

样本分析报告


文件名称：SabbatOfTheWitch.exe

SHA256：fb4466a0132238d6584a6f595da6f2eb7ce595789b6eea57cdd29919f1038d37

文件大小：4.42 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

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



未知

SabbatOfTheWitch.exe

首次提交：2026/01/03 末次提交：2026/01/03 末次分析：2026/01/03 22:47:32

文件大小：4.42 MB 文件类型：PE32 executable (GUI) Intel 80386, for MS Windows, 7 sections
引擎检出：1 / 28 分析环境： Win10(1903 64bit,Office2016)

HASH
SHA256: fb4466a0132238d6584a6f595da6f2eb7ce595789b6eea57cdd29919f1038d37
MD5: 4ae03412c4944a586f0a4b4f0851ed1e
SHA1: 4d1367ca01c3307c557d6ca0ebe2c65e0030cae1

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 (5)		
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	该可执行文件使用了已经公开的软件保护壳	▼

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
suspicious_packer_section	The packer/protector section names/keywords	fb4466a0132238d6584a6f595da6f2eb7ce595789...	查看	Github	Win10(1903 ...)

释放文件：1

规则	描述	路径	匹配项	源	分析环境
GenerateTLSClientHelloPacket_Test	(no description)	c:\Users\Administrator\AppData\Local\Temp\krkr_...	查看	Github	Win10(1903 ...)

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. This...	execution; t1204.002	info	查看	SigmaHQ	Win10(1903 ...)

多引擎检测

重新分析

检出率：1 / 28

最近检测时间：2026-01-03 22:45:18

引擎	检出	引擎	检出
江民 (JiangMin)	! Backdoor.Remcos.ebt	微软 (MSE)	无检出
ESET	无检出	卡巴斯基 (Kaspersky)	无检出

引擎	检出	引擎	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
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	fb4466a0132238d6584a6f595da6f2eb7ce595789b6eea57cdd29919f1038d37
文件格式	EXEx86
文件类型(Magic)	PE32 executable (GUI) Intel 80386, for MS Windows
文件大小	4.42MB
SHA256	fb4466a0132238d6584a6f595da6f2eb7ce595789b6eea57cdd29919f1038d37
SHA1	4d1367ca01c3307c557d6ca0ebe2c65e0030cae1
MD5	4ae03412c4944a586f0a4b4f0851ed1e
CRC32	C0883423
SSDEEP	98304:C68Y7OydqjTTsBs7SBTSJM9Hbmq5qW6K27okXwFYkz:xnOydqjcxTr9H6qiAFvz
TLSH	T17426BF11BB91C13AE9F202B19A7DAB9F502CBE241B2440CB73DC5E9D19B16D32B36717
AuthentiHash	6233E2FBADAEFF1D8370D70573E21D517993DDE8D94E234F8B9A04E0AB642947
peHashNG	54a6d65dd30baa0e4715d6078304ee95a44ef85aaa47108fe3e03e1fd0604ac9
impfuzzy	96:dXYKYXeX1fnXpJYpSLR1GnGtjFJ+SnfcpiUVPrCUCzJ/VEI:YuFfnZPRz+S7UVPOUCN0
ImpHash	277b6e27b5785f425f2394d28495d60e
ICON SHA256	a6c0231d782c07dfc6bf8180fc42d56d602551eb359bc8c9336f455c036c4139
ICON DHash	3064e0ccb7f52d97
Tags	exe,pdb_path,lang_japanese,encrypt_algorithm

元数据

ExifTool	
CharacterSet	Unicode
CodeSize	2876416
Comments	Yuzusoft/HIKARIFIELD
EntryPoint	0x239653
FileDescription	Sabbat of the Witch
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	1583616
InternalName	tpv2/win32
LanguageCode	Japanese
LegalCopyright	(KIRIKIRI core) (C) W.Deer 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	tpvwin32.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	2021:11:23 18:00:37+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	6.880514545592253
语言	C/C++
操作系统	Windows(XP)[I]386, 32位, GUI]

FindCrypt	
FindCrypt	地址
Look for Base64 table	0x2f2778
Look for CRC32 [poly]	0x3063f0
Look for CRC32 table	0x3061f0
Look for MD5 constants	0x1ccc6
	0x1cccd
	0x1ccd4
	0x1ccdb
	0xe2df3
Look for TEA Encryption	0x442262

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	2021-11-23 18:00:37
入口点(OEP)	0x239653
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	Sabbat of the Witch
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	tv2/win32
原始文件名	tvwin32.exe
注释	Yuzusoft/HIKARIFIELD
语言	0x0411 0x04b0
版权	(KIRIKIRI core) (C) W.Deer 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	tvwin32.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	0x002be000	0x00000400	0x002bde00	R-E	6.664306674136838	781538b5a651eb2688086527ce47f7a3
.adata	0x002bf000	0x00001000	0x002be200	0x00000600	R-E	3.8507259769745703	94e7328775b7111989f1f77ff89f2ca3
.rdata	0x002c0000	0x000af000	0x002be800	0x000aec00	R--	5.543717792181645	a73c6d9fac70af9cb3e074e2a13210e8

PE资源(70)

资源名	资源类型	资源大小	偏移地址	语言	子语言
TEXT	data	0x00000048	0x0041abac	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	ASCII text	0x000000ea	0x0041abf4	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	UTF-8 Unicode text, with very long lines, with CRLF line terminators	0x0000b12f	0x0041ace0	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	UTF-8 Unicode text, with very long lines, with CRLF line terminators	0x0000ea07	0x00425e10	LANG_JAPANESE	SUBLANG_DEFAULT

文件内容

字符串

UnicodeASCII

输入搜索内容

Q

B B@B`B

@Oct 28 2021 16:12:22

0123456789ABCDEF

unimplemented: ttVPCharacterData::Bold for FullColored

tstring

currentDevice

复制

下载

URLs

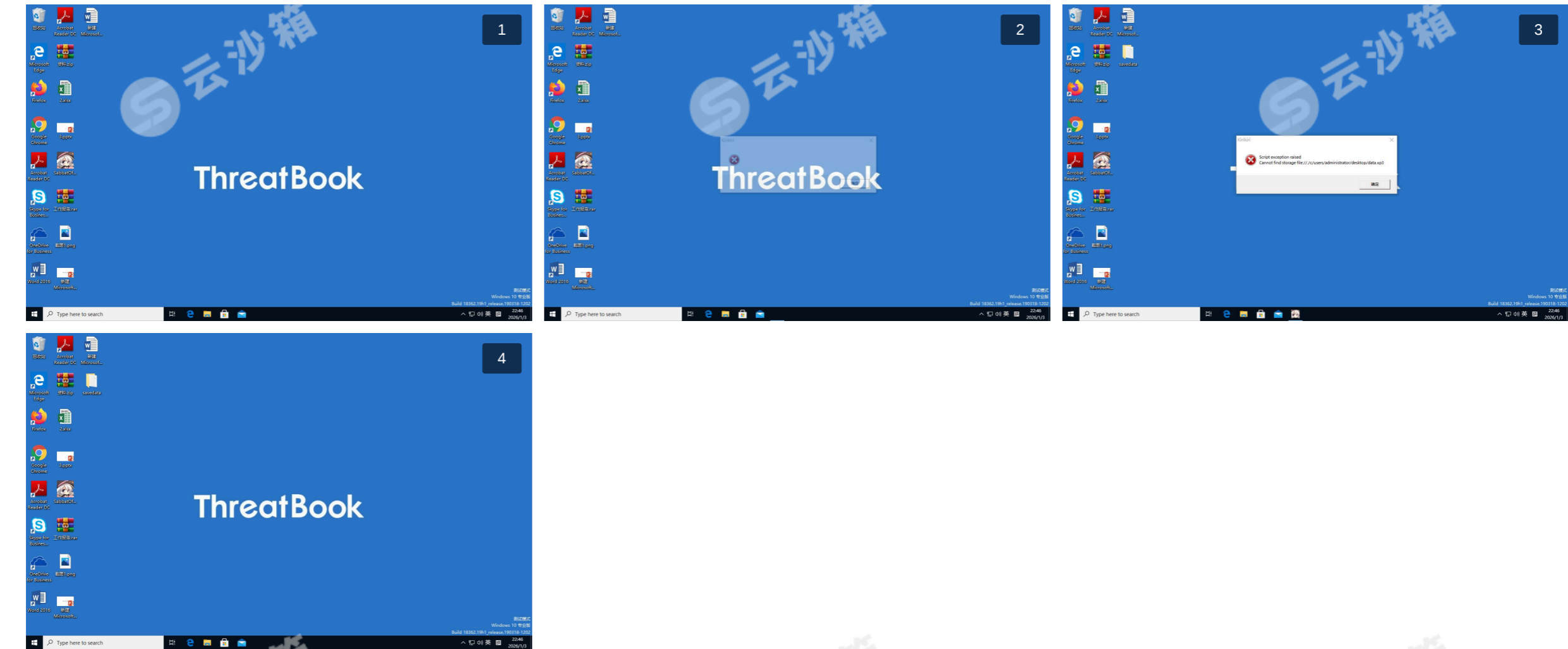
- http://www.apache.org/licenses/
- http://schemas.microsoft.com/SMI/2016/WindowsSettings
- http://www.freetype.org
- http://schemas.microsoft.com/SMI/2005/WindowsSettings
- http://mozilla.org/MPL/2.0/.

沙箱动态检测

Win10(1903 64bit,Office2016)

执行流程





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
e4f4b1858b56.dll(745.5 KB) 文件类型： PE32 executable (DLL) (GUI) Intel 80386, for MS Windows 文件路径： c:\Users\Administrator\AppData\Local\Temp\krkr_55f5bc686b5b_249498078_6884\krkr_1858b56.dll SHA256： f642c927f245d3025e059e79edfe538c68b5cac1826c17c0c2ef398f6ad894b3	(6884) SabbatOfTheWitch.exe	0/28	-	未知
krkr.console.log(14.06 KB) 文件类型： Unicode text, UTF-16, little-endian text, with CRLF, LF line terminators 文件路径： c:\Users\administrator\Desktop\savedata\krkr.console.log SHA256： abab62397f68dd912520cf04dd2e066cc70ffd3fa6a19b6f333fbbfe3078e567	(6884) SabbatOfTheWitch.exe	0/27	-	未知