样本分析报告

文件名称： sickly_days.exe

SHA256： 08e76d0abba967b416b2f79ac840f692ae5904185e71da4c9054c91abb81246d

文件大小： 4.35 MB

文件类型： PE32 executable (GUI) Intel 80386, for MS Windows, 7 sections

分析环境： Win10(1903 64bit,Office2016)

微步判定： 未知

云沙箱

目录

sickly_days.exe

首次提交: 2026/01/05　末次提交: 2026/01/05　末次分析: 2026/01/05 22:06:53

文件大小： 4.35 MB　文件类型： PE32 executable (GUI) Intel 80386, for MS Windows, 7 sections

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

未知

HASH

SHA256: 08e76d0abba967b416b2f79ac840f692ae5904185e71da4c9054c91abb81246d

MD5: 1ae55ce989a346d410d29ddb7afb90c5

SHA1: bcf8ba1d39d7a69a3e5fb0bd05328a2d2f1609ae

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)

系统敏感操作	在用户目录下创建可执行文件

可疑行为 (3)

一般行为	感知时区，常用于躲避恶意软件分析系统
信息搜集	获取按键信息
反逆向工程	这个二进制可能包含被加密或被压缩的数据，可能被加壳

通用行为 (6)

一般行为	在临时目录中创建文件
	这个可执行文件存在调试数据库文件（PDB）路径
系统环境探测	包含查询计算机时区的功能
系统敏感操作	在文件系统上创建可执行文件
静态文件特征	在文件内存中发现IP地址或URL
	该可执行文件使用了已经公开的软件保护壳

多引擎检测

检出率：0 / 28　最近检测时间：2026-01-05 22:06:44

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	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	08e76d0abba967b416b2f79ac840f692ae5904185e71da4c9054c91abb81246d
文件格式	EXEx86
文件类型(Magic)	PE32 executable (GUI) Intel 80386, for MS Windows
文件大小	4.35MB
SHA256	08e76d0abba967b416b2f79ac840f692ae5904185e71da4c9054c91abb81246d
SHA1	bcf8ba1d39d7a69a3e5fb0bd05328a2d2f1609ae
MD5	1ae55ce989a346d410d29ddb7afb90c5
CRC32	6C4FB4EB
SSDEEP	98304:l69SFlOydqj7YmAUblxLSlwfJwlBAmA5qPdphw3u:Q2lOydqjvArLxJwNAwphwe
TLSH	T1FF26AE21BB92C17AE9F202B19A7DAF5F202CBE25173840DB72D81D5D19B06D32B36717
AuthentiHash	7CA35A23E6CD6B3CE4E28752A0B80D4C52D14F2984E0B538274B33625F286BCB
peHashNG	3dc9b9296f8911bbccd40e1c32bd4fe073f72f49293ad5ba6fdee846e614fedc
impfuzzy	96:dXYKYXeX1fnXpJYpSLR1GnGtjFJ+SnfcpfiUVPrCUCzJ/VEl:YuFfnZPRz+S7UVPOUCN0
ImpHash	277b6e27b5785f425f2394d28495d60e
ICON SHA256	29253aaa06b96813826cb59715a712fc4c94e22dedf99ef389aa0260599ffc96
ICON DHash	6791c306bebab6fa
Tags	exe,pdb_path,lang_japanese,encrypt_algorithm

元数据

ExifTool

CharacterSet	Unicode
CodeSize	2878464
Comments	sister position
EntryPoint	0x239e03
FileDescription	痴情哥哥與病弱妹妹的鄉間生活
FileFlags	(none)
FileFlagsMask	0x003f
FileOS	Windows NT 32-bit
FileSubtype	0
FileType	Win32 EXE
FileTypeExtension	exe
FileVersion	1.2.0.3
FileVersionNumber	1.2.0.3
ImageFileCharacteristics	Executable, Large address aware, 32-bit
ImageVersion	0.0
InitializedDataSize	1494016
InternalName	tvp2/win32
LanguageCode	Chinese (Traditional)
LegalCopyright	(KIRIKIRI core) (C) W.Dee and contributors All Rights Reserved. This software is based in part on the work of Independent JPEG Group. For details: Run this program with '-about' option.
LinkerVersion	11.0
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
OSVersion	5.1
ObjectFileType	Executable application
OriginalFileName	tvpwin32.exe
PEType	PE32
ProductName	TVP(KIRIKIRI) Z core / Scripting Platform for Win32
ProductVersion	1.2.0.3
ProductVersionNumber	1.2.0.3
Subsystem	Windows GUI
SubsystemVersion	5.1
TimeStamp	2024:12:05 14:44:13+08:00
UninitializedDataSize	0

TrID

26.1% (.EXE)	Win64 Executable (generic) (10523/12/4)
16.3% (.DLL)	Win32 Dynamic Link Library (generic) (6578/25/2)
13.7% (.FON)	Windows Font (5545/9/1)
12.5% (.EXE)	Win16 NE executable (generic) (5038/12/1)
11.1% (.EXE)	Win32 Executable (generic) (4505/5/1)

DIE

编译器	Microsoft Visual C/C++(15.00-16.00)
字节序	LE
模式	32
程序类型	GUI
文件类型	PE32
熵	6.85461037738114
语言	C/C++
操作系统	Windows(XP)[I386, 32位, GUI]

FindCrypt

FindCrypt	地址
Look for Base64 table	0x2f2fd0
Look for CRC32 [poly]	0x306d18
Look for CRC32 table	0x306b18
Look for MD5 constants	0x1cd76 0x1cd7d

	0x1cd84 0x1cd8b 0xe2ee3
Look for TEA Encryption	0x42cc62

Magika

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

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	2024-12-05 14:44:13
入口点(OEP)	0x239e03
入口所在段	.text
镜像基地址	0x400000
节区数量	7
LinkerVersion	11

PE版本信息

文件说明	痴情哥哥與病弱妹妹的鄉間生活
文件版本	1.2.0.3
产品名称	TVP(KIRIKIRI) Z core / Scripting Platform for Win32
产品版本	1.2.0.3
内部名称	tvp2/win32
原始文件名	tvpwin32.exe
注释	sister position
语言	0x0404 0x04b0
版权	(KIRIKIRI core) (C) W.Dee and contributors All Rights Reserved. This software is based in part on the work of Independent JPEG Group. For details: Run this program with '-about' option.

调试信息

PDB	tvpwin32.pdb
GUID	-

签名信息

签名验证	Unsigned

导入表(13)

DLL	DLL描述	函数数量	
KERNEL32.dll	-	164	展开
USER32.dll	-	92	展开
GDI32.dll	-	23	展开
COMDLG32.dll	-	3	展开
ADVAPI32.dll	-	3	展开

查看全部

PE节区(7)

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	0x002bf000	0x00000400	0x002be600	R-E	6.666999348766738	e8eea7e8b481559beca38d976b1c82f7
.adata	0x002c0000	0x00001000	0x002bea00	0x00000600	R-E	3.8634308709902707	c7003a12185ed27e7e3b5da2e435f086
.rdata	0x002c1000	0x000af000	0x002bf000	0x000af000	R--	5.544429336680242	b5eb99fa788de03023882762d670fbe2
.data	0x00370000	0x000ab000	0x0036e000	0x0000a600	RW-	5.684793288925671	338d8d54b050a5d217

PE资源(71)

资源名	资源类型	资源大小	偏移地址	语言	子语言
TEXT	data	0x00000048	0x0041bb7c	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	ASCII text	0x00000033	0x0041bbc4	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	UTF-8 Unicode text, with very long lines, with CRLF line terminators	0x0000b12f	0x0041bbf8	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	UTF-8 Unicode text, with very long lines, with CRLF line terminat	0x0000ea07	0x00426d28	LANG_JAPANESE	SUBLANG_DEFAULT

文件内容

字符串

Unicode ASCII

输入搜索内容

```
@Jul  9 2024 15:34:21
B0BPBpB
0123456789ABCDEF
process
belgian
HH:mm:ss
```

复制 下载

URLs

http://www.apache.org/licenses/

http://www.freetype.org

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

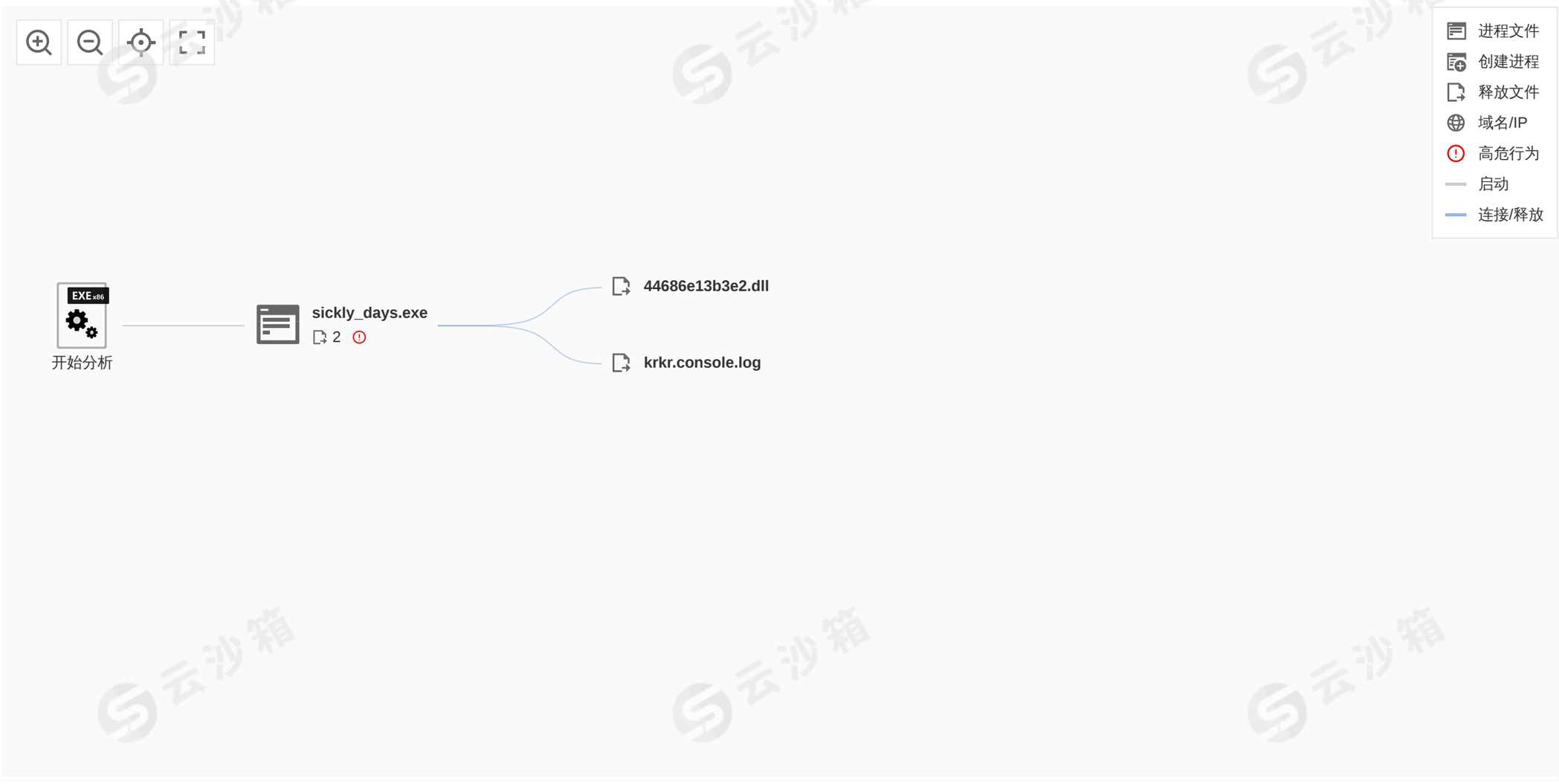
http://schemas.microsoft.com/SMI/2005/WindowsSettings

http://mozilla.org/MPL/2.0/.

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

sickly_days.exe（PID：3888）

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

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（2）

释放样本	进程	多引擎检出	威胁类型/木马家族	微步判定
44686e13b3e2.dll(745.5 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\krkr_81b07b2e58e2_277177531_3888\44686e13b3e2.dll SHA256： d3378f3a7b47835a1bcd19a8035f1b0bf2a44732204ead8e526f07bca8bd85f8	（3888）sickly_days.exe	0/28	-	未知
krkr.console.log(13.49 KB) 文件类型： Unicode text, UTF-16, little-endian text, with CRLF, LF line terminators	（3888）sickly_days.exe	0/27	-	未知

释放样本	进程	多引擎检出	威胁类型/木马家族	微步判定
文件路径： c:\Users\administrator\Desktop\savedata\krkr.console.log SHA256： 24836ee4874f5507ad6731c3a970f7c158032b02d7eac99ef0fb37c377ddca08				