样本分析报告

文件名称： nekopara_extra.exe

SHA256： c004bd0570cf7ba40a3edb4994892651d3583af6009442f14156655fbc0a5391

文件大小： 4.36 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

nekopara_extra.exe

首次提交: 2026/01/03　末次提交: 2026/01/03　末次分析: 2026/01/03 21:08:14

文件大小： 4.36 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: c004bd0570cf7ba40a3edb4994892651d3583af6009442f14156655fbc0a5391

MD5: 518050cc66cbc2a4c51c4e8537ea522c

SHA1: 3b7086ae33b114ca8133a31c9f2d5eb2d0124494

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)

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 (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

多引擎检测

检出率：1 / 28　最近检测时间：2026-01-03 21:07:19

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	c004bd0570cf7ba40a3edb4994892651d3583af6009442f14156655fbc0a5391
文件格式	EXEx86
文件类型(Magic)	PE32 executable (GUI) Intel 80386, for MS Windows
文件大小	4.36MB
SHA256	c004bd0570cf7ba40a3edb4994892651d3583af6009442f14156655fbc0a5391
SHA1	3b7086ae33b114ca8133a31c9f2d5eb2d0124494

MD5	518050cc66cbc2a4c51c4e8537ea522c
CRC32	574D2487
SSDEEP	49152:ttnKg7x+RgOIfBHqGsXQQvHN7kX0wjwS65TE/t5FtuwKQL0dNBExglLvtmyTV7Sq:tRgRgOydqjAuAkp5T0tmEClLvtm8E
TLSH	T1E226BF11BB91C636E9E112B16ABDAF5F202CAE24176440DB73E80C5E6DB07D32736B17
AuthentiHash	5033760ACFEB1445B2032F6EA6F8788F45CCB40F5A0301A485B8D79B0F7C851E
peHashNG	fab566dbf301c0c0cbf0e495fcc79856f0b63164531d4b1828af61205498775a
impfuzzy	96:Q7KwXXeX1f4X1UYKSLR1G8jl3J+SnfcpNAxUVuelUC9J0VEl:IuFf4lxlZ+SjxUV1lUCY0
ImpHash	9567e2dba4e003d705d55f3641eaa38e
ICON SHA256	15a289e2c2f6327ef3dcb2b47b3e254495397a706589b6963a5de04ffa4c3379
ICON DHash	6868e892f068f010
Tags	exe,pdb_path,lang_japanese,encrypt_algorithm

元数据

ExifTool

CharacterSet	Unicode
CodeSize	2874880
EntryPoint	0x23b053
FileDescription	ネコぱら Extra
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, 32-bit
ImageVersion	0.0
InitializedDataSize	1552384
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	2017:11:30 19:41:37+08:00
UninitializedDataSize	0

TrID

31.2% (.EXE)	Win64 Executable (generic) (10523/12/4)
16.4% (.FON)	Windows Font (5545/9/1)
14.9% (.EXE)	Win16 NE executable (generic) (5038/12/1)
13.3% (.EXE)	Win32 Executable (generic) (4505/5/1)
6.0% (.EXE)	OS/2 Executable (generic) (2029/13)

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	6.729269774953697
语言	C/C++
操作系统	Windows(XP)[I386, 32位, GUI]

FindCrypt

FindCrypt	地址
Look for Base64 table	0x33e900
Look for CRC32 [poly]	0x352580
Look for CRC32 table	0x352380
Look for MD5 constants	0x1d576 0x1d57d 0x1d584 0x1d58b 0xda443
Look for TEA Encryption	0x43a272

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	2017-11-30 19:41:37
入口点(OEP)	0x23b053
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	ネコぱら Extra
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.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	-	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

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	0x002bd800	R-E	6.668526671905061	1e64288883876aa901ecd3f2ccdcbec6d
.adata	0x002bf000	0x00001000	0x002bdc00	0x00000600	R-E	3.860619706000931	829658b5dc4f0fcd5c975d52f9ec439e
.rdata	0x002c0000	0x000ed000	0x002be200	0x000ec800	R--	6.4031303086811295	e93e965eddde6964fc86c448c3a03922
.data	0x003ad000	0x000ab000	0x003aaa00	0x0000a200	RW-	5.729720166402808	91b99cb7f4b95243f682

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	0x000000d6	0x00458b8c	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	UTF-8 Unicode text, with very long lines, with CRLF line terminators	0x0000ad7d	0x00458c64	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	UTF-8 Unicode text, with very long lines, with CRLF line terminators	0x0000eef7	0x004639e4	LANG_JAPANESE	SUBLANG_DEFAULT

文件内容

字符串

Unicode　ASCII

输入搜索内容

```
@Nov 30 2017 20:15:28
0123456789ABCDEF
holland
Clipboard
eventDisabled
TVPStorageInArchiveNotFound
```

复制　下载

URLs

http://www.freetype.org

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

沙箱动态检测

Win10(1903 64bit,Office2016)

执行流程

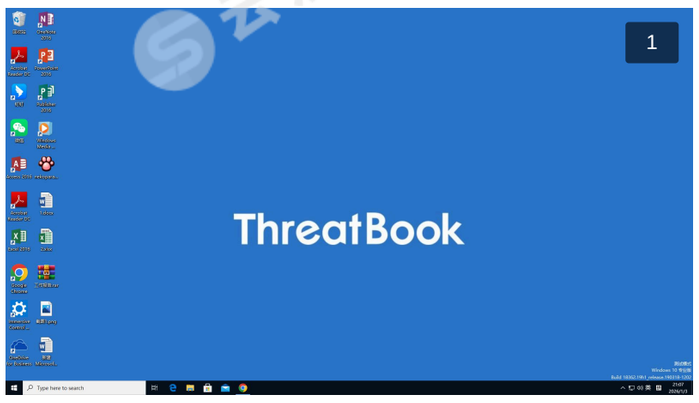
进程详情

共分析了1个进程

nekopara_extra.exe（PID：7008）

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

运行截图（1）



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

无释放文件