

样本分析报告


文件名称：BinanceSquarePoster-master.zip

SHA256：fa9ab7f13a788012135399a1744074d9e10fcd30e8ad6093682673dfe38e3034

文件大小：68.14 KB

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	多维检测	-----
2	引擎检测	-----
3	静态分析	-----
4	动态分析	-----



安全

BinanceSquarePoster-master.zip

首次提交: 2025/03/27 末次提交: 2025/03/27 末次分析: 2025/03/27 10:15:57

文件大小: 68.14 KB 文件类型: Zip archive data, at least v1.0 to extract
引擎检出: 0 / 26 分析环境: Win10(1903 64bit,Office2016)

HASH
SHA256: fa9ab7f13a788012135399a1744074d9e10fcd30e8ad6093682673dfe38e3034
MD5: 22b6b96fe75d7ad200977e22561030a6
SHA1: 8b0e922f4bfc6cb5077b6f9c5350afaca14e7183

多维检测

Sigma 规则 (1)					Win10(1903 64bit,Office2016)	
标题	描述	标签	危险等级	匹配项	源	分析环境
New Application in AppCompat	A General detection for a new a pplication in AppCompat. Thi...	execution; t1204.002	info	查看	SigmaHQ	Win10(1903 ...

多引擎检测

检出率: 0 / 26最近检测时间: 2025-03-27 10:15:57

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	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
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

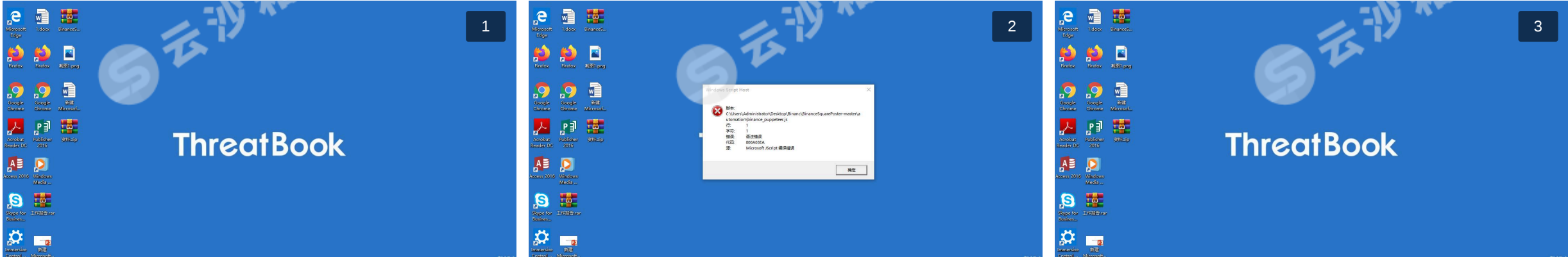
基础信息	
文件名称	fa9ab7f13a788012135399a1744074d9e10fcd30e8ad6093682673dfe38e3034
文件格式	Zip
文件类型(Magic)	Zip archive data, at least v1.0 to extract
文件大小	68.14KB
SHA256	fa9ab7f13a788012135399a1744074d9e10fcd30e8ad6093682673dfe38e3034
SHA1	8b0e922f4bfc6cb5077b6f9c5350afaca14e7183
MD5	22b6b96fe75d7ad200977e22561030a6
CRC32	D9974BD5
SSDEEP	1536:28nyimffdeju8uoa03MuWOS3YmG8fXBHe2S/:2+y9ffdeuYx/tSBXXBHe2O
TLSH	T1A563AD3E7F0FC621CD2674FDDA514302DBA9651681C59A130A8D26321FD7A8CBEAD36C
Tags	zip

元数据

ExifTool	
Comment	e3580b8ca5b3a1d6f836c89f5f20a3b3bd37e7b3
FileType	ZIP
FileTypeExtension	zip
MIMEType	application/zip
ZipRequiredVersion	10
ZipBitFlag	0
ZipCompression	None
ZipModifyDate	2025:03:26 19:08:26
ZipCRC	0x00000000

└─  wscript.exe (PID : 6780)
"C:\Windows\System32\wscript.exe" C:\Users\Administrator\Desktop\Binanc\BinanceSquarePoster-master\automation\binance_puppeteer.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