样本分析报告

文件名称： CafeStella.exe

SHA256： 1d22021b9cfe68b7eb8d8d2375215662f5815fd41224d134b77839fb0f8fd63d

文件大小： 4.45 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

CafeStella.exe

首次提交: 2026/01/03　末次提交: 2026/01/03　末次分析: 2026/01/03 23:11:11

文件大小： 4.45 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: 1d22021b9cfe68b7eb8d8d2375215662f5815fd41224d134b77839fb0f8fd63d

MD5: ba84d44fe1dc5462448aef7cf3ae43b0

SHA1: fbde94b4d782dd94028df723718ededc9d57662b

未知

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

多引擎检测

检出率：1 / 28　最近检测时间：2026-01-03 23:10:05

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
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	1d22021b9cfe68b7eb8d8d2375215662f5815fd41224d134b77839fb0f8fd63d
文件格式	EXEx86
文件类型(Magic)	PE32 executable (GUI) Intel 80386, for MS Windows
文件大小	4.45MB
SHA256	1d22021b9cfe68b7eb8d8d2375215662f5815fd41224d134b77839fb0f8fd63d
SHA1	fbde94b4d782dd94028df723718ededc9d57662b
MD5	ba84d44fe1dc5462448aef7cf3ae43b0
CRC32	0A5AD49D
SSDEEP	98304:768Y7OydqjTTsBs7SBTSJM9H5mq5qW6K27439Ynv5W4J:unOydqjcxTr9Hwqx39g
TLSH	T10426CF11BB91C13AE9F202B19A7DAB9F502CBE241B2440CB73DC5E5D19B16D32B36B17
AuthentiHash	B5F4A57C45DDCBD97561FEFC4DBEF644762BC97D888AFE9DF865E1A6C3E7C527
peHashNG	9eb5a9977b2cb5e976995b0a6109bb19c559f9afe5f606b09f7bd1e3b6717190
impfuzzy	96:dXYKYXeX1fnXpJYpSLR1GnGtjFJ+SnfcpfiUVPrCUCzJ/VEl:YuFfnZPRz+S7UVPOUCN0
ImpHash	277b6e27b5785f425f2394d28495d60e
ICON SHA256	e8de0dfdce521bb76330f23e80e74861330d93649edba0c0f692ab2908a08ffd
ICON DHash	0d1dec7a7143723d
Tags	exe,pdb_path,lang_japanese,encrypt_algorithm

元数据

ExifTool

CharacterSet	Unicode
CodeSize	2876416
Comments	YuzuSoft
EntryPoint	0x239653
FileDescription	Cafe Stella and the Reapers Butterflies
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	1590784
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

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	6.8966359559853005
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

Look for TEA Encryption	0x443e62

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	Cafe Stella and the Reapers Butterflies
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	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--	5.543810709734313	0e4767d502f186fd4cbb3db97e979f88
.data	0x0036f000	0x000ab000	0x0036d400	0x0000a600	RW-	5.68285889066352	5df51dc7ac89a689230

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	0x000000dd	0x0041abf4	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	UTF-8 Unicode text, with very long lines, with CRLF line terminators	0x0000b12f	0x0041acd4	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	UTF-8 Unicode text, with very long lines, with CRLF line terminat	0x0000ea07	0x00425e04	LANG_JAPANESE	SUBLANG_DEFAULT

文件内容

字符串

Unicode ASCII

输入搜索内容

```
0123456789ABCDEF
B B@B`B
@Oct 28 2021 16:12:22
Index Registers  : ESI:0x%08X  EDI:0x%08X
$(exepath)\savedata
Windows 7
```

复制 下载

URLs

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

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

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

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

http://www.freetype.org

沙箱动态检测

Win10(1903 64bit,Office2016)

执行流程

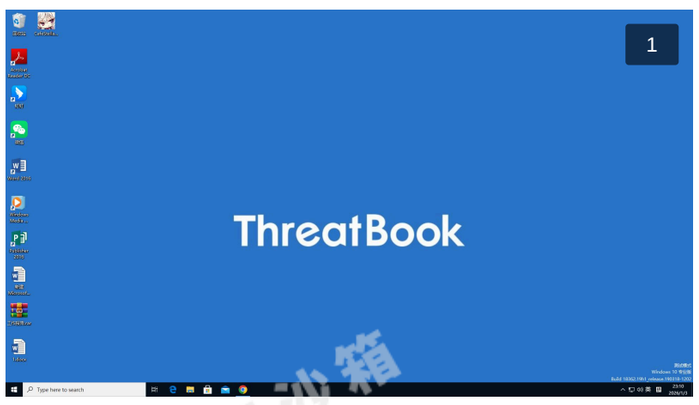
进程详情

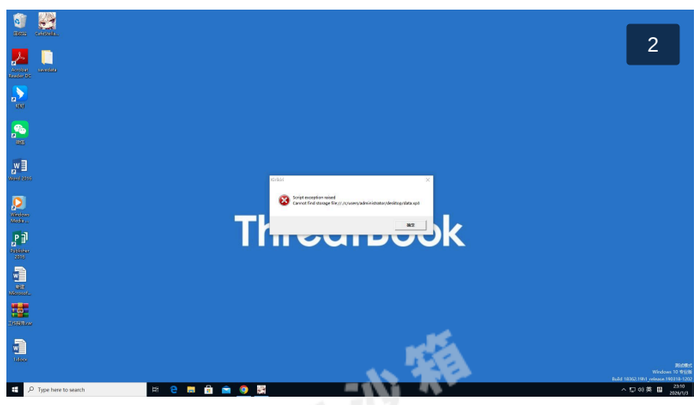
共分析了1个进程

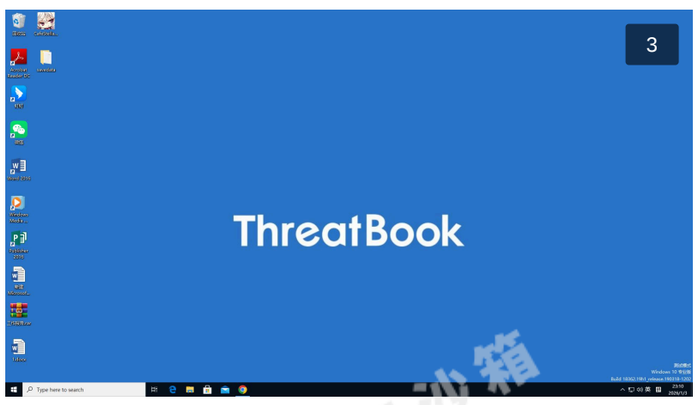
CafeStella.exe（PID：2364）

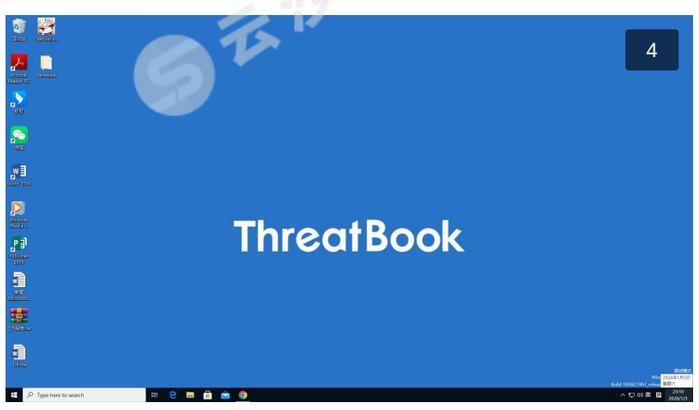
"C:\Users\Administrator\Desktop\CafeStella.exe"

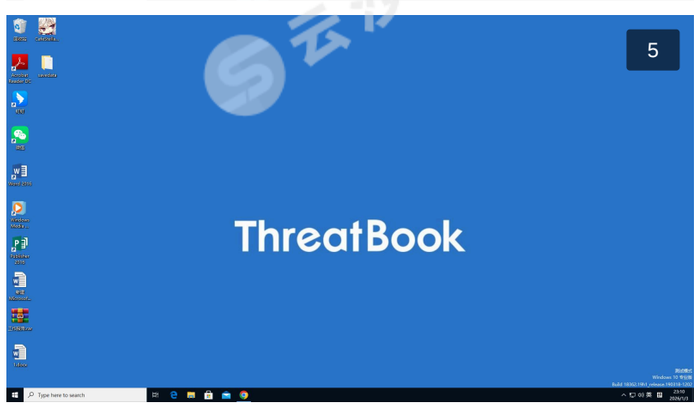
运行截图（5）











网络行为

指纹	TCP	Hosts	域名	DNS	HTTP	HTTPS	UDP	SMTP	ICMP	IRC	Dead-Hosts
2	2	1	0	0	0	0	0	0	0	0	0

指纹：2

协议	地址	指纹类型	指纹哈希	详情
TLS	目的 IP 142.250.73.74:443	JA3	c30794e94ee14ad1fafac083f5031aec	771,0xdada-0x1301-0x1302-0x1303-0xc02b-0xc02f-0xc02c-0xc030-0xcca9-0xcca8-0xc013-0xc014-0x009c-0x009d-0x002f-0x0035,16-18-65281-17513-35-51-5-45-65037-0-11-43-10-27-13-23,4588-29-23-24,0
TLS	目的 IP 142.250.73.74:443	JA3	f5f3103ef2a5e2cf3a1f6ad4d462b6f3	771,0xcaca-0x1301-0x1302-0x1303-0xc02b-0xc02f-0xc02c-0xc030-0xcca9-0xcca8-0xc013-0xc014-0x009c-0x009d-0x002f-0x0035,13-65281-16-27-65037-11-43-45-10-35-18-17513-51-0-23-5,4588-29-23-24,0

TCP：2

源地址	目标地址
100.64.8.63	142.250.73.74
100.64.8.63	142.250.73.74

Hosts：1

IP地址	微步判定	情报内容	地理信息	ASN	使用场景
142.250.73.74	恶意	[redacted]	United States Washington Seattle	15169(GOOGLE)	Cloud Provider

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
1960da20a1eb.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_8e9ebbfd0dcc_268758031_2364\1960da20a1eb.dll SHA256： dbf699ffb518edd2e31f706ff76b0ff47c9fc91f2c4784114f0ab413556e1288	（2364）CafeStella.exe	0/28	-	未知
krkr.console.log(13.93 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： 1069606987b12b48577250bac13b95e19abbb7b367539b11fecce57b21841687	（2364）CafeStella.exe	0/27	-	未知