

Interactivity is now available in beta. Submit or resubmit a file or URL and select 'Live interaction' to explore feature.

Sandbox Report

File: pplnk.exe

Resubmit
Print
Download options

SHA-256
 73fe4fef701bf731...30fb81e433240736

Submitted by
 prashant.deshmukh@fisglobal.com

Discovered

Detonation environment
 Windows 10 64, Professional, 10.0 (build 16299)

Network settings
 Default network connectivity

Timestamp
 Jan. 9, 2024 17:43:48

Threat level ⓘ
 Suspicious

Threat score ⓘ
 39/100

- Static analysis
- Dynamic analysis
- Intelligence
- MITRE ATT&CK

File information

Classifications

pplnk.exe			
Size	Type	Description	Architecture
1.55MB	peexe, 64bits, assembly...	PE32+ executable (GUI) x86-64 Mono/.Net assembly,...	64 Bit
SHA256	Compiler/Packer		
73fe4fef701bf731274e6e7efd97a1a91566e842ba44f7...	Microsoft visual C++ vx...		

Version info					
Translation	Legal copyright	Assembly Version	Internal name	File version	Comments
0x0000 0x04b0	Copyright 2019 Weizhi ...	1.8.3.19170	pplnk.exe	1.8.3.*	A tiny screen whiteboar...
Product name	Product version	File description	Original file name		
pplnk from glnk	1.8.3.*	pplnk	pplnk.exe		

- File information
- Classifications
- File sections
- File resources
- Data directories
- Risk assessment
- JSON report

Additional static data

Entrypoint	Image base	Image file characteristics	Major OS version	Minor OS version
0x140000000	0x140000000	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE	4	4
Subsystem	DLL characteristics			
Windows Gui	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_B...			

Resources ▼

Visualization ▼

Entrypoint preview ▼

Classification (TrID) 5 ▼

Metadata

File sections

Name	Entropy	Virtual ad...	Virtual size	Raw size	MD5	Characteristics
.text	7.2504577231	0x2000	0x182e44	0x183000	b05ab96702df140ae40366195acad882	IMAGE_SCN_MEM_E; IMAGE_SCN_CNT_CC IMAGE_SCN_MEM_RI
.rsrc	3.91021248003	0x186000	0xaa0	0xc00	266e1c232420b1f35b697669ea397dd4	IMAGE_SCN_CNT_IN IMAGE_SCN_MEM_RI

File resources

Name	RVA	Size	Type	Language
RT_ICON	0x186100	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024, ...	neutral
RT_GROUP_ICON	0x186578	0x14	data	neutral
RT_VERSION	0x18659c	0x39c	data	neutral
RT_MANIFEST	0x186948	0x154	ASCII text, with CRLF line terminators	neutral

4 results (1-4 shown)

Items per page

5

Page 1 of 1



Data directories

Name	Virtual address	Virtual size	Is in section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	--
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	--
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x186000	0xaa0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	--
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	--

16 results (1-5 shown)

Items per page

5

Page 1 of 4



Risk assessment



Remote Access

1 ▾

Spyware

1 ▾

Fingerprint

1 ▾

Evasive

1 ▾

JSON report



Raw JSON output from the Sandbox detonation

