496b2caca72

Static PE Info

General

Entrypoint:	0x4b5eec
Entrypoint Section:	.itext
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, BYTES_REVERSED_HI
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x5E6D1B8D [Sat Mar 14 17:59:41 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6

File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	5a594319a0d69dbc452e748bcf05892e

Authenticode Signature	
Signature Valid:	**true**
Signature Issuer:	CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 7/19/2020 5:00:00 PM 8/18/2022 4:59:59 PM
Subject Chain	• CN=Softdeluxe Ltd., O=Softdeluxe Ltd., STREET="Universitetskaya St., 19", L=Dubna, PostalCode=141980, C=RU
Version:	3
Thumbprint MD5:	3AAC0AA93E2ED65917ADA968712E5829
Thumbprint SHA-1:	0ADD9C997572DA93D4D6478BD57E1F931C7C4328
Thumbprint SHA-256:	7B8685C6C289A1195F26993ADFE0C7331701695346BF4610A40ADAE7B2876D80
Serial:	009D94DF2E075539EBE7F0AAF27135A533

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
add esp, FFFFFFA4h
push ebx
push esi
push edi
xor eax, eax
mov dword ptr [ebp-3Ch], eax
mov dword ptr [ebp-40h], eax
mov dword ptr [ebp-5Ch], eax
mov dword ptr [ebp-30h], eax
mov dword ptr [ebp-38h], eax
mov dword ptr [ebp-34h], eax
mov dword ptr [ebp-2Ch], eax
mov dword ptr [ebp-28h], eax
mov dword ptr [ebp-14h], eax
mov eax, 004B10D8h
call 00007F1030961F65h
xor eax, eax
push ebp
push 004B65DEh
push dword ptr fs:[eax]
mov dword ptr fs:[eax], esp
xor edx, edx
push ebp
push 004B659Ah
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
mov eax, dword ptr [004BE634h]
call 00007F1030A04677h
call 00007F1030A041CEh
lea edx, dword ptr [ebp-14h]
xor eax, eax
call 00007F10309779D8h
mov edx, dword ptr [ebp-14h]
mov eax, 004C1D3Ch
call 00007F103095CB57h
push 00000002h
push 00000000h
push 00000001h

Instruction
mov ecx, dword ptr [004C1D3Ch]
mov dl, 01h
mov eax, dword ptr [004237A4h]
call 00007F1030978A3Fh
mov dword ptr [004C1D40h], eax
xor edx, edx
push ebp
push 004B6546h
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
call 00007F1030A046FFh
mov dword ptr [004C1D48h], eax
mov eax, dword ptr [004C1D48h]
cmp dword ptr [eax+0Ch], 01h
jne 00007F1030A0ACFAh
mov eax, dword ptr [004C1D48h]
mov edx, 00000028h
call 00007F1030979334h
mov edx, dword ptr [004C1D48h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xc4000	0x9a	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc2000	0xf36	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc7000	0x4600	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x21cf248	0x24c0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xc6000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xc22e4	0x244	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0xc3000	0x1a4	.didata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb3604	0xb3800	False	0.34484761272632314	data	6.354329115342966	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.itext	0xb5000	0x1684	0x1800	False	0.5445963541666666	data	5.970901565517897	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xb7000	0x37a4	0x3800	False	0.36104910714285715	data	5.0421620677813435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0xbb000	0x6da0	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0xc2000	0xf36	0x1000	False	0.3681640625	data	4.8987046479600425	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.didata	0xc3000	0x1a4	0x200	False	0.345703125	data	2.7563628682496506	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.edata	0xc4000	0x9a	0x200	False	0.2578125	data	1.8722228665884297	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.tls	0xc5000	0x18	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0xc6000	0x5d	0x200	False	0.189453125	data	1.3838943752217987	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc7000	0x4600	0x4600	False	0.32260044642857144	data	4.437327489999006	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc74c8	0x128	GLS_BINARY_LSB_FIRST	Dutch	Netherlands
RT_ICON	0xc75f0	0x568	GLS_BINARY_LSB_FIRST	Dutch	Netherlands
RT_ICON	0xc7b58	0x2e8	data	Dutch	Netherlands
RT_ICON	0xc7e40	0x8a8	data	Dutch	Netherlands
RT_STRING	0xc86e8	0x360	data		
RT_STRING	0xc8a48	0x260	data		
RT_STRING	0xc8ca8	0x45c	data		
RT_STRING	0xc9104	0x40c	data		
RT_STRING	0xc9510	0x2d4	data		
RT_STRING	0xc97e4	0xb8	data		
RT_STRING	0xc989c	0x9c	data		
RT_STRING	0xc9938	0x374	data		
RT_STRING	0xc9cac	0x398	data		
RT_STRING	0xca044	0x368	data		
RT_STRING	0xca3ac	0x2a4	data		
RT_RCDATA	0xca650	0x10	data		
RT_RCDATA	0xca660	0x2c4	data		
RT_RCDATA	0xca924	0x2c	data		
RT_GROUP_ICON	0xca950	0x3e	data	English	United States
RT_VERSION	0xca990	0x584	data	English	United States
RT_MANIFEST	0xcaf14	0x62c	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
kernel32.dll	GetACP, GetExitCodeProcess, LocalFree, CloseHandle, SizeofResource, VirtualProtect, VirtualFree, GetFullPathNameW, ExitProcess, HeapAlloc, GetCPInfoExW, RtlUnwind, GetCPInfo, GetStdHandle, GetModuleHandleW, FreeLibrary, HeapDestroy, ReadFile, CreateProcessW, GetLastError, GetModuleFileNameW, SetLastError, FindResourceW, CreateThread, CompareStringW, LoadLibraryA, ResetEvent, GetVersion, RaiseException, FormatMessageW, SwitchToThread, GetExitCodeThread, GetCurrentThread, LoadLibraryExW, LockResource, GetCurrentThreadId, UnhandledExceptionFilter, VirtualQuery, VirtualQueryEx, Sleep, EnterCriticalSection, SetFilePointer, LoadResource, SuspendThread, GetTickCount, GetFileSize, GetStartupInfoW, GetFileAttributesW, InitializeCriticalSection, GetThreadPriority, SetThreadPriority, GetCurrentProcess, VirtualAlloc, GetSystemInfo, GetCommandLineW, LeaveCriticalSection, GetProcAddress, ResumeThread, GetVersionExW, VerifyVersionInfoW, HeapCreate, GetWindowsDirectoryW, VerSetConditionMask, GetDiskFreeSpaceW, FindFirstFileW, GetUserDefaultUILanguage, lstrlenW, QueryPerformanceCounter, SetEndOfFile, HeapFree, WideCharToMultiByte, FindClose, MultiByteToWideChar, LoadLibraryW, SetEvent, CreateFileW, GetLocaleInfoW, GetSystemDirectoryW, DeleteFileW, GetLocalTime, GetEnvironmentVariableW, WaitForSingleObject, WriteFile, ExitThread, DeleteCriticalSection, TlsGetValue, GetDateFormatW, SetErrorMode, IsValidLocale, TlsSetValue, CreateDirectoryW, GetSystemDefaultUILanguage, EnumCalendarInfoW, LocalAlloc, GetUserDefaultLangID, RemoveDirectoryW, CreateEventW, SetThreadLocale, GetThreadLocale
comctl32.dll	InitCommonControls
version.dll	GetFileVersionInfoSizeW, VerQueryValueW, GetFileVersionInfoW
user32.dll	CreateWindowExW, TranslateMessage, CharLowerBuffW, CallWindowProcW, CharUpperW, PeekMessageW, GetSystemMetrics, SetWindowLongW, MessageBoxW, DestroyWindow, CharUpperBuffW, CharNextW, MsgWaitForMultipleObjects, LoadStringW, ExitWindowsEx, DispatchMessageW
oleaut32.dll	SysAllocStringLen, SafeArrayPtrOfIndex, VariantCopy, SafeArrayGetLBound, SafeArrayGetUBound, VariantInit, VariantClear, SysFreeString, SysReAllocStringLen, VariantChangeType, SafeArrayCreate
netapi32.dll	NetWkstaGetInfo, NetApiBufferFree
advapi32.dll	RegQueryValueExW, AdjustTokenPrivileges, LookupPrivilegeValueW, RegCloseKey, OpenProcessToken, RegOpenKeyExW

Exports

Name	Ordinal	Address
TMethodImplementationIntercept	3	0x454058
__dbk_fcall_wrapper	2	0x40d0a0

Name	Ordinal	Address
dbkFCallWrapperAddr	1	0x4be63c

Possible Origin

Language of compilation system	Country where language is spoken	Map
Dutch	Netherlands	
English	United States