

# 样本分析报告

文件名称 : 6442C1299B389455F7A18AE79F2077D2

SHA256 : b94886eb62c44d0c8651da037c9142dfd6eca6074e5eb5c212680af7c74fc3a5

文件大小 : 4.22 MB

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

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

# 6442C1299B389455F7A18AE79F2077D2

首次提交: 2025/07/01

末次提交: 2026/01/03

末次分析: 2026/01/03 21:01:25

文件大小: 4.22 MB

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

引擎检出: 1 / 28

分析环境: Win10(1903 64bit,Office2016)

## HASH

SHA256: b94886eb62c44d0c8651da037c9142dfd6eca6074e5eb5c212680af7c74fc3a5

MD5: 6442c1299b389455f7a18ae79f2077d2

SHA1: 7556c9f90f80df4367c9ffb9c0aba27b66e50782

## 行为检测

MITRE ATT&CK™ 矩阵 (技术) 检测到 1 条技术指标。 [查看完整结果](#)

Win10(1903 64bit,Office2016)

### ! 可疑行为 (2)

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

### ! 通用行为 (4)

一般行为

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

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	b94886eb62c44d0c8651da037c9142dfd6eca6074e5eb5c212680af7c74fc3a5	查看	Github	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 20:58:11

引擎	检出	引擎	检出
江民 (JiangMin)	TrojanDownloader.Banload.bsym	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
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	b94886eb62c44d0c8651da037c9142dfd6eca6074e5eb5c212680af7c74fc3a5
文件格式	EXE x86
文件类型(Magic)	PE32 executable (GUI) Intel 80386, for MS Windows
文件大小	4.22MB
SHA256	b94886eb62c44d0c8651da037c9142dfd6eca6074e5eb5c212680af7c74fc3a5
SHA1	7556c9f90f80df4367c9ffb9c0aba27b66e50782
MD5	6442c1299b389455f7a18ae79f2077d2
CRC32	9D70F285
SSDEEP	49152:EtnKg7x+RgOlfbHqGsXQQvHN7kX0wjwS65TE/t5FtuwKQL0dNBExglLztmmyTV7S2:ERgRgOydqjAuAkp5T0tmECILztm8Q
TLSH	T17826BF11BB91C636E9E112B16ABDAF5F202CAE14176440DB73E80C5E6DB07D32B36B17
AuthentiHash	D727B6BE290F658CF67C02BB8A1CAC7200F02233DC36194A6A880BB3113E0F6
peHashNG	a6bc3fc63871bed2ecc97cb1564a1c7e6a428b9fb977754e24d0b86fa095e0a
RichHash	2cb2bc92015a75b453e0b19a7c79afef
impfuzzy	96:Q7KwXXeX1f4X1UYKSLR1G8j3J+SnfcpNAxUVuelUC9J0VEI:luFf4lxlZ+SjxUV1IUCY0
ImpHash	9567e2dba4e003d705d55f3641eaa38e
ICON SHA256	15a289e2c2f6327ef3dcbb2b47b3e254495397a706589b6963a5de04ffa4c3379
ICON DHash	6868e892f068f010
Tags	exe,pdb_path,lang_japanese,encrypt_algorithm

### 元数据

#### ExifTool

FileType	Win32 EXE
FileTypeExtension	exe
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
TimeStamp	2017:11:30 19:41:37+08:00
ImageFileCharacteristics	Executable, 32-bit
PEType	PE32
LinkerVersion	11.0
CodeSize	2874880
InitializedDataSize	1552384
UninitializedDataSize	0
EntryPoint	0x23b053
OSVersion	5.1
ImageVersion	0.0
SubsystemVersion	5.1
Subsystem	Windows GUI
FileVersionNumber	1.2.0.3
ProductVersionNumber	1.2.0.3
FileFlagsMask	0x003f
FileFlags	(none)
FileOS	Windows NT 32-bit
ObjectFileType	Executable application
FileSubtype	0
LanguageCode	Japanese
CharacterSet	Unicode
FileDescription	NEKOPARA After
FileVersion	1.2.0.3
InternalName	tvp2/win32
LegalCopyright	(KIRIKIRI core) (C) W.Deel 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.
OriginalFileName	tvpwin32.exe
ProductName	TVP(KIRIKIRI) Z core / Scripting Platform for Win32
ProductVersion	1.2.0.3

#### TrID

86.1% (.CPL)	Windows Control Panel Item (generic) (197083/11/60)
4.6% (.EXE)	Win64 Executable (generic) (10523/12/4)
2.4% (.FON)	Windows Font (5545/9/1)
2.2% (.EXE)	Win16 NE executable (generic) (5038/12/1)
1.9% (.EXE)	Win32 Executable (generic) (4505/5/1)

#### DIE

链接器	Microsoft Linker(11.00.61030)
编译器	Microsoft Visual C/C++(17.00.61030)[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	6.670145091824261
语言	C/C++
操作系统	Windows(XP)[I386, 32位, GUI]

#### FindCrypt

FindCrypt	地址
Look for CRC32 [poly]	0x352580
Look for CRC32 table	0x352380
Look for MD5 constants	0x1d576

Look for Base64 table	0x1d57d 0x1d584 0x1d58b 0xda443
	0x33e900

Magika ②	
可信度 (Score)	1
识别结果 (Cl_label)	pebin
Magic	PE executable
Mime_type	application/x-dosexec
分类 (Group)	executable
描述信息 (Description)	PE executable

## ④ 格式深度分析

### 文档分析

#### ① 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	2017-11-30 19:41:37
入口点(OEP)	0x23b053
入口所在段	.text
镜像基址	0x400000
节区数量	6
LinkerVersion	11

#### ② PE版本信息

文件说明	NEKOPARA After
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
语言	0x0411 0x04b0
版权	(KIRIKIRI core) (C) W.Deel 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.

#### ③ 调试信息

PDB	tvpwin32.pdb
GUID	-

#### ④ 签名信息

签名验证	Unsigned
------	----------

#### ⑤ 导入表(13)

DLL	DLL描述	函数数量	展开
KERNEL32.dll	-	161	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 ⊗

#### ⑥ PE节区(6)

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	0x002bd70c	0x00000400	0x002bd800	R-E	6.668526671905061	1e6428883876aa901ec d3f2ccdcbec6d
.adata	0x002bf000	0x000005f0	0x002bcd00	0x00000600	R-E	3.860619706000931	829658b5dc4f0fcdf5c97 5d52f9ec439e
.rdata	0x002c0000	0x000ec7f8	0x002be200	0x000ec800	R--	6.402608777377792	95559d1e1e8c948151c 19ba79aa155c8
data	0x003ad000	0x00033200	0x00332000	0x00032000	RW-	5.729720166402802	91b99cb7f4b95243f682

#### ⑦ 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	ASCII text	0x00000049	0x00458b8c	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	UTF-8 Unicode text, with very long lines, with CRLF line terminators	0x0000ad7d	0x00458bd8	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	UTF-8 Unicode text, with very long lines, with CRLF line terminators	0x0000efef	0x00463958	LANG_JAPANESE	SUBLANG_DEFAULT

### 文件内容

#### ⑧ 字符串

Unicode    ASCII

输入搜索内容

```
jjjjjjh
jjjjjj
TVPChangeDisplaySettingsFailedDispChangeFailed
belgian
eventDisabled
TTSSubstitutionInBooleanContext
```

复制    下载

URLs

- http://www.apache.org/licenses/
- http://mozilla.org/MPL/2.0/.
- http://schemas.microsoft.com/SMI/2005/WindowsSettings
- http://www.freetype.org
- http://www.opensource.org/licenses/mit-license.php

## 沙箱动态检测

Win10(1903 64bit,Office2016)

执行流程

+ - ⌂ ⌂ ⌂ ⌂

开始分析

EXE\_x64 4fc3a5.exe

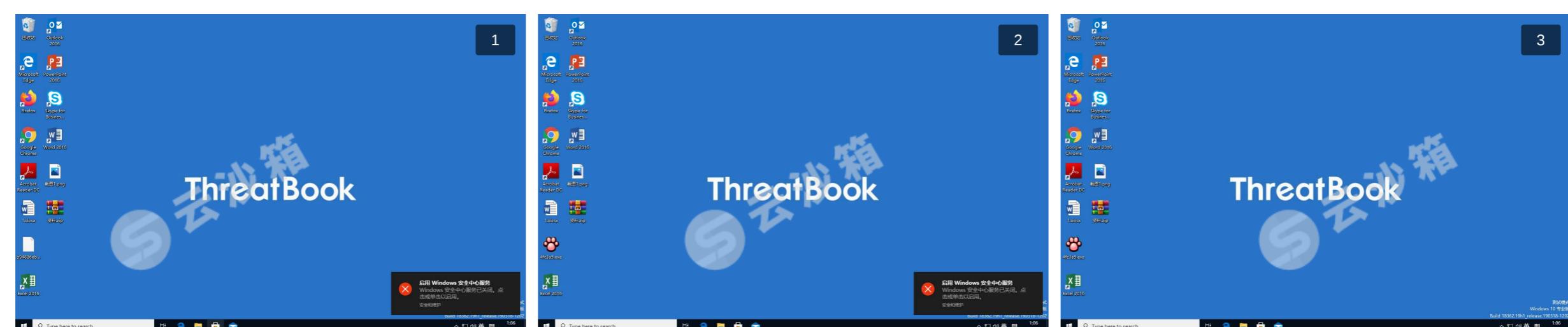
进程文件    创建进程    释放文件    域名/IP    高危行为    启动    连接/释放

## 进程详情

共分析了1个进程

- 4fc3a5.exe (PID : 6996)  
"C:\Users\Administrator\Desktop\4fc3a5.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

① 无释放文件