样本分析报告

文件名称： SunCoordinates.exe

SHA256： f68e5700bfc538313ad9e00eaba07bafa83e7edaf323d399d7fc6569500d7a5c

文件大小： 7.11 MB

文件类型： PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections

分析环境： Win10(1903 64bit,Office2016) Win7(64bit,Office2013)

微步判定： 安全

云沙箱

目录

SunCoordinates.exe

安全

首次提交: 2025/06/08　末次提交: 2025/06/08　末次分析: 2025/06/08 10:52:18

文件大小：	7.11 MB	文件类型：	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
引擎检出：	0 / 24	分析环境：	Win10(1903 64bit,Office2016)　Win7(64bit,Office2013)

HASH

SHA256: f68e5700bfc538313ad9e00eaba07bafa83e7edaf323d399d7fc6569500d7a5c

MD5: 02ccb9c70330193438a682db72c44661

SHA1: 2e05e42505ba79d7d8695e4cbcb69a29931f345a

行为检测

MITRE ATT&CK™ 矩阵（技术）检测到 **5** 条技术指标。 查看完整结果

全部分析环境签名

可疑行为 (6)

一般行为	感知时区，常用于躲避恶意软件分析系统	2 个分析环境
信息搜集	获取按键信息	2 个分析环境
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	2 个分析环境
	这个二进制可能包含被加密或被压缩的数据，可能被加壳	2 个分析环境
	尝试拖慢分析任务的进度	Win7(64bit,Office2013)
系统敏感操作	检查系统上的唯一标识符是否具有可疑的权限	2 个分析环境

通用行为 (9)

一般行为	枚举文件和目录	Win10(1903 64bit,Office2016)
	这个可执行文件存在调试数据库文件（PDB）路径	2 个分析环境
	读取系统支持的语言信息	Win7(64bit,Office2013)
系统环境探测	获取系统信息	2 个分析环境
	包含查询计算机时区的功能	2 个分析环境
	读取计算机名称	Win10(1903 64bit,Office2016)
	查询计算机名	Win7(64bit,Office2013)
静态文件特征	PE文件的节大小异常	2 个分析环境
	样本的时间戳异常	2 个分析环境

多维检测

Sigma 规则 (2)

Win10(1903 64bit,Office2016)

标题	描述	标签	危险等级	匹配项	源	分析环境
Autorun Keys Modification	Detects modification of autostart extensibility point (ASEP) in …	persistence; t1547.001; t1060	中	查看	SigmaHQ	Win10(1903 …
New Application in AppCompat	A General detection for a new application in AppCompat. Thi…	execution; t1204.002	info	查看	SigmaHQ	Win10(1903 …

多引擎检测

检出率：**0** / 24

最近检测时间：2025-06-08 10:49:01

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

引擎	检出	引擎	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
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	f68e5700bfc538313ad9e00eaba07bafa83e7edaf323d399d7fc6569500d7a5c
文件格式	EXEx86
文件类型(Magic)	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
文件大小	7.11MB
SHA256	f68e5700bfc538313ad9e00eaba07bafa83e7edaf323d399d7fc6569500d7a5c
SHA1	2e05e42505ba79d7d8695e4cbcb69a29931f345a
MD5	02ccb9c70330193438a682db72c44661
CRC32	2D2E8E41
SSDEEP	98304:seeeTlLtUHQYsqs8v74A3R8eqdVLih/YQIUAJjTtnJP+s:seeeTlLtUHp4e8eaVOoUGjhJP
TLSH	T1EB765B51E3001584D05CCFF88C1344F05AE1AF96AA90959AA6563EB7FFD4B9FCB2318E
AuthentiHash	F6E2FAC60C7DEA4BA6B7927823093A468DE35B639072561496596768D62930F9
peHashNG	e4d296c80049072b563227e1b04668b5e6c9f164af794c3b3ea540d3e6904e2a
impfuzzy	3:rGsLdAIEK:tf
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
MVID	b9e5bf31-c9ad-4ffa-af06-556a08bb99a8
TLID	078f908c-9390-40fa-91a2-221406057a31
ICON SHA256	621d097a407f58b5921d8a1aaf0ad44482ba4b7ddaf49057d055f9c060a2d8ad
ICON DHash	a0b4a6aa9c9e7efe
Tags	exe,pdb_path,lang_neutral,timestamp_exception

元数据

ExifTool

FileType	Win32 EXE
FileTypeExtension	exe
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
TimeStamp	2046:11:21 15:22:58+08:00
ImageFileCharacteristics	Executable, Large address aware
PEType	PE32
LinkerVersion	48.0
CodeSize	6743552
InitializedDataSize	706560
UninitializedDataSize	0
EntryPoint	0x609072
OSVersion	4.0
ImageVersion	0.0
SubsystemVersion	6.0
Subsystem	Windows GUI
FileVersionNumber	1.0.0.0
ProductVersionNumber	1.0.0.0
FileFlagsMask	0x003f
FileFlags	(none)
FileOS	Win32
ObjectFileType	Executable application
FileSubtype	0
LanguageCode	Neutral
CharacterSet	Unicode
Comments	
CompanyName	个人
FileDescription	SunCoordinates
FileVersion	1.0.0.0
InternalName	SunCoordinates.exe
LegalCopyright	Copyright © HP 2025
LegalTrademarks	
OriginalFileName	SunCoordinates.exe
ProductName	SunCoordinates
ProductVersion	1.0.0.0

AssemblyVersion	1.0.0.0

TrID

71.1% (.EXE)	Generic CIL Executable (.NET, Mono, etc.) (73123/4/13)
10.2% (.EXE)	Win64 Executable (generic) (10523/12/4)
6.3% (.DLL)	Win32 Dynamic Link Library (generic) (6578/25/2)
4.3% (.EXE)	Win32 Executable (generic) (4505/5/1)
2.0% (.ICL)	Windows Icons Library (generic) (2059/9)

DIE

链接器	Microsoft Linker()
Library	.NET(v4.0.30319)
字节序	LE
模式	32
程序类型	GUI
文件类型	PE32
熵	7.319153376602532
语言	C#
操作系统	Windows(95)[I386, 32位, GUI]

格式深度分析

文档分析

PE头信息

平台	Intel 386 or later processors and compatible processors
子系统	Windows graphical user interface (GUI) subsystem
编译时间戳	2046-11-21 15:22:58
入口点(OEP)	0x609072
入口所在段	.text
镜像基地址	0x400000
节区数量	3
LinkerVersion	48

PE版本信息

文件说明	SunCoordinates
文件版本	1.0.0.0
产品名称	SunCoordinates
产品版本	1.0.0.0
内部名称	SunCoordinates.exe
原始文件名	SunCoordinates.exe
注释	
语言	0x0000 0x04b0
版权	Copyright © HP 2025

调试信息

PDB	D:\程序\SunCoordinates\obj\Debug\SunCoordinates.pdb
GUID	-

签名信息

签名验证	Unsigned

导入表(1)

DLL	DLL描述	函数数量	
mscoree.dll	-	1	展开

PE节区(3)

节名	虚拟地址	虚拟大小	物理地址	物理大小	节权限	熵值	节哈希
.text	0x00002000	0x0066e518	0x00000200	0x0066e600	R-E	7.464615503744996	c82ee07ced69570da042fbd7fdcb18c0
.rsrc	0x00672000	0x000ac4a8	0x0066e800	0x000ac600	R--	4.934200927334346	07f40edb1eeab685001700544dda5ece
.reloc	0x00720000	0x0000000c	0x0071ae00	0x00000200	R--	0.10191042566270775	761c1eea629ae49a1c24f4a2aec259ec

PE资源(16)

资源名	资源类型	资源大小	偏移地址	语言	子语言
RT_ICON	GLS_BINARY_LSB_FIRST	0x00000468	0x00672280	LANG_NEUTRAL	SUBLANG_NEUTRAL
RT_ICON	data	0x000006b8	0x006726f8	LANG_NEUTRAL	SUBLANG_NEUTRAL
RT_ICON	data	0x00000988	0x00672dc0	LANG_NEUTRAL	SUBLANG_NEUTRAL
RT_ICON	data	0x000010a8	0x00673758	LANG_NEUTRAL	SUBLANG_NEUTRAL
RT_ICON	data	0x00001a68	0x00674810	LANG_NEUTRAL	SUBLANG_NEUTRAL

文件内容

字符串

Unicode ASCII

输入搜索内容

```
EET -
UTC-11 ( MIT -
MtsmGotoForGLongLatDecimal
CtsmShowTwilight
LblMorning
TxtTimeOfDay
```

复制 下载

沙箱动态检测

Win10(1903 64bit,Office2016)

执行流程

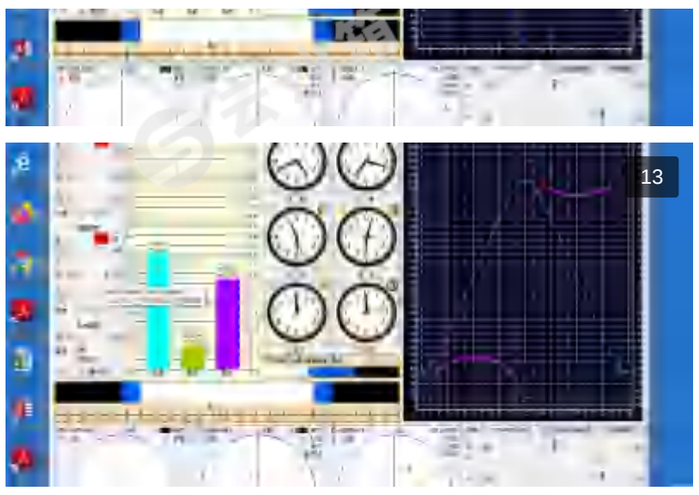
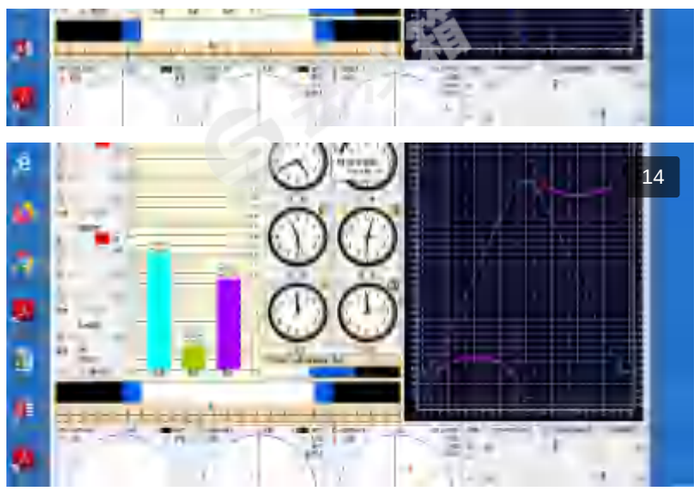
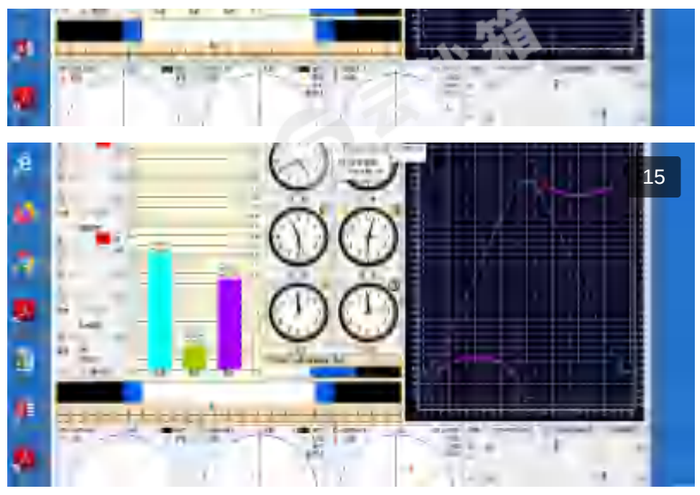
进程详情

共分析了1个进程

SunCoordinates.exe（PID：6828）

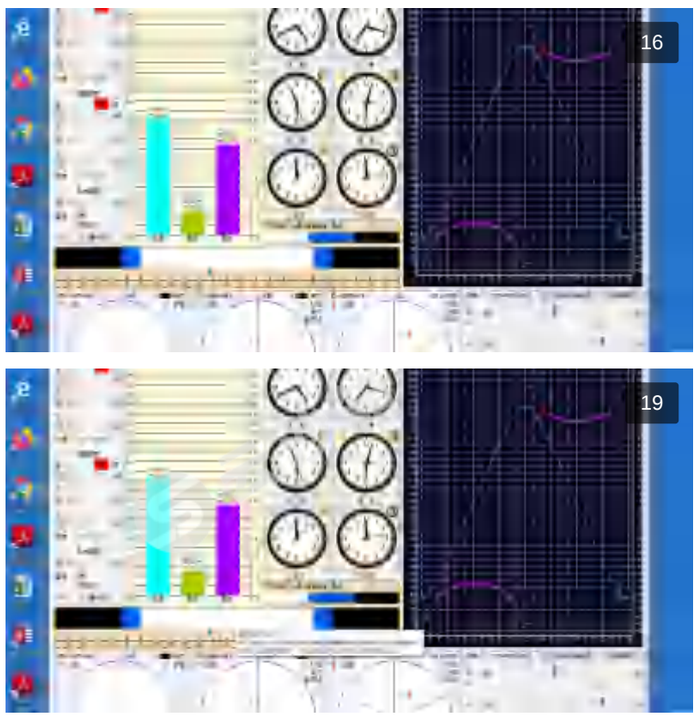
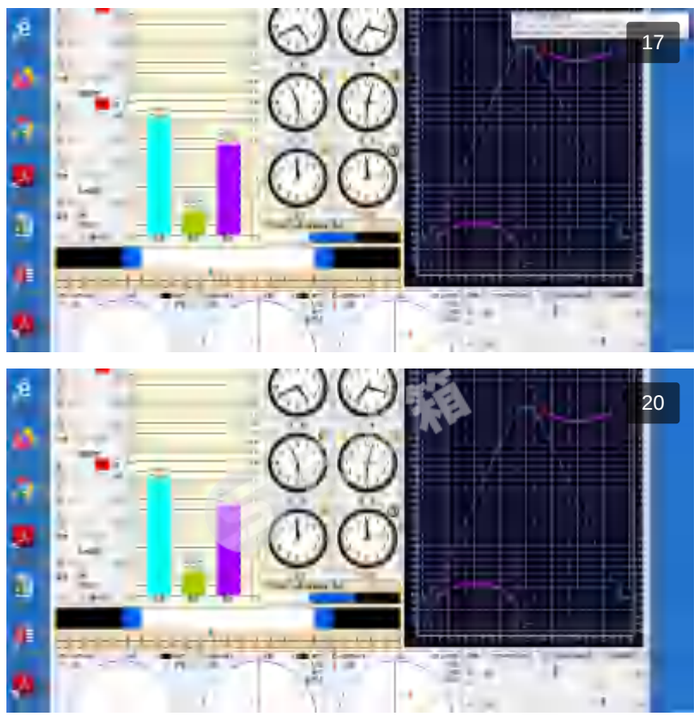
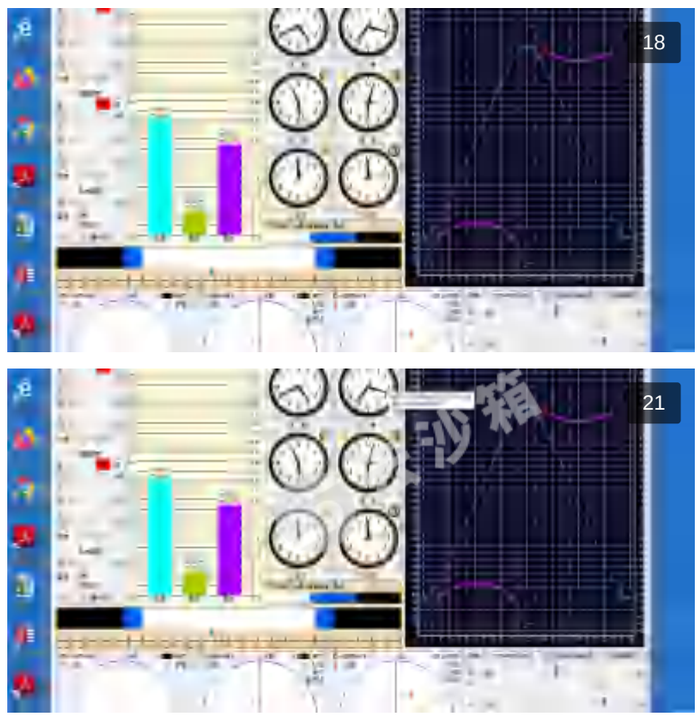
"C:\Users\Administrator\Desktop\SunCoordinates.exe"

运行截图（64）

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

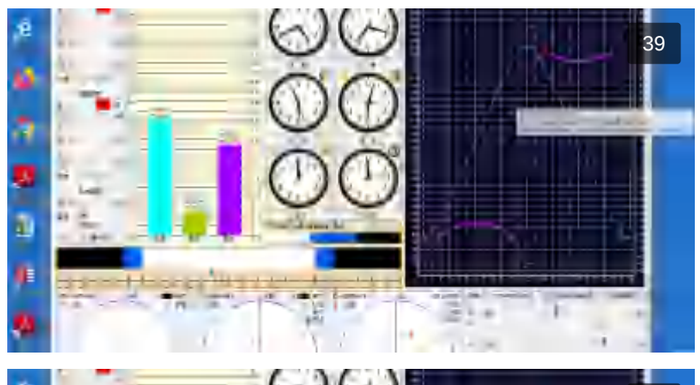
33

34

35

36

37

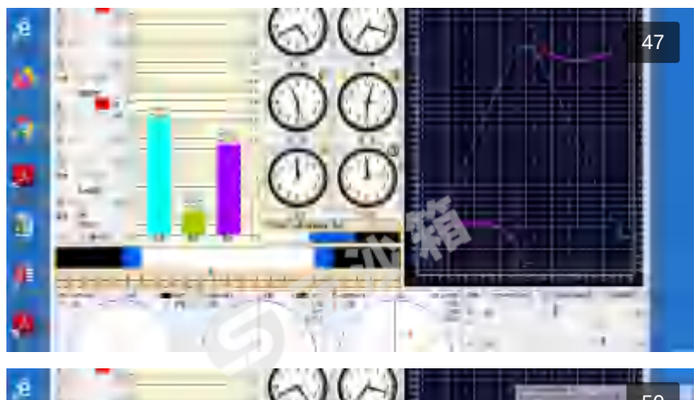
38

39

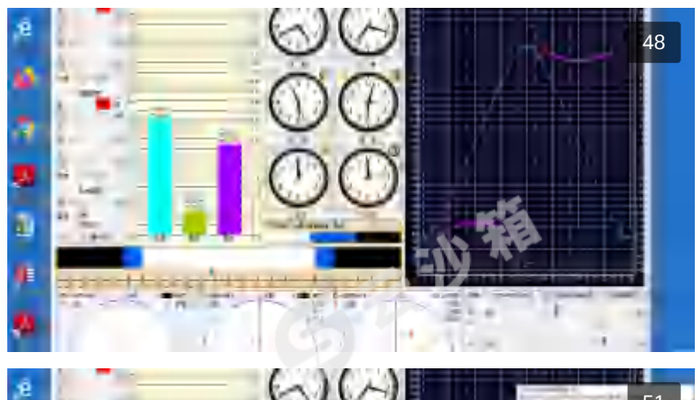
40

41

42





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
SunCoordinatesSet.xml(3.8 KB)	（6828）SunCoordinates.exe	0/23	-	安全

释放样本	进程	多引擎检出	威胁类型/木马家族	微步判定
文件类型： XML 1.0 document, ISO-8859 text, with CRLF line terminators 文件路径： C:\Users\Administrator\Desktop\SunCoordinatesSet.xml SHA256： c3a020417358bc509a7e85a7a3d35e85b086df6a86d192149db0881a1a6df695				

Win7(64bit,Office2013)

执行流程

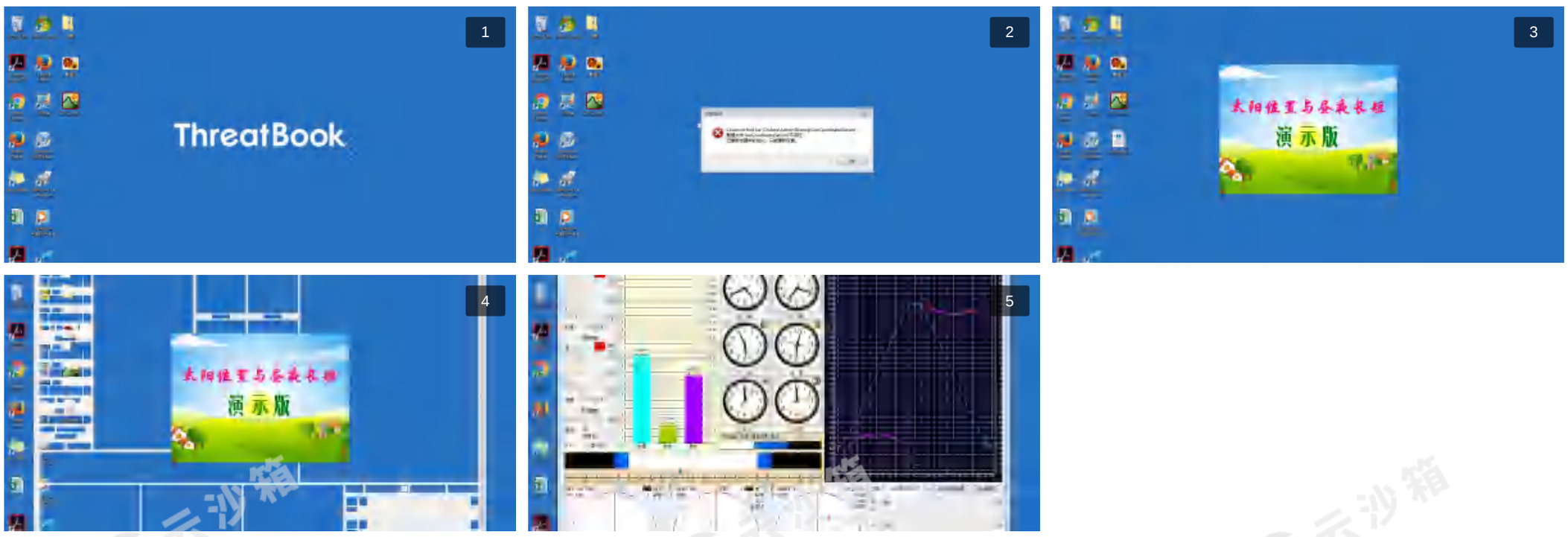
进程详情

共分析了1个进程

└ SunCoordinates.exe（PID：2816）

"C:\Users\Admin\Desktop\SunCoordinates.exe"

运行截图（5）



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
SunCoordinatesSet.xml(3.8 KB) 文件类型： XML 1.0 document, ISO-8859 text, with CRLF line terminators 文件路径： C:\Users\Admin\Desktop\SunCoordinatesSet.xml SHA256： c3a020417358bc509a7e85a7a3d35e85b086df6a86d192149db0881a1a6df695	（2816）SunCoordinates.exe	0/23	-	安全