云沙箱
微步旗下文件威胁分析平台

S-240223-093811

样本分析报告

文件名称：Pwdump4.zip

SHA256：0938119f55bcf7e56e7dbd94270e8d74613322caf59274fedc4d93c9d866b32c

文件大小：174.6 KB

文件类型：Zip archive data, at least v2.0 to extract

分析环境：Win10(1903 64bit,Office2016)

微步判定：可疑

目录

云沙箱 云沙箱 云沙箱 云沙箱

Pwdump4.zip

可疑

首次提交: 2024/02/23　末次提交: 2024/02/23　末次分析: 2024/02/23 19:17:01

文件大小： 174.6 KB　文件类型： Zip archive data, at least v2.0 to extract

引擎检出： 5 / 25　分析环境： Win10(1903 64bit,Office2016)

威胁分类： 风险软件　木马家族： PWDump

HASH

SHA256: 0938119f55bcf7e56e7dbd94270e8d74613322caf59274fedc4d93c9d866b32c

MD5: 2750b5ac403f54b3e2165ebeedcfe76b

SHA1: fbf81253ea0286f123610735bf0296227c8081f3

行为检测

MITRE ATT&CK™ 矩阵（技术）检测到 **1** 条技术指标。 查看完整结果

Win10(1903 64bit,Office2016)

通用行为（1） 全部展开

系统环境探测　读取计算机名称　Win10(1903 64bit,Office2016)

多引擎检测

检出率：**5** / 25

最近检测时间：2024-02-23 19:17:01

引擎	检出	引擎	检出
卡巴斯基（Kaspersky）	not-a-virus:PSWTool.Win32.PWDump.4	IKARUS	not-a-virus:PSWTool.Win32.PWDump
安天（Antiy）	Trojan[PSWTool]/Win32.PWDump	江民（JiangMin）	PSWTool.PWDump.bi
NANO	Riskware.Win32.PWDump.tbmqn	微软（MSE）	无检出
ESET	无检出	小红伞（Avira）	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	360（Qihoo 360）	无检出
Baidu	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
OneAV	无检出	OneStatic	无检出
MicroNonPE	无检出		

收起全部

静态分析

基础信息

文件名称	0938119f55bcf7e56e7dbd94270e8d74613322caf59274fedc4d93c9d866b32c
文件格式	Zip
文件类型(Magic)	Zip archive data, at least v2.0 to extract
文件大小	174.60KB
SHA256	0938119f55bcf7e56e7dbd94270e8d74613322caf59274fedc4d93c9d866b32c
SHA1	fbf81253ea0286f123610735bf0296227c8081f3
MD5	2750b5ac403f54b3e2165ebeedcfe76b
CRC32	59164BDC
SSDEEP	3072:MduDPsQeVFrtaPJdTQQvjcEDKecTjfbRulpn4bP2+c3lXquDPsQe5FrtaPJdTQQb:McUNtaPhcmKecTjfbe91U9taPhcmKY
TLSH	T1D0040299C244E0EBF76AB2F0F79F1285D9C1435E1BB46312C1BA244D8E1B2B91B36D4D
Tags	zip,contains_pe

元数据

ExifTool

FileType	ZIP
FileTypeExtension	zip
MIMEType	application/zip
ZipRequiredVersion	20
ZipBitFlag	0
ZipCompression	None
ZipModifyDate	2024:01:16 09:42:42
ZipCRC	0x00000000
ZipCompressedSize	0
ZipUncompressedSize	0
ZipFileName	Pwdump4/

TrID

80.0% (.ZIP)	ZIP compressed archive (4000/1)
20.0% (.PG/BIN)	PrintFox/Pagefox bitmap (640x800) (1000/1)

格式深度分析

压缩通用

子文件摘要

子文件数量	33
最早修改时间	2006-12-18 17:49:46
最晚修改时间	2006-12-18 17:49:54

子文件扩展名(13)

扩展名	数量	扩展名	数量
cpp	8	txt	8
h	3	dll	2
dsp	2	exe	2
plg	2	bak	1
def	1	dsw	1

子文件类型(6)

扩展名	数量	扩展名	数量
unknown	25	DLLx86	2
EXEx86	2	IE	2
Office Document(OLE)	1	Zip	1

子文件详情(34)

文件	Magic	文件大小	修改时间	
C:\Users\Administrator\Desktop\staticscan\ca…		-	-	展开
Pwdump4\Pwdump4\COPYING.txt	ASCII text, with CRLF line terminators	18353	2006-12-18 17:49:52	展开
Pwdump4\Pwdump4\Declaim.txt	ASCII text, with CRLF line terminators	2119	2006-12-18 17:49:52	展开
Pwdump4\Pwdump4\LsaExt.dll	PE32 executable (DLL) (GUI) Intel 80386, for…	40960	2006-12-18 17:49:52	展开
Pwdump4\Pwdump4\PwDump4.exe	PE32 executable (console) Intel 80386, for M…	73728	2006-12-18 17:49:52	展开

查看全部

沙箱动态检测

Win10(1903 64bit,Office2016)

执行流程

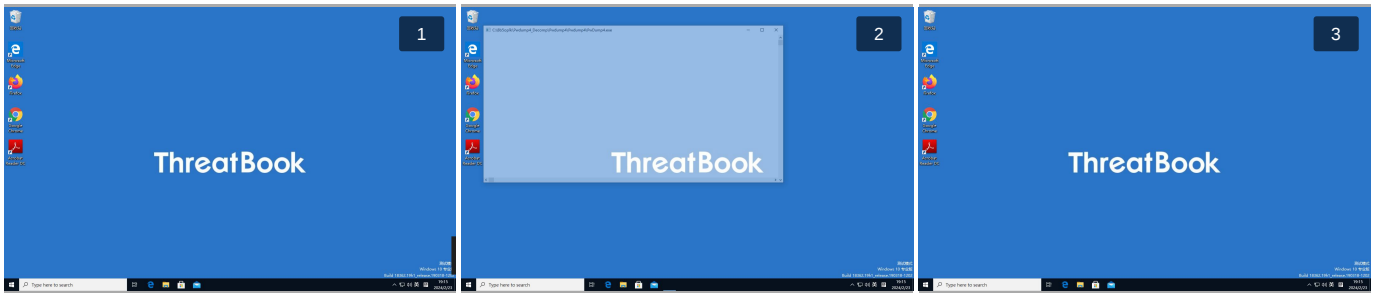
进程详情

共分析了1个进程

PwDump4.exe（PID：1296）

"C:\8b5oplk\Pwdump4_Decomp\Pwdump4\Pwdump4\PwDump4.exe"

运行截图（3）



网络行为

指纹	域名	DNS	HTTP	HTTPS	TCP	UDP	SMTP	ICMP	IRC	Hosts	Dead-Hosts
0	0	0	0	0	0	0	0	0	0	0	0

释放文件

无释放文件