样本分析报告

文件名称： sysvolume.7z

SHA256： d54d4ea3a38755d91f2ee20800a3e48569863634b452d2da904139cf4c05cad5

文件大小： 9.53 MB

文件类型： 7-zip archive data, version 0.3

分析环境： Win10(1903 64bit,Office2016)

微步判定： 恶意

云沙箱

目录

sysvolume.7z

首次提交: 2025/12/26　末次提交: 2025/12/26　末次分析: 2025/12/26 19:25:09

文件大小： 9.53 MB　文件类型： 7-zip archive data, version 0.3

引擎检出： 6 / 28　分析环境： Win10(1903 64bit,Office2016)

威胁分类： 木马　木马家族： BitCoinMiner

恶意

HASH

SHA256: d54d4ea3a38755d91f2ee20800a3e48569863634b452d2da904139cf4c05cad5

MD5: e8909ea3dd2eb99056fb8391e5761699

SHA1: 50d9e45ee12ede5bb2685c2be9729b96ea0b16a1

情报IOC

情报IOC	IOC类型	微步判定	情报内容	发现IOC环境
d54d4ea3a38755d91f2ee20800a3e48569863634b452d2da904139cf4c05cad5	Hash	恶意	BitCoinMiner 木马	Win10(1903 64bit,Office2016)

行为检测

MITRE ATT&CK™ 矩阵（技术）检测到 **2** 条技术指标。 查看完整结果　Win10(1903 64bit,Office2016)

高危行为 (1)

网络相关	进程powershell.exe启动的文档或脚本文件发起了网络通信，表示存在一个潜在的漏洞利用或攻击载荷（Payload）被下载

可疑行为 (6)

一般行为	请求访问系统服务
	利用Windows操作系统的空闲时间计算系统持续运行时间
信息搜集	安装消息钩子
反检测技术	检查适配器地址，可用于检测虚拟网络接口
反逆向工程	创建PAGE_GUARD属性的内存页，通常用于反逆向和反调试
系统敏感操作	添加文件到Windows Defender白名单

通用行为 (6)

一般行为	读写ini文件
	命令行控制台有数据输出
	在临时目录中创建文件
	创建日志文件
系统环境探测	查询计算机名
系统敏感操作	调用COM相关API

多维检测

Yara 规则

Win10(1903 64bit,Office2016)

初始样本：1

规则	描述	SHA256	匹配项	源	分析环境
shellcode	Matched shellcode byte patterns	d54d4ea3a38755d91f2ee20800a3e48569863634…	查看	General	Win10(1903 …

释放文件：1

规则	描述	路径	匹配项	源	分析环境
powershell	(no description)	C:\Users\Administrator\AppData\Local\Microsoft\…	查看	Github	Win10(1903 …

Sigma 规则 (3)

Win10(1903 64bit,Office2016)

标题	描述	标签	危险等级	匹配项	源	分析环境
Powershell Defender Exclusion	Detects requests to exclude files, folders or processes from …	defense_evasion; t1562.001	高	查看	SigmaHQ	Win10(1903 …
Non Interactive PowerShell	Detects non-interactive PowerShell activity by looking at pow…	execution; t1086; t1059.001	低	查看	SigmaHQ	Win10(1903 …
PowerShell Network Connections	Detects a Powershell process that opens network connectio…	execution; t1059.001; t1086	低	查看	SigmaHQ	Win10(1903 …

多引擎检测

检出率：**6** / 28

最近检测时间：2025-12-26 19:24:10

引擎	检出	引擎	检出
ESET	multiple detections	卡巴斯基（Kaspersky）	Trojan.Win32.BitCoinMiner.hau
Avast	Script:SNH-gen	AVG	Script:SNH-gen
GDATA	Application.Generic.4665939	安天（Antiy）	Trojan[Miner]/Win32.BitCoinMiner
微软（MSE）	无检出	小红伞（Avira）	无检出
IKARUS	无检出	大蜘蛛（Dr.Web）	无检出
K7	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	d54d4ea3a38755d91f2ee20800a3e48569863634b452d2da904139cf4c05cad5
文件格式	7-zip
文件类型(Magic)	7-zip archive data, version 0.3
文件大小	9.53MB
SHA256	d54d4ea3a38755d91f2ee20800a3e48569863634b452d2da904139cf4c05cad5
SHA1	50d9e45ee12ede5bb2685c2be9729b96ea0b16a1
MD5	e8909ea3dd2eb99056fb8391e5761699
CRC32	CD899B59
SSDEEP	196608:ZzwRw+JvsEWVH9BnI1KmHhTJsGOeugsq1wXjpCQQMQqscCExWJeSbv9:9wi+EVH9xI1K05JBNvbal9QMQe0bbv9
TLSH	T1E4A633C664169FA72D998403CF6749D4C0D7BA570D3C1C56A09832EA89FEBB23EF3191
Tags	7z,contains_pe

元数据

ExifTool

FileType	7Z
FileTypeExtension	7z
FileVersion	7z v0.03
MIMEType	application/x-7z-compressed

TrID

100.0% (.7Z)	7-Zip compressed archive (gen) (6000/1)

Magika

Mime_type	application/x-7z-compressed
分类 (Group)	archive
描述信息 (Description)	7-zip archive data

格式深度分析

压缩通用

子文件摘要

子文件数量	6
最早修改时间	2025-12-25 10:39:06.8654000
最晚修改时间	2025-12-25 12:01:30.5452245

子文件扩展名(5)

扩展名	数量	扩展名	数量
bat	1	bin	1
dat	1	dll	1
vbs	1	-	-

子文件类型(3)

扩展名	数量	扩展名	数量
DLLx64	2	unknown	2
BAT	1	-	-

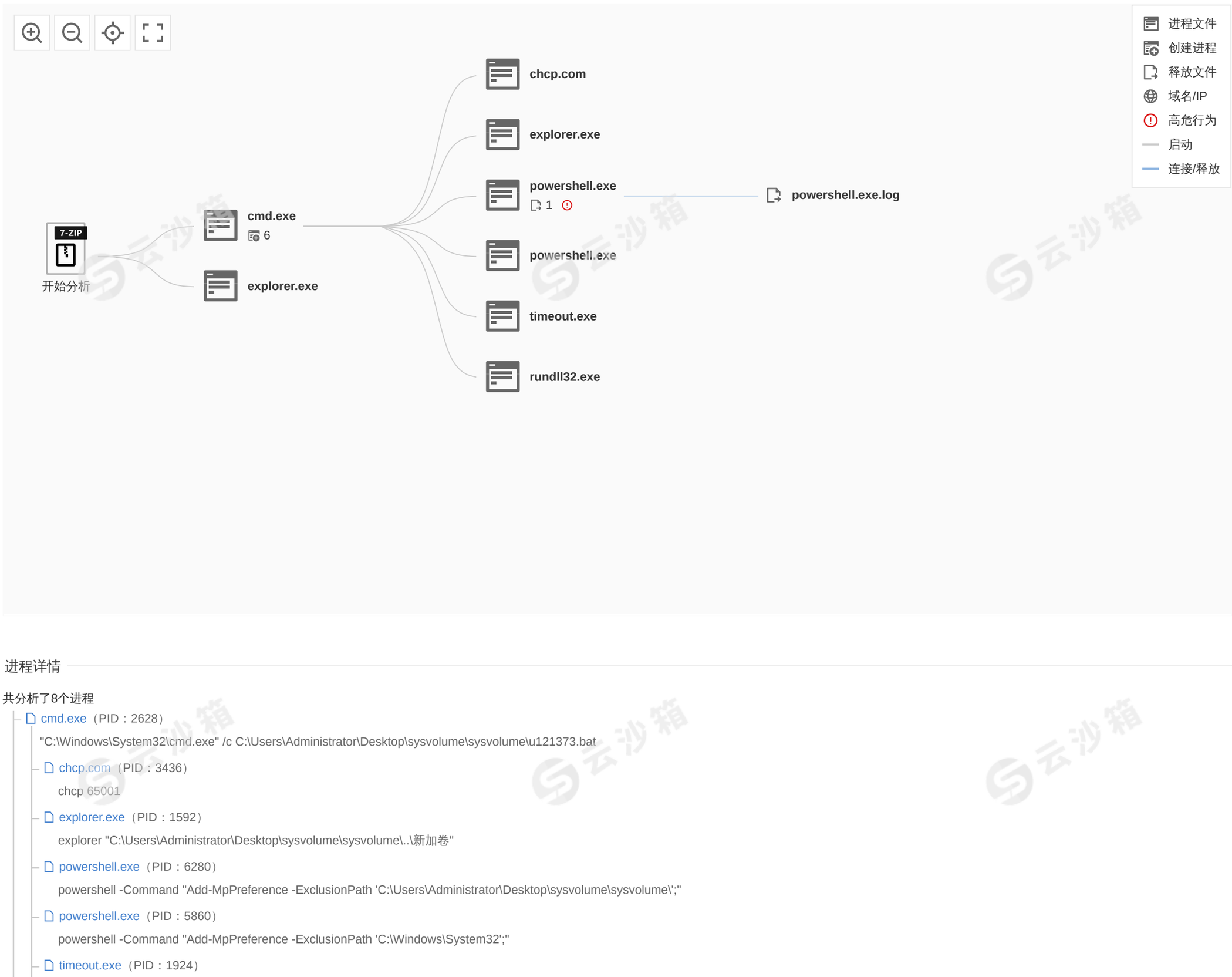
子文件详情(5)

文件	Magic	文件大小	修改时间	
sysvolume\u121373.bat	DOS batch file, UTF-8 Unicode text, with CRLF line terminators	442	2025-12-25 12:01:30.4791717	展开
sysvolume\u501702.bin	data	4	2025-12-25 12:01:30.5452245	展开
sysvolume\u253774.dat	PE32+ executable (DLL) (GUI) x86-64, for MS Windows	12669952	2025-12-25 10:40:34.5800757	展开
sysvolume\u377573.dll	PE32+ executable (DLL) (GUI) x86-64, for MS Windows	6658048	2025-12-25 10:39:06.8654000	展开
sysvolume\u889079.vbs	ASCII text, with CRLF line terminators	485	2025-12-25 12:01:30.4871043	展开

沙箱动态检测

Win10(1903 64bit,Office2016)

执行流程

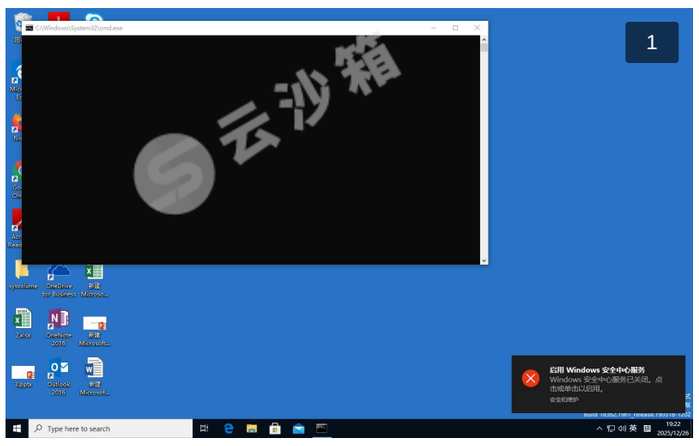


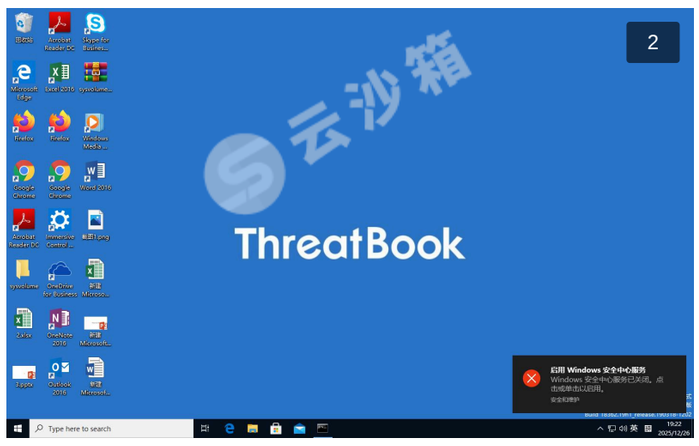
进程详情

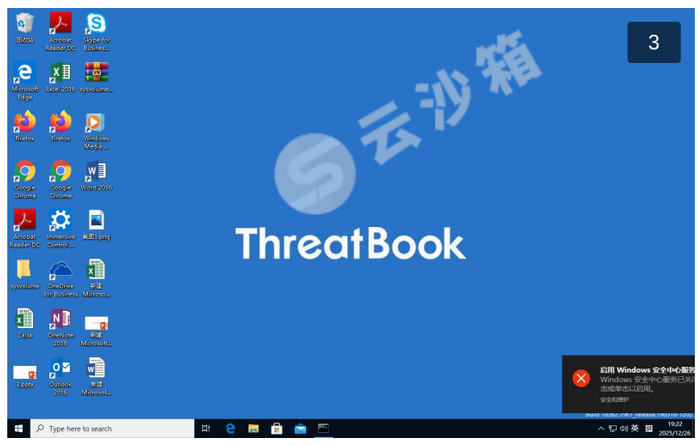
共分析了8个进程

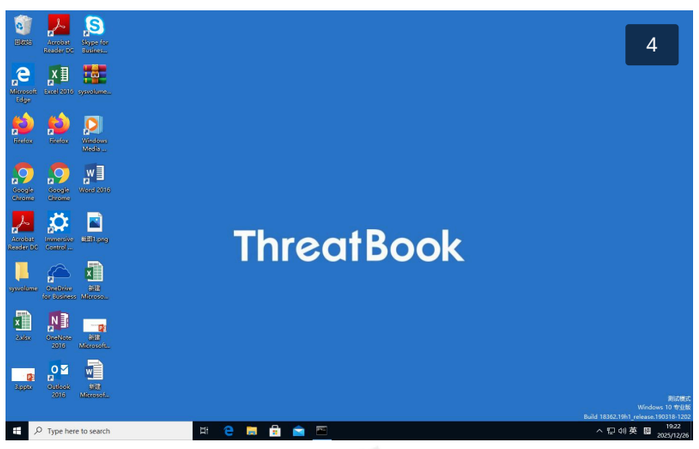
- cmd.exe（PID：2628）
  - "C:\Windows\System32\cmd.exe" /c C:\Users\Administrator\Desktop\sysvolume\sysvolume\u121373.bat
  - chcp.com（PID：3436）
    - chcp 65001
  - explorer.exe（PID：1592）
    - explorer "C:\Users\Administrator\Desktop\sysvolume\sysvolume\..\新加卷"
  - powershell.exe（PID：6280）
    - powershell -Command "Add-MpPreference -ExclusionPath 'C:\Users\Administrator\Desktop\sysvolume\sysvolume\';"
  - powershell.exe（PID：5860）
    - powershell -Command "Add-MpPreference -ExclusionPath 'C:\Windows\System32';"
  - timeout.exe（PID：1924）
    - timeout /t 3 /nobreak
  - rundll32.exe（PID：3568）
    - C:\Windows\System32\rundll32.exe C:\Windows\System32\u253774.dll,IdllEntry 1
- explorer.exe（PID：2588）
  - C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding

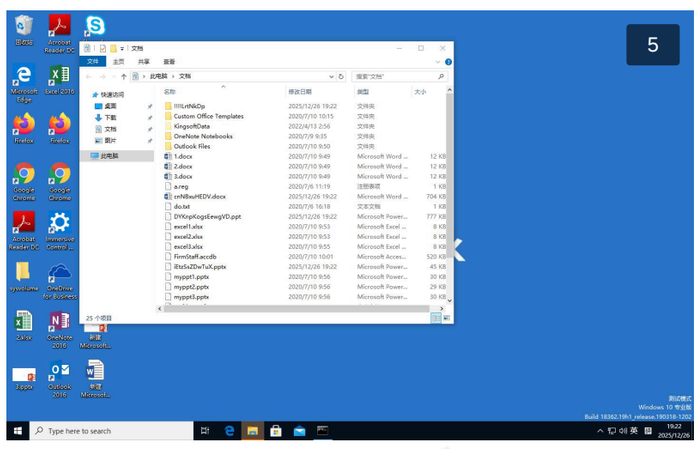
运行截图（10）

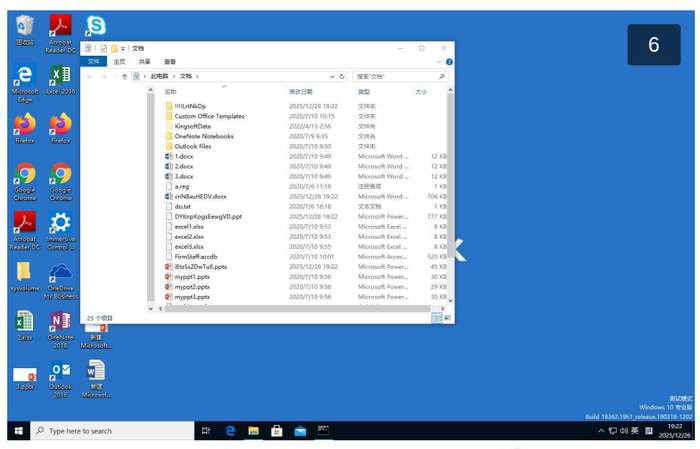


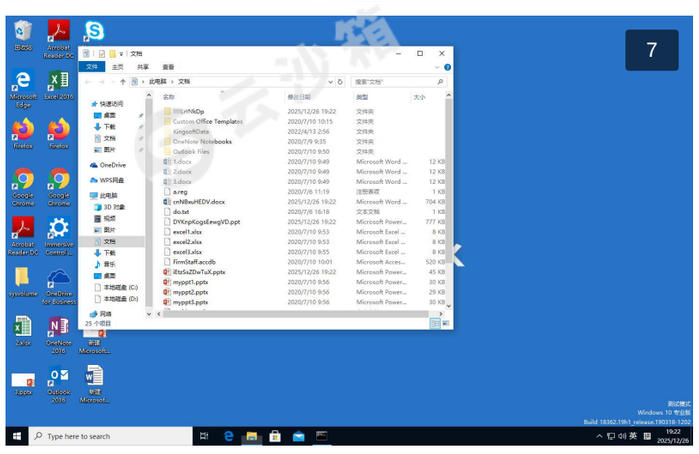


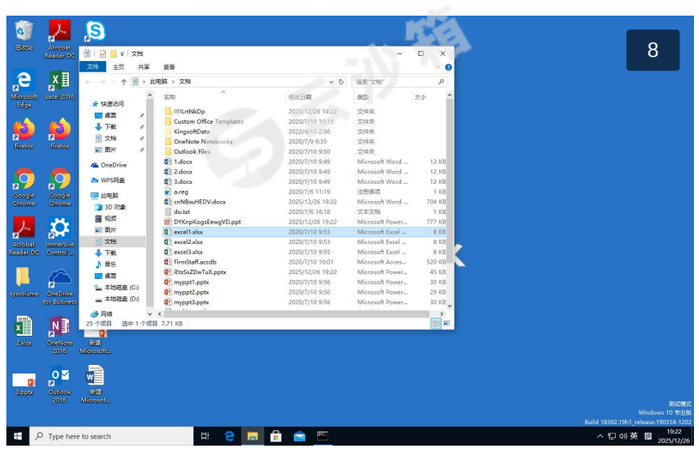


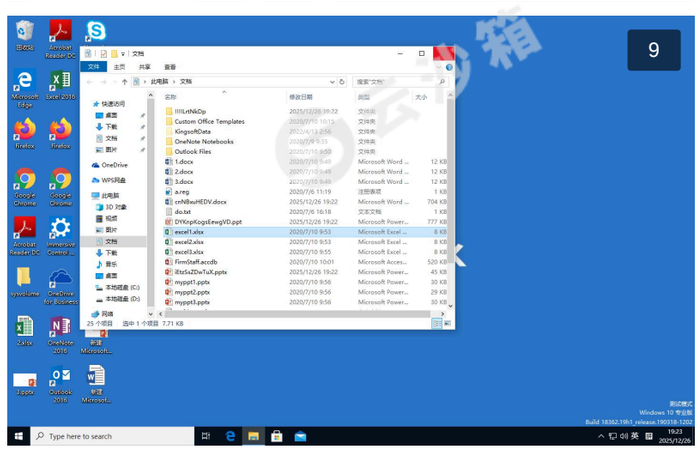


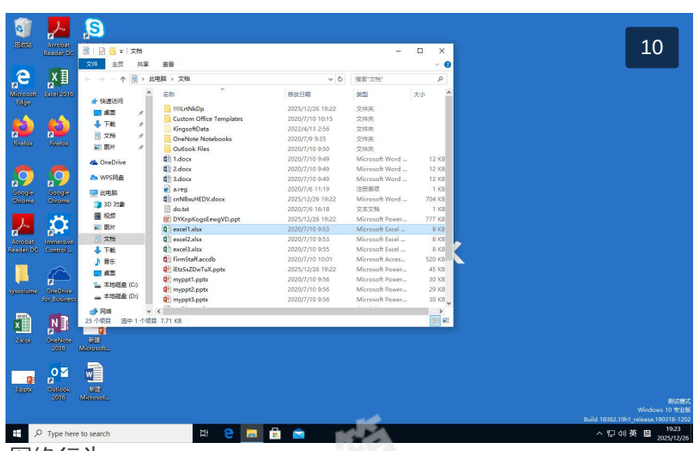












网络行为

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（1）

释放样本	进程	多引擎检出	威胁类型/木马家族	微步判定
powershell.exe.log(3.73 KB) 文件类型： CSV text 文件路径： C:\Users\Administrator\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\powershell.exe.log SHA256： 190193e95223640e734b260c6bd338d87eac2f2fef24d4ced35a9b1f75bdff72	（6280）powershell.exe	0/28	-	未知