样本分析报告

文件名称： 图片工具_1.3.0_x64-setup.exe

SHA256： 3f4015c72410b8721cd21496411a64955c8fe0621b38626cabde85b9999f617d

文件大小： 6.17 MB

文件类型： PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive, 5 sections

分析环境： Win10(1903 64bit,Office2016)

微步判定： 未知

云沙箱

目录

1 行为检测

2 多维检测

3 引擎检测

4 静态分析

5 动态分析

图片工具_1.3.0_x64-setup.exe

首次提交: 2026/10/04　末次提交: 2026/10/04　末次分析: 2026/10/04 12:20:00

文件大小： 6.17 MB　文件类型： PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting…

引擎检出： 0 / 28　分析环境： Win10(1903 64bit,Office2016)

未知

HASH

SHA256: 3f4015c72410b8721cd21496411a64955c8fe0621b38626cabde85b9999f617d

MD5: f96e6440bf782cf29c2b4b9da9bf85e9

SHA1: b977ac0ff63aaaa2467850a22f46b12c1f04d6eb

行为检测

MITRE ATT&CK™ 矩阵（技术）检测到 **4** 条技术指标。 查看完整结果　Win10(1903 64bit,Office2016)

高危行为 (2)

系统环境探测	收集有关已安装应用程序的信息
系统敏感操作	在用户目录下创建可执行文件

可疑行为 (6)

一般行为	将文件属性设置为删除
信息搜集	获取按键信息
	安装消息钩子
恶意行为特征	疑似创建Shellcode
持久化	创建快捷方式
系统敏感操作	枚举进程或线程

通用行为 (7)

一般行为	在临时目录中创建文件
系统环境探测	查询计算机名
	获取系统信息
系统敏感操作	调用COM相关API
	在文件系统上创建可执行文件
	向系统软件管理程序注册了卸载方法
静态文件特征	安装程序

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
PsExec Tool Execution	Detects PsExec service installation and execution events (se…	execution; t1035; t1569.002; s0029	低	查看	SigmaHQ	Win10(1903 …
PsExec Service Start	Detects a PsExec service start	execution; t1035; s0029; t1569.002	低	查看	SigmaHQ	Win10(1903 …

多引擎检测

重新分析

检出率：0 / 28

最近检测时间：2026-10-04 12:14:56

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	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

云沙箱

收起全部

静态分析

基础信息

文件名称	3f4015c72410b8721cd21496411a64955c8fe0621b38626cabde85b9999f617d
文件格式	NSIS
文件类型(Magic)	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
文件大小	6.17MB
SHA256	3f4015c72410b8721cd21496411a64955c8fe0621b38626cabde85b9999f617d
SHA1	b977ac0ff63aaaa2467850a22f46b12c1f04d6eb
MD5	f96e6440bf782cf29c2b4b9da9bf85e9
CRC32	9E3568A1
SSDEEP	98304:LckRBhvDrjqtgpgd4ixi7/G7cFA0DDEVEfQPxc6xCnk9GWCn4y9RyNCs4FDp:LckRzDPtgyixiU0B4J70k0Xq4b
TLSH	T1A056336CBB051E66C40159B3367027055B7B8D7E24A8992D3B94CF8D3AADB32F910FC6
peHashNG	dc68786d4c804643b53c32aa7dede397b158b2c9c8148ef4d8abf9d9f61c6513
RichHash	dbbea5de38bb665ba46f5da13ef89ab8
impfuzzy	48:7/dKePusa/toE77+nzEqQ7/allLHAOe+ztlkAOr8L5Sv0WbP06Uyv5/1byAknBod:bdKemvafl5A66PF84JB
ImpHash	46ce5c12b293febbeb513b196aa7f843
ICON SHA256	ffd2ef3dbabbd38ace0630c0a7cac30192719d4aaf2cd5c13be4d1e0e9dcfd98
ICON DHash	71c08cf8d8dcc870
Tags	exe,lang_english

元数据

ExifTool

CharacterSet	Unicode
CodeSize	26624
EntryPoint	0x369f
FileDescription	图片工具
FileFlags	(none)
FileFlagsMask	0x0000
FileOS	Win32
FileSubtype	0
FileType	Win32 EXE
FileTypeExtension	exe
FileVersion	1.3.0
FileVersionNumber	1.3.0.0
ImageFileCharacteristics	No relocs, Executable, No line numbers, No symbols, 32-bit
ImageVersion	6.0
InitializedDataSize	139776
LanguageCode	English (U.S.)
LegalCopyright	
LinkerVersion	6.0
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
OSVersion	4.0
ObjectFileType	Executable application
PEType	PE32
ProductName	图片工具
ProductVersion	1.3.0
ProductVersionNumber	1.3.0.0
Subsystem	Windows GUI
SubsystemVersion	4.0
TimeStamp	2025:03:09 07:05:20+08:00
UninitializedDataSize	2048

TrID

47.3% (.EXE)	Win32 Executable MS Visual C++ (generic) (31206/45/13)
15.9% (.EXE)	Win64 Executable (generic) (10523/12/4)
9.9% (.DLL)	Win32 Dynamic Link Library (generic) (6578/25/2)

7.6% (.EXE)	Win16 NE executable (generic) (5038/12/1)
6.8% (.EXE)	Win32 Executable (generic) (4505/5/1)

Magika

Mime_type	application/x-dosexec
分类 (Group)	executable
描述信息 (Description)	PE Windows executable

格式深度分析

格式详情

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	2025-03-09 07:05:20
入口点(OEP)	0x369f
入口所在段	.text
镜像基地址	0x400000
节区数量	5
LinkerVersion	6

PE版本信息

文件说明	图片工具
文件版本	1.3.0
产品名称	图片工具
产品版本	1.3.0
语言	0x0409 0x04b0
版权	

导入表(7)

DLL	DLL描述	函数数量	
ADVAPI32.dll	-	12	展开
SHELL32.dll	-	5	展开
ole32.dll	-	5	展开
COMCTL32.dll	-	4	展开
USER32.dll	-	64	展开

查看全部

PE节区(5)

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	0x00001000	0x00006711	0x00000400	0x00006800	R-E	6.454334667833774	afb6c5993570f82e85ec446bbb886505
.rdata	0x00008000	0x00001358	0x00006c00	0x00001400	R--	5.0996952412494 63	e913094d8cceaca6b405bbbb52936387
.data	0x0000a000	0x0001fb78	0x00008000	0x00000600	RW-	4.12304901988063	9d011beba2fe64a93f62fbb227cc9c35
.ndata	0x0002a000	0x0002e000	0x00000000	0x00000000	RW-	0	d41d8cd98f00b204e98

PE资源(15)

资源名	资源类型	资源大小	偏移地址	语言	子语言
RT_ICON	data	0x000010a8	0x00058358	LANG_ENGLISH	SUBLANG_ENGLISH_US
RT_ICON	data	0x00000ea8	0x00059400	LANG_ENGLISH	SUBLANG_ENGLISH_US
RT_ICON	data	0x000008a8	0x0005a2a8	LANG_ENGLISH	SUBLANG_ENGLISH_US
RT_ICON	GLS_BINARY_LSB_FIRST	0x00000568	0x0005ab50	LANG_ENGLISH	SUBLANG_ENGLISH_US
RT_ICON	GLS_BINARY_LSB_FIRST	0x00000468	0x0005b0b8	LANG_ENGLISH	SUBLANG_ENGLISH_US

文件内容

字符串

Unicode ASCII

输入搜索内容

```
Error launching installer
http://nsis.sf.net/NSIS_Error
%s%S.dll
Error writing temporary file. Make sure your temp folder is valid.
More information at:
unpacking data: %d%%
```

复制 下载

URLs

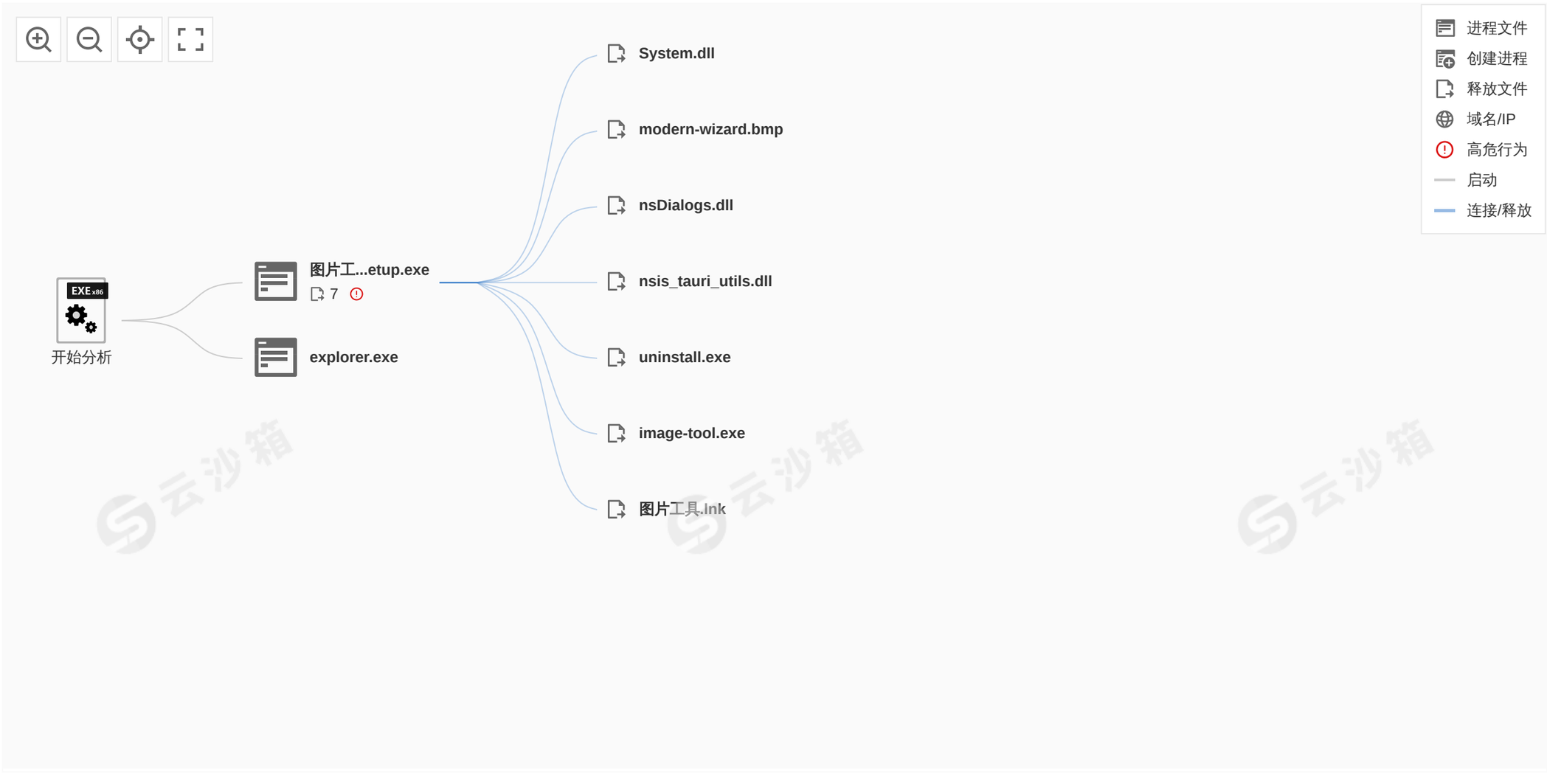
http://schemas.microsoft.com/SMI/2016/WindowsSettings

> http://schemas.microsoft.com/SMI/2005/WindowsSettings

沙箱动态检测

Win10(1903 64bit,Office2016)

执行流程

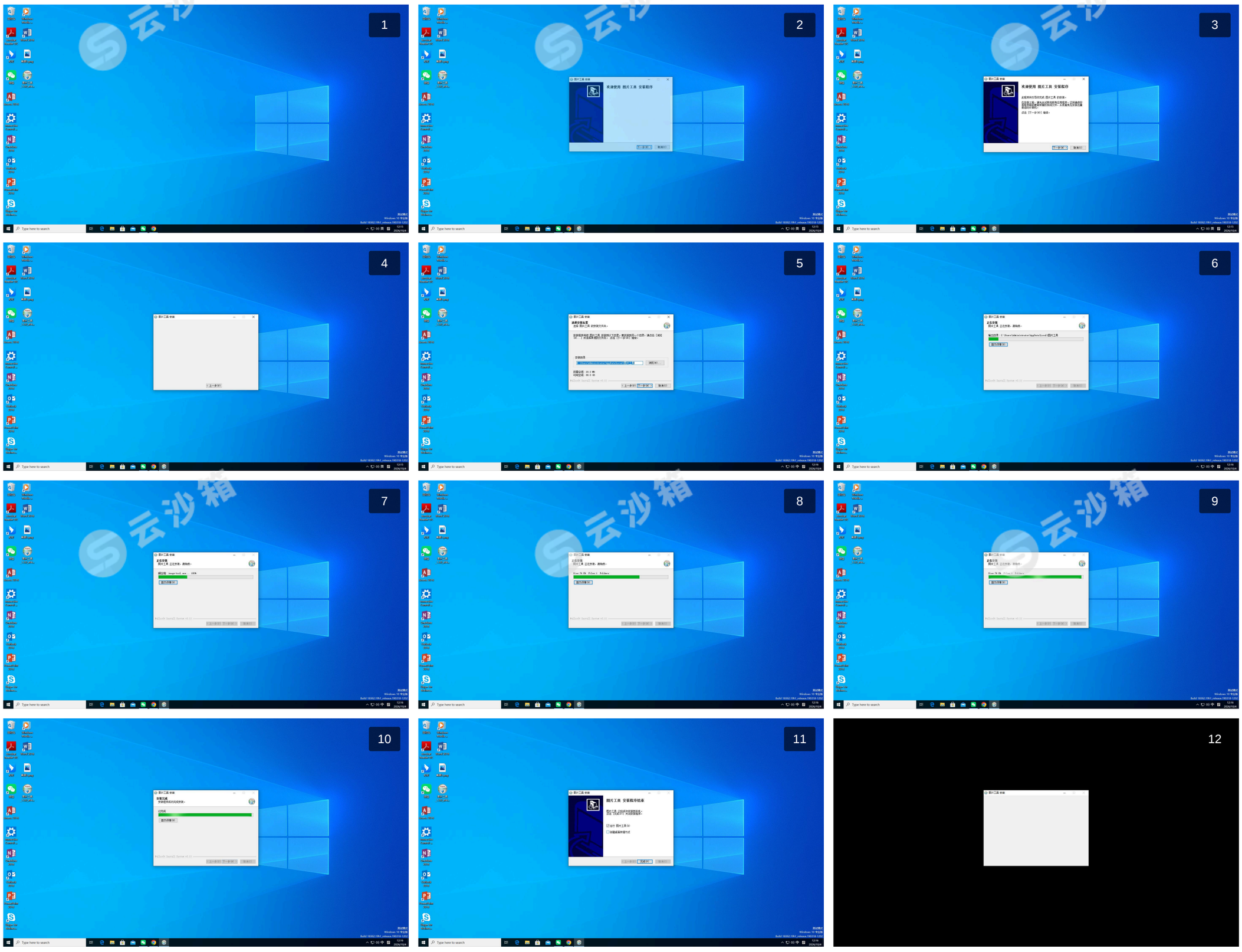


进程详情

共分析了2个进程

- 图片工具_1.3.0_x64-setup.exe（PID：2436）
  "C:\Users\Administrator\Desktop\图片工具_1.3.0_x64-setup.exe"
- explorer.exe（PID：3344）
  C:\Windows\Explorer.EXE

运行截图（15）









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（7）

释放样本	进程	多引擎检出	威胁类型/木马家族	微步判定
System.dll(12 KB) 文件类型： PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, 4 sections 文件路径： C:\Users\Administrator\AppData\Local\Temp\nsm32C6.tmp\System.dll SHA256： 8b4c47c4cf5e76ec57dd5a050d5acd832a0d532ee875d7b44f6cdaf68f90d37c	（2436）图片工具_1.3.0_x64-setup.exe	0/28	-	未知
modern-wizard.bmp(25.87 KB) 文件类型： PC bitmap, Windows 3.x format, 164 x 314 x 4, image size 26376, resolution 2834 x 2834 px/m, cbSize 26494, bits offset 118 文件路径： C:\Users\Administrator\AppData\Local\Temp\nsm32C6.tmp\modern-wizard.bmp SHA256： 3ad2dc318056d0a2024af1804ea741146cfc18cc404649a44610cbf8b2056cf2	（2436）图片工具_1.3.0_x64-setup.exe	0/28	-	未知
nsDialogs.dll(9.5 KB) 文件类型： PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, 5 sections 文件路径： C:\Users\Administrator\AppData\Local\Temp\nsm32C6.tmp\nsDialogs.dll SHA256： b1350f487692057c8ffde75dcc55287a52a3272240d4d4912f24464b27551fc0	（2436）图片工具_1.3.0_x64-setup.exe	0/28	-	未知
nsis_tauri_utils.dll(32.5 KB) 文件类型： PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, 4 sections 文件路径： C:\Users\Administrator\AppData\Local\Temp\nsm32C6.tmp\nsis_tauri_utils.dll SHA256： f3e9b0d43b66fa6b05d2fa4de4547517a3ec0bc0b14de3c349d817465bbf7ab4	（2436）图片工具_1.3.0_x64-setup.exe	0/28	-	未知
image-tool.exe(18.62 MB) 文件类型： PE32+ executable (GUI) x86-64, for MS Windows, 7 sections 文件路径： C:\Users\Administrator\AppData\Local\图片工具\image-tool.exe SHA256： 506d8ab52deac3c6ab1c943381e800f96521a44c94ce87f10030151b7d5de551	（2436）图片工具_1.3.0_x64-setup.exe	0/27	-	未知