样本分析报告

文件名称： tenshi_sz.exe

SHA256： a02f03a9ca53f6cbf6a2365ba68b5a889fe0cfcd8bffac1676c9d5c23942a980

文件大小： 4.37 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

tenshi_sz.exe

首次提交: 2026/01/03　末次提交: 2026/01/03　末次分析: 2026/01/03 23:06:30

文件大小： 4.37 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)

未知

HASH

SHA256: a02f03a9ca53f6cbf6a2365ba68b5a889fe0cfcd8bffac1676c9d5c23942a980

MD5: 72077bbf60e50a5a0392a229dc4286f7

SHA1: 4dcfda465cb2c0c1cfafbe1928a50cf557ce6c06

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	a02f03a9ca53f6cbf6a2365ba68b5a889fe0cfcd8b…	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 …

多引擎检测

检出率：**1** / 28　最近检测时间：2026-01-03 23:06:00

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
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

引擎	检出	引擎	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	a02f03a9ca53f6cbf6a2365ba68b5a889fe0cfcd8bffac1676c9d5c23942a980
文件格式	EXEx86
文件类型(Magic)	PE32 executable (GUI) Intel 80386, for MS Windows
文件大小	4.37MB
SHA256	a02f03a9ca53f6cbf6a2365ba68b5a889fe0cfcd8bffac1676c9d5c23942a980
SHA1	4dcfda465cb2c0c1cfafbe1928a50cf557ce6c06
MD5	72077bbf60e50a5a0392a229dc4286f7
CRC32	C1CF0B76
SSDEEP	98304:b68Y7OydqjTTsBs7SBTSJM9HGmq5qW6K27ICLmnz5i7:OnOydqjcxTr9HXqLC
TLSH	T1F226BF11BB91C13AE9F202B19A7DAB9F502CBE241B2440CB72D87E5D1DB16D32B36717
peHashNG	a8016c4095190c3f5979f376ca8ecc9e9679aee14eea9261ca6c2d74fdd0da93
RichHash	3c0d9e7d3593e207906b97e4c7afb820
impfuzzy	96:dXYKYXeX1fnXpJYpSLR1GnGtjFJ+SnfcpfiUVPrCUCzJ/VEl:YuFfnZPRz+S7UVPOUCN0
ImpHash	277b6e27b5785f425f2394d28495d60e
ICON SHA256	88c43ec194a6b9f81d85cfda21c88875b756652373af99fc56e5518ecded4511
ICON DHash	98352d99e5a7f235
Tags	exe,pdb_path,lang_japanese,encrypt_algorithm

元数据

ExifTool

CharacterSet	Unicode
CodeSize	2893312
Comments	YuzuSoft
EntryPoint	0x239653
FileDescription	Angelic☆Chaos RE-BOOT!
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	1689600
InternalName	tvp2/win32
LanguageCode	Japanese
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	2021:11:23 18:00:37+08:00
UninitializedDataSize	0

TrID

83.7% (.CPL)	Windows Control Panel Item (generic) (197083/11/60)
4.4% (.EXE)	Win64 Executable (generic) (10523/12/4)
2.7% (.DLL)	Win32 Dynamic Link Library (generic) (6578/25/2)
2.3% (.FON)	Windows Font (5545/9/1)
2.1% (.EXE)	Win16 NE executable (generic) (5038/12/1)

DIE

链接器	Microsoft Linker(11.00.61030)

编译器	Microsoft Visual C/C++(17.00.61219)[LTCG/C++]
工具	Visual Studio(2012)
字节序	LE
模式	32
程序类型	GUI
文件类型	PE32
熵	-
语言	C/C++
操作系统	Windows(XP)[I386, 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

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	Angelic☆Chaos RE-BOOT!
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	YuzuSoft
语言	0x0411 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	NotSigned

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	0x002bdc1b	0x00000400	0x002bde00	R-E	6.664306674136838	781538b5a651eb2688086527ce47f7a3
.adata	0x002bf000	0x000005f0	0x002be200	0x00000600	R-E	3.8507259769745703	94e7328775b7111989f1f77ff89f2ca3
.rdata	0x002c0000	0x000aeaf0	0x002be800	0x000aec00	R--	5.543745419336201	43d13abacbd3b51666205d5515360a5d
.data	0x0036f000	0x000aa740	0x0036d400	0x0000a600	RW-	5.68285889066352	5df51dc7ac89a689230

PE资源(74)

资源名	资源类型	资源大小	偏移地址	语言	子语言
TEXT	data	0x00000048	0x0041ac6c	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	ASCII text	0x0000017b	0x0041acb4	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	UTF-8 Unicode text, with very long lines, with CRLF line terminators	0x0000b12f	0x0041ae30	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	UTF-8 Unicode text, with very long lines, with CRLF line terminat	0x0000ea07	0x00425f60	LANG_JAPANESE	SUBLANG_DEFAULT

文件内容

字符串

Unicode ASCII

输入搜索内容

```
@Oct 28 2021 16:12:22
0123456789ABCDEF
B B@B`B
-laxtimer
TVPCDDADriveNotFound
cl %%%d
```

复制 下载

URLs

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

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

http://www.freetype.org

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

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

沙箱动态检测

Win10(1903 64bit,Office2016)

执行流程

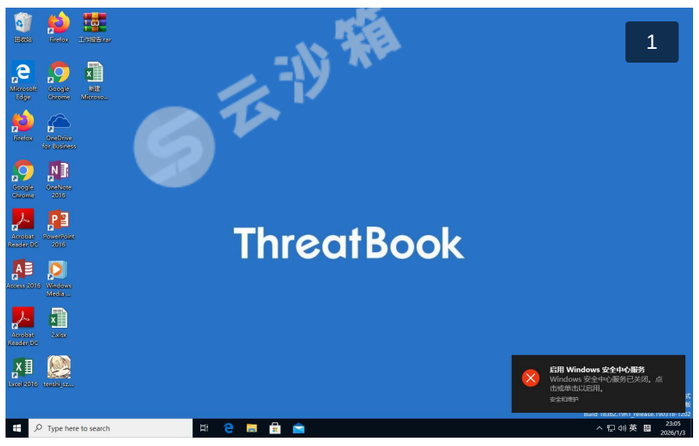
进程详情

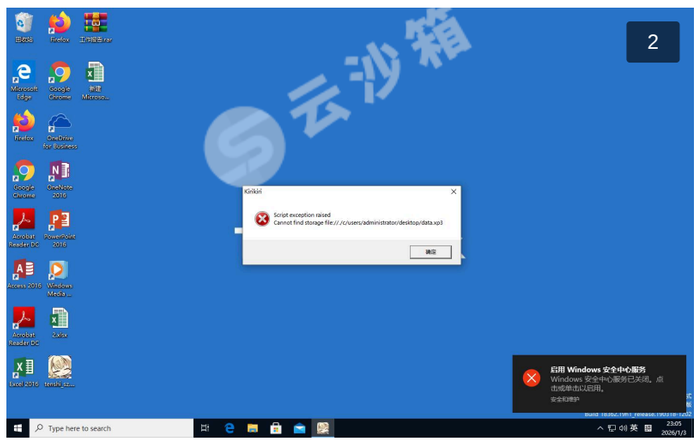
共分析了1个进程

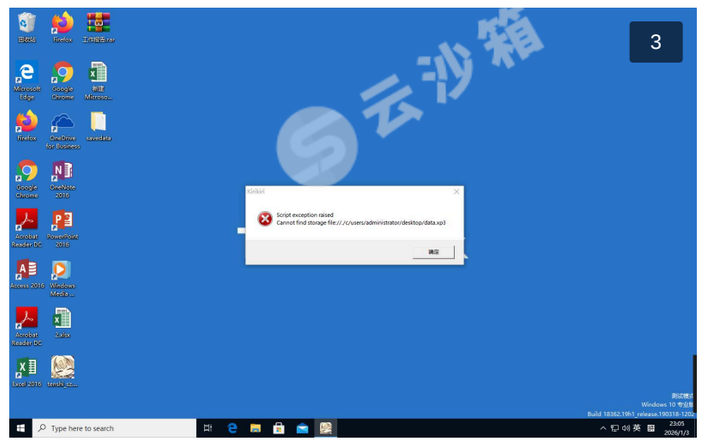
tenshi_sz.exe（PID：7124）

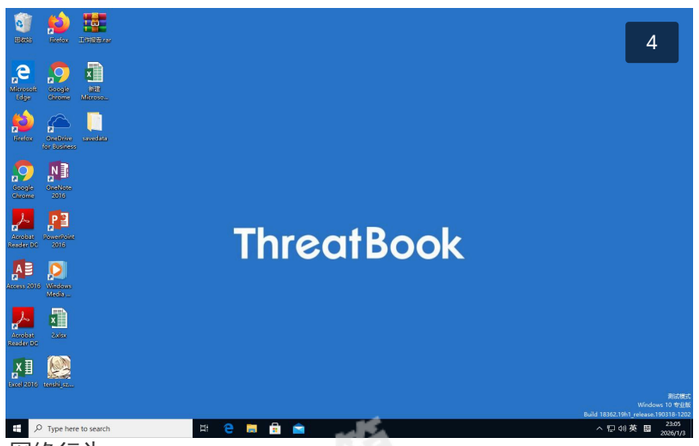
"C:\Users\Administrator\Desktop\tenshi_sz.exe"

运行截图（4）









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
5381e1272a6f.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_f83506759fb0_261447906_7124\5381e1272a6f.dll SHA256： a6d0ec524b3286f99cf46b534d6dfc2f1381e46c54acd23130dda4bed5519b36	（7124）tenshi_sz.exe	0/28	-	未知
krkr.console.log(14.25 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： d3cc792aaf7a953d4c40cfb092787ee6df901a42c80aee5dbee426e5e8b3b494	（7124）tenshi_sz.exe	0/22	-	安全