

样本分析报告

文件名称：panel6_2.zip

SHA256：df1b09da75bde93d73efb4b28a9cf67a5ca280f357278aad65d9bd2ca076b3d8

文件大小：33.91 MB

文件类型：Zip archive data, at least v1.0 to extract

分析环境： Win10(1903 64bit, Office2016)

微步判定： 安全



目录

1 引擎检测 -----

2 静态分析 -----

3 动态分析 -----





安全

panel6_2.zip

首次提交：2024/08/11 末次提交：2024/08/11 末次分析：2024/08/11 22:39:15

文件大小：33.91 MB 文件类型：Zip archive data, at least v1.0 to extract
引擎检出：0 / 28 分析环境：Win10(1903 64bit,Office2016)

HASH
SHA256: df1b09da75bde93d73efb4b28a9cf67a5ca280f357278aad65d9bd2ca076b3d8
MD5: 8e479054d7992616c0da697054e64b71
SHA1: f4eab1a2f088be79669963ac3b04488f1ca3bd19

多引擎检测

检出率：0 / 28

最近检测时间：2024-08-11 22:38:56

引擎	检出	引擎	检出
微软 (MSE)	无检出	ESET	无检出
卡巴斯基 (Kaspersky)	无检出	小红伞 (Avira)	无检出
IKARUS	无检出	大蜘蛛 (Dr.Web)	无检出
Avast	无检出	AVG	无检出
GDATA	无检出	K7	无检出
安天 (Antiy)	无检出	江民 (JiangMin)	无检出
360 (Qihoo 360)	无检出	Baidu	无检出
NANO	无检出	Trustlook	无检出
瑞星 (Rising)	无检出	熊猫 (Panda)	无检出
Sophos	无检出	ClamAV	无检出
WebShell专杀	无检出	Baidu-China	无检出
MicroAPT	无检出	OneAV	无检出
OneStatic	无检出	MicroNonPE	无检出
OneAV-PWSH	无检出	ShellPub	无检出

收起全部

静态分析

基础信息

文件名称 df1b09da75bde93d73efb4b28a9cf67a5ca280f357278aad65d9bd2ca076b3d8
文件格式 Zip
文件类型(Magic) Zip archive data, at least v1.0 to extract
文件大小 33.91MB

SHA256	df1b09da75bde93d73efb4b28a9cf67a5ca280f357278aad65d9bd2ca076b3d8
SHA1	f4eab1a2f088be79669963ac3b04488f1ca3bd19
MD5	8e479054d7992616c0da697054e64b71
CRC32	FF93592D
SSDEEP	786432:5RV90/dU7/Qe6EoWDZXrgf/8q4Cu6z72FP7w3iXXw3iX7qJfg86p:5RUaP6ERhTq4oCP7DGfg8g
TLSH	T1BB7723B8CBE855D9C99FB8329A0B23F0F57251D28A93380B69149EB0FB5B1033774756
Tags	zip,contains_zip

元数据

ExifTool	
FileType	ZIP
FileTypeExtension	zip
MIMEType	application/zip
ZipRequiredVersion	10
ZipBitFlag	0
ZipCompression	None
ZipModifyDate	2024:08:11 01:13:44
ZipCRC	0x00000000
ZipCompressedSize	0
ZipUncompressedSize	0
ZipFileName	panel/

TrID	
34.4% (.SH3D)	Sweet Home 3D design (generic) (10500/1/3)
26.2% (.XPI)	Mozilla Firefox browser extension (8000/1/1)
22.9% (.MAFF)	Mozilla Archive Format (gen) (7000/1/1)
13.1% (.ZIP)	ZIP compressed archive (4000/1)
3.2% (.PG/BIN)	PrintFox/Pagefox bitmap (640x800) (1000/1)

Magika ?	
可信度 (Score)	0.9952883720397949
识别结果 (Ct_label)	zip
Magic	Zip archive data
Mime_type	application/zip
分类 (Group)	archive
描述信息 (Description)	Zip archive data

格式深度分析

压缩通用

子文件摘要

子文件数量	4675
最早修改时间	2017-02-20 18:16:50
最晚修改时间	2024-08-11 01:13:44

子文件扩展名(26)

扩展名	数量	扩展名	数量
js	1817	png	1280
svg	719	py	506
html	72	conf	70

json	55	css	30
gif	23	sh	20

子文件类型(8)

扩展名	数量	扩展名	数量
unknown	2713	IMAGE	1386
PYTHON	483	IE	67
SH	18	EOT	5
PHP	2	Zip	1

子文件详情(100+)

文件	Magic	文件大小	修改时间	
panel\config\link.json	ASCII text, with no line terminators	2	2023-05-10 17:33:00	展开
panel\config\update_time.pl	ASCII text, with no line terminators	10	2024-08-07 11:03:28	展开
panel\config\install_check.json	ASCII text	3606	2024-08-07 11:03:38	展开
panel\config\GeoLite2-City.mmdb	data	8351184	2023-11-17 14:15:26	展开
panel\config\dns_api_init.json	UTF-8 Unicode text	1950	2024-08-07 11:03:38	展开

查看全部

沙箱动态检测

Win10(1903 64bit,Office2016)

执行流程

