

# 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	

# 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

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

#### ▮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)	<ul><li>✓ 无检出</li><li>✓ 无检出</li></ul>
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	<ul><li>✓ 无检出</li><li>✓ 无检出</li></ul>
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 zrt ##II(Magic) Zip ar

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 1536:28nyimffdejju8uoa03MuWOS3YmG8fXBHe2S/:2+y9ffdeuYx/tSBXXBHe2O

TLSH T1A563AD3E7F0FC621CD2674FDDA514302DBA9651681C59A130A8D26321FD7A8CBEAD36C

Tags zip

# ☑ 元数据

ExifTool Comment e3580b8ca5b3a1d6f836c89f5f20a3b3bd37e7b3 ZIP FileType FileTypeExtension zip MIMEType application/zip  ${\it Zip Required Version}$ 10 ZipBitFlag 0 ZipCompression None 2025:03:26 19:08:26 ZipModifyDate ZipCRC 0x00000000

ZipCompressedSize 0
ZipUncompressedSize 0

ZipFileName BinanceSquarePoster-master/

TrID

 58.3% (.MAFF)
 Mozilla Archive Format (gen) (7000/1/1)

 33.3% (.ZIP)
 ZIP compressed archive (4000/1)

 8.3% (.PG/BIN)
 PrintFox/Pagefox bitmap (640x800) (1000/1)

### ❷ 格式深度分析

压缩通用

#### □ 子文件摘要

子文件数量 39

最早修改时间 2025-03-27 10:08:26 最晚修改时间 2025-03-27 10:08:26

#### □ 子文件扩展名(13)

扩展名	数量	扩展名	数量
js	11	json	7
md	4	css	2
gitignore	2	svg	2
ts	2	tsx	2
yaml	2	html	1

# 一 子文件类型(2)

扩展名	数量	扩展名	数量
unknown	38	IE	1

#### ─ 子文件详情(39)

文件	Magic	文件大小	修改时间	
BinanceSquarePoster-master\.vscode\launch.json	UTF-8 Unicode text	468	2025-03-27 10:08:26	展开 🛇
BinanceSquarePoster-master\.vscode\settings.json	ASCII text	64	2025-03-27 10:08:26	展开 🛇
BinanceSquarePoster-master\LICENSE	UTF-8 Unicode text	1491	2025-03-27 10:08:26	展开 🛇
BinanceSquarePoster-master\README.md	UTF-8 Unicode text	1816	2025-03-27 10:08:26	展开 🛇
BinanceSquarePoster-master\automation\README.md	ASCII text	43	2025-03-27 10:08:26	展开 🛇

查看全部 ♡

# ▮沙箱动态检测

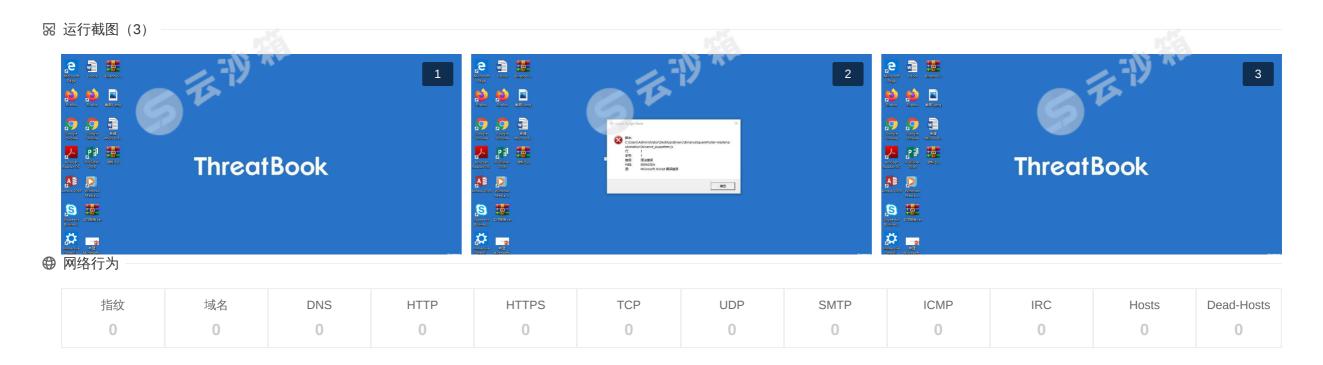
# Win10(1903 64bit,Office2016)

# ┗ 执行流程



# 28 进程详情

共分析了1个进程



## □ 释放文件

无释放文件

