微步云沙箱

一站式文件分析平台，场景化专业云沙箱

S-230528-c03d9b

样本分析报告

文件名称：send

SHA256：c03d9b3c4729eecc032d62230ca3b54dd82d8f41cd46c25b638fcbdcdbba01ff

文件大小：140.36 KB

文件类型：ASCII text, with very long lines, with no line terminators

分析环境：Linux(CentOS 7.0 64bit) Win10(1903 64bit,Office2016)

微步判定：安全

目录

微步云沙箱

send

首次提交: 2023/05/28　　末次提交: 2023/05/28　　末次分析: 2023/05/28 04:09:00

文件大小： 140.36 KB　　文件类型： ASCII text, with very long lines, with no line terminators

引擎检出： 0 / 24　　分析环境： Win10(1903 64bit,Office2016)　Linux(CentOS 7.0 64bit)

HASH

SHA256: c03d9b3c4729eecc032d62230ca3b54dd82d8f41cd46c25b638fcbdcdbba01ff

MD5: afdf8f9d79a753d18e026af27e21ae5f

SHA1: 560cba76fdff68b2806a8a9b2be2211f3d20c431

安全

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

一般行为　读取系统的信任设置　Win10(1903 64bit,Office2016)

多引擎检测

检出率：0 / 24

最近检测时间：2023-05-28 04:01:12

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

收起全部

静态分析

基础信息

文件名称	c03d9b3c4729eecc032d62230ca3b54dd82d8f41cd46c25b638fcbdcdbba01ff
文件格式	JS
文件类型(Magic)	ASCII text, with very long lines, with no line terminators
文件大小	140.36KB
SHA256	c03d9b3c4729eecc032d62230ca3b54dd82d8f41cd46c25b638fcbdcdbba01ff
SHA1	560cba76fdff68b2806a8a9b2be2211f3d20c431
MD5	afdf8f9d79a753d18e026af27e21ae5f
CRC32	7BF57F5F
SSDEEP	1536:x3DA0p0QVh35tJ1ryamorHLPHZrHLPHwGy:VtTkorHLPHZrHLPHwt
TLSH	T173E3D4D47AAAE10F5B8D0D83AE542BEB1179D723A6C4630793E8FF4E01E515AC5ACCD0
Tags	js

元数据

ExifTool

FileType	js
FileTypeExtension	txt
MIMEType	text/plain
MIMEEncoding	us-ascii
Newlines	(none)
LineCount	1
WordCount	49

沙箱动态检测

Win10(1903 64bit,Office2016)

执行流程

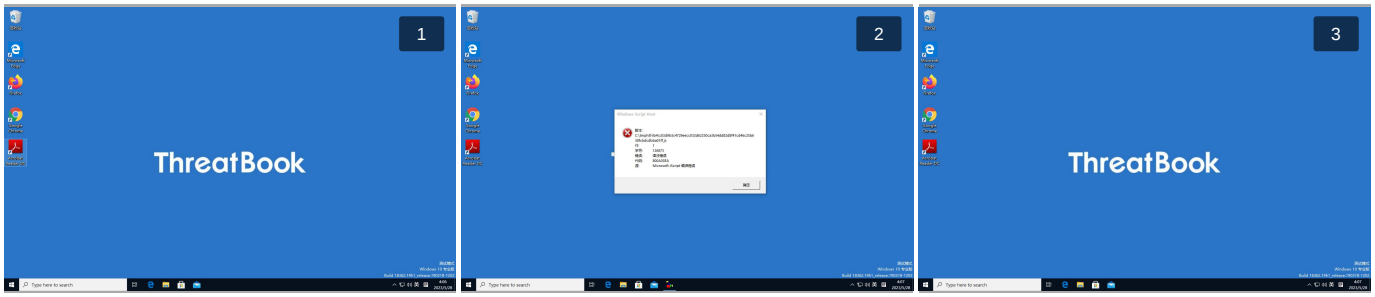
进程详情

共分析了1个进程

wscript.exe（PID：876）

"C:\Windows\System32\wscript.exe" C:\tmph5hlb4\c03d9b3c4729eecc032d62230ca3b54dd82d8f41cd46c25b638fcbdcdbba01ff.js

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

Linux(CentOS 7.0 64bit)

分析失败

文件类型与分析环境不匹配，请尝试其他环境分析