SHA256: 1baab40705fd5ed3b01341fd1effac02803859431d50bd5e8026daedd8825dd6

File name: FreePDF4.14.EXE

Detection ratio: 0 / 55

Analysis date: 2016-06-05 14:14:35 UTC (6 days, 11 hours ago)

☺ **Probably harmless!** There are strong indicators suggesting that this file is safe to use.

Analysis File detail Relationships Additional information Comments 7 Votes Behavioural information

Antivirus	Result	Update
ALYac	✔	20160605
AVG	✔	20160605
AVware	✔	20160605
Ad-Aware	✔	20160605
AegisLab	✔	20160604
AhnLab-V3	✔	20160605
Alibaba	✔	20160603
Antiy-AVL	✔	20160605
Arcabit	✔	20160605
Avast	✔	20160605
Baidu	✔	20160603
Baidu-International	✔	20160605
BitDefender	✔	20160605
Bkav	✔	20160604
CAT-QuickHeal	✔	20160604
CMC	✔	20160602
ClamAV	✔	20160605
Comodo	✔	20160605
Cyren	✔	20160605
DrWeb	✔	20160605
ESET-NOD32	✔	20160604

Emsisoft	✔	20160605
F-Prot	✔	20160605
F-Secure	✔	20160605
Fortinet	✔	20160605
GData	✔	20160605
Ikarus	✔	20160605
Jiangmin	✔	20160605
K7AntiVirus	✔	20160605
K7GW	✔	20160605
Kaspersky	✔	20160605
Kingsoft	✔	20160605
Malwarebytes	✔	20160605
McAfee	✔	20160605
McAfee-GW-Edition	✔	20160605
eScan	✔	20160605
Microsoft	✔	20160605
NANO-Antivirus	✔	20160605
Panda	✔	20160605
Qihoo-360	✔	20160605
Rising	✔	20160605
SUPERAntiSpyware	✔	20160605
Sophos	✔	20160605
Symantec	✔	20160605
Tencent	✔	20160605
TheHacker	✔	20160604
TrendMicro	✔	20160605
TrendMicro-HouseCall	✔	20160605
VBA32	✔	20160603
VIPRE	✔	20160605
ViRobot	✔	20160605
Yandex	✔	20160604
Zillya	✔	20160603
Zoner	✔	20160605

nProtect	✔	20160603

virustotal (/en/)

SHA256: 1baab40705fd5ed3b01341fd1effac02803859431d50bd5e8026daedd8825dd6

File name: FreePDF4.14.EXE

Detection ratio: 0 / 55

Analysis date: 2016-06-05 14:14:35 UTC (6 days, 12 hours ago)

☺ **Probably harmless!** There are strong indicators suggesting that this file is safe to use.

The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the Windows GUI subsystem.

FileVersionInfo properties

Copyright	© Microsoft Corporation. All rights reserved.
Product	Internet Explorer
Original name	WEXTRACT.EXE .MUI
Internal name	Wextract
File version	11.00.9600.16428 (winblue_gdr.131013-1700)
Description	Win32 Cabinet Self-Extractor

Packers identified

F-PROT	appended, Unicode, SFX

PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2013-10-14 05:50:27
Entry Point	0x000067CC
Number of sections	5

PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.text	4096	26060	26112	6.38	e9bf1a1e456a9a811b1b86e6602e3636
.data	32768	6796	1024	3.18	317f8a934ee443eee01c2a315bde9ca1
.idata	40960	4216	4608	5.05	d8675ba112ef922c6057a02546757a1a
.rsrc	49152	2527232	2523648	7.99	a8e87230c46188a19875935fa39b8454
.reloc	2576384	5038	5120	3.72	83de2f9b2c95be6fea06bced7e8a058e

PE imports

[+] ADVAPI32.dll ()

[+] COMCTL32.dll ()

[+] Cabinet.dll ()

[+] GDI32.dll ()

[+] KERNEL32.dll ()

[+] USER32.dll ()

[+] VERSION.dll ()

[+] msvcrt.dll ()

Number of PE resources by type

RT_RCDATA	14
RT_ICON	13
RT_DIALOG	12
RT_STRING	12
RT_VERSION	2
RT_MANIFEST	1
AVI	1
RT_GROUP_ICON	1

Number of PE resources by language

ENGLISH US	33
GERMAN	23

Debug information

Type	Timestamp	Offset	Size
IMAGE_DEBUG_TYPE_CODEVIEW (2) ()	Mon Oct 14 05:50:27 2013	1972	37 Bytes

ExifTool file metadata

SubsystemVersion	5.1
LinkerVersion	11.0
ImageVersion	6.3
FileSubtype	0
FileVersionNumber	11.0.9600.16428
UninitializedDataSize	0
LanguageCode	German
FileFlagsMask	0x003f
CharacterSet	Unicode
InitializedDataSize	2534400
EntryPoint	0x67cc
OriginalFileName	WEXTRACT.EXE .MUI
MIMEType	application/octet-stream
LegalCopyright	Microsoft Corporation. Alle Rechte vorbehalten.
FileVersion	11.00.9600.16428 (winblue_gdr.131013-1700)
TimeStamp	2013:10:14 06:50:27+01:00
FileType	Win32 EXE
PEType	PE32
InternalName	Wextract

ProductVersion	11.00.9600.16428
FileDescription	Win32 Cabinet Self-Extractor
OSVersion	6.3
FileOS	Windows NT 32-bit
Subsystem	Windows GUI
MachineType	Intel 386 or later, and compatibles
CompanyName	Microsoft Corporation
CodeSize	26112
ProductName	Internet Explorer
ProductVersionNumber	11.0.9600.16428
FileTypeExtension	exe
ObjectFileType	Executable application

SHA256: 1baab40705fd5ed3b01341fd1effac02803859431d50bd5e8026daedd8825dd6

File name: FreePDF4.14.EXE

Detection ratio: 0 / 55

Analysis date: 2016-06-05 14:14:35 UTC (6 days, 12 hours ago)

☺ **Probably harmless!** There are strong indicators suggesting that this file is safe to use.

CarbonBlack CarbonBlack acts as a surveillance camera for computers (http://www.carbonblack.com/)

While monitoring an end-user machine in-the-wild, CarbonBlack noticed the following files in execution **wrote this sample to disk**.

17ddac2b01ecb5bcbc1324db4df292ad (/latest-scan/17ddac2b01ecb5bcbc1324db4df292ad)

a24bfbae8b50a6780b68ff3673fab52f (/latest-scan/a24bfbae8b50a6780b68ff3673fab52f)

332feab1435662fc6c672e25beb37be3 (/latest-scan/332feab1435662fc6c672e25beb37be3)

b3f4eceb90d6f303c675ed042b654906 (/latest-scan/b3f4eceb90d6f303c675ed042b654906)

While monitoring an end-user machine in-the-wild, CarbonBlack noticed this **sample wrote the following files to disk**.

580fece173b4b2e396f90b0bdebc9175 (/latest-scan/580fece173b4b2e396f90b0bdebc9175)

6eb38bbd21b20f8c2fc289e9bd423206 (/latest-scan/6eb38bbd21b20f8c2fc289e9bd423206)

a5b5a716d6d2ab1e677d7e09097d8f7f (/latest-scan/a5b5a716d6d2ab1e677d7e09097d8f7f)

2e8c8e9aae4216a6ba20848f8260bca6 (/latest-scan/2e8c8e9aae4216a6ba20848f8260bca6)

d1a86f021ca50ca752fed410fe0dbc6a (/latest-scan/d1a86f021ca50ca752fed410fe0dbc6a)

bbbe928ff61c35367ff6e08cf79af0ae (/latest-scan/bbbe928ff61c35367ff6e08cf79af0ae)

8166a224bce403856d9820a3b95fea64 (/latest-scan/8166a224bce403856d9820a3b95fea64)

4c383f06d906a1a77eb90557f9c180be (/latest-scan/4c383f06d906a1a77eb90557f9c180be)

7d4a0d6c685107ac1b5089806cd4273b (/latest-scan/7d4a0d6c685107ac1b5089806cd4273b)

Execution parents

This file was created during the sandboxed execution of the following files.

43597bdd9d4ec083670c9470bf44efedf0958fa73d9ee96cc556645c0e43c33c
(/en/file/43597bdd9d4ec083670c9470bf44efedf0958fa73d9ee96cc556645c0e43c33c/analysis/)

Compressed bundles

This file was also submitted to VirusTotal in the following compressed file bundles.

1e77cb07b39c4d94a075d5eacc8129708e7f74b6039c7994c27ad001737bf599
(/en/file/1e77cb07b39c4d94a075d5eacc8129708e7f74b6039c7994c27ad001737bf599/analysis/)

49e99b9143894fbc4f33907b63bae4f4b4d913798c7609b268c4f928b971eaf5
(/en/file/49e99b9143894fbc4f33907b63bae4f4b4d913798c7609b268c4f928b971eaf5/analysis/)

a5802f154ec27fb0a919a575c6cacaa6f3edc4a3975ff400dcad4e2add8448d6
(/en/file/a5802f154ec27fb0a919a575c6cacaa6f3edc4a3975ff400dcad4e2add8448d6/analysis/)

SHA256: 1baab40705fd5ed3b01341fd1effac02803859431d50bd5e8026daedd8825dd6

File name: FreePDF4.14.EXE

Detection ratio: 0 / 55

Analysis date: 2016-06-05 14:14:35 UTC (6 days, 12 hours ago)

☺ **Probably harmless!** There are strong indicators suggesting that this file is safe to use.

Analysis | File detail | Relationships | Additional information | Comments 7 | Votes | Behavioural information

File identification

MD5	51fa9f7e0ee48f9ea9bc231d1df49556
SHA1	0b73035d5455489c50413829eef970c55d91fa71
SHA256	1baab40705fd5ed3b01341fd1effac02803859431d50bd5e8026daedd8825dd6
ssdeep	49152:iQq3jTD/nNRw80twhBJMD+PXY3+iduh4KtmkvbjF:oDMShAD+PXY3+Guh4Rkvl
authentihash (http://download.microsoft.com/download/9/c/5/9c5b2167-8017-4bae-9fde-d599bac8184a/Authenticode_PE.docx)	b48d891c4a64a15140ed9aba8f9e62acc8affcac90dc088eb8696872d1c4554c
imphash (https://www.mandiant.com/blog/tracking-malware-import-hashing/)	bc70c4fa605f17c85050b7c7b6d42e44
File size	2.4 MB (2561536 bytes)
File type	Win32 EXE
Magic literal	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 MS Cabinet Self-Extractor (WExtract stub) (86.7%) Win32 Executable MS Visual C++ (generic) (8.9%) Win32 Dynamic Link Library (generic) (1.8%) Win32 Executable (generic) (1.2%) Generic Win/DOS Executable (0.5%)
Tags	**peexe**

VirusTotal metadata

First submission	2014-03-19 11:55:51 UTC (2 years, 2 months ago)
Last submission	2016-06-05 14:14:35 UTC (6 days, 12 hours ago)
File names	freepdf4.14.exe 2__FreePDF4.14.EXE freepdf4.14 (1).exe FreePDF4.14(1).EXE

SHA256: 1baab40705fd5ed3b01341fd1effac02803859431d50bd5e8026daedd8825dd6

File name: FreePDF4.14.EXE

Detection ratio: 0 / 55

Analysis date: 2016-06-05 14:14:35 UTC (6 days, 12 hours ago)

☺ **Probably harmless!** There are strong indicators suggesting that this file is safe to use.

Condensed report! The following is a condensed report of the behaviour of the file when executed in a controlled environment. The actions and events described were either performed by the file itself or by any other process launched by the executed file or subjected to code injection by the executed file.

Opened files

C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\IXP000.TMP\TMP4351$.TMP (successful)

C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\IXP000.TMP\ (successful)

C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\ (successful)

C:\DOCUME~1\<USER>~1\LOCALS~1\ (successful)

C:\DOCUME~1\<USER>~1\ (successful)

C:\DOCUME~1\ (successful)

\\.\MountPointManager (successful)

\\.\PIPE\lsarpc (successful)

Runtime DLLs

c:\windows\system32\advapi32.dll (successful)

feclient.dll (successful)

rpcrt4.dll (successful)

comctl32.dll (successful)

Additional details

The file sends control codes directly to certain device drivers making use of the DeviceIoControl (http://msdn.microsoft.com/en-us/library/windows/desktop/aa363216%28v=vs.85%29.aspx) Windows API function.

	FreePDF4.14.exe FreePDF4.14.EXE FreePDF4.14.EXE FreePDF4.145.EXE FreePDF4.14.EXE FreePDF4.14.EXE bnzqgxkukvejyucbhau656lqyvozd6tr.exe FreePDF4.14 (1).EXE freepdf FreePDF4.14 (1).EXE filename freepdf4.14.exe.p0jk21x.partial freepdf4.14.exe freepdf4.14.exe FreePDF4.14.EXE freepdf4.14[1].exe freepdf4.14.exe FreePDF_v4.14.EXE freepdf4.14.exe FreePDF_4_14.exe file-6810321_EXE

Advanced heuristic and reputation engines

ClamAV	Possibly Unwanted Application. While not necessarily malicious, the scanned file presents certain characteristics which depending on the user policies and environment may or may not represent a threat. For full details see: http://www.clamav.net/doc/pua.html (http://www.clamav.net/doc/pua.html).
Symantec reputation	**Suspicious.Insight** (http://www.symantec.com/security_response/writeup.jsp?docid=2010-021223-0550-99)