

样本分析报告


文件名称：PARQUET.exe


SHA256：83c40f84b722be859531795d0afd2722182cbf09f041a60916279b1103153d00

文件大小：4.3 MB

文件类型：PE32 executable (GUI) Intel 80386, for MS Windows, 6 sections

分析环境：

 Win7(32bit,Office2013)

 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

PARQUET.exe

首次提交：2021/08/28 末次提交：2026/01/03 末次分析：2026/01/03 22:58:26

文件大小：4.3 MB 文件类型：PE32 executable (GUI) Intel 80386, for MS Windows, 6 sections
引擎检出：1 / 28 分析环境： Win7(32bit,Office2013) Win10(1903 64bit,Office2016)

HASH
SHA256: 83c40f84b722be859531795d0afd2722182cbf09f041a60916279b1103153d00
MD5: a749b840fcb6aa5802b71c675b96c99f
SHA1: cf3e356e93b95e72b6d75ce74435f932112aef24

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](#) 全部分析环境签名 ▼

! 可疑行为 (4)			
一般行为	感知时区，常用于躲避恶意软件分析系统	2 个分析环境	▼
信息搜集	获取按键信息	2 个分析环境	▼
反检测技术	检测系统内存大小，可能通过内存大小来判断是否运行在虚拟机中	Win7(32bit,Office2013)	▼
反逆向工程	检测自身是否正在被调试	Win7(32bit,Office2013)	▼
! 通用行为 (5)			
一般行为	这个可执行文件存在调试数据库文件（PDB）路径	2 个分析环境	▼
系统环境探测	包含查询计算机时区的功能	2 个分析环境	▼
	获取系统信息	Win7(32bit,Office2013)	▼
静态文件特征	在文件内存中发现IP地址或URL	Win10(1903 64bit,Office2016)	▼
	该可执行文件使用了已经公开的软件保护壳	Win10(1903 64bit,Office2016)	▼

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	83c40f84b722be859531795d0afd2722182cbf09f...	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 22:58:26

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

引擎	检出	引擎	检出
MicroAPT	<div><div></div>无检出</div>	OneAV	<div><div></div>无检出</div>
OneStatic	<div><div></div>无检出</div>	MicroNonPE	<div><div></div>无检出</div>
OneAV-PWSH	<div><div></div>无检出</div>	ShellPub	<div><div></div>无检出</div>

收起全部

静态分析

基础信息

文件名称	83c40f84b722be859531795d0afd2722182cbf09f041a60916279b1103153d00
文件格式	EXEx86
文件类型(Magic)	PE32 executable (GUI) Intel 80386, for MS Windows
文件大小	4.30MB
SHA256	83c40f84b722be859531795d0afd2722182cbf09f041a60916279b1103153d00
SHA1	cf3e356e93b95e72b6d75ce74435f932112aef24
MD5	a749b840fcb6aa5802b71c675b96c99f
CRC32	8E22DBD0
SSDEEP	49152:mtnKg7x+RgOIfBHqGsXQQvHN7kX0wjwS65TE/t5FtuwKQL0dNBExglLKHvtmyTVZ:mRgRgOydqjAuAkp5T0tmECILKHvtm8O
TLSH	T12426AF11BA91C536E9E102B16ABDEB6F202CAE14176440DB72E83C5F7DB47D22732B17
peHashNG	ec1a1a33b46b29560477cffe9d524591f55a933a0f64fca54eee7de7e7f10ff4
impfuzzy	96:Q7KwXxeX1f4X1UYKSLR1G8jl3J+SnfcpNAXUVueIUC9J0VEI:luFf4xlZ+SjxUV1IUCY0
ImpHash	9567e2dba4e003d705d55f3641eaa38e
ICON SHA256	b127d9f26b34e92f9af88d440e298c32f2e1da930bf981ef9710a1b1839a79c1
ICON DHash	4d963b4d450b964d
Tags	exe,modify_clipboard,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
CodeSize	2874880
InitializedDataSize	1630208
UninitializedDataSize	0
EntryPoint	0x23b053
OSVersion	5.1
ImageVersion	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	PARQUET
FileVersion	1.2.0.3
InternalName	tpv2/win32
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.
OriginalFileName	tpvwin32.exe
ProductName	TVP(KIRIKIRI) Z core / Scripting Platform for Win32
ProductVersion	1.2.0.3

TrID	
38.7% (.EXE)	Win64 Executable (generic) (10525/10/4)
20.4% (.FON)	Windows Font (5545/9/1)
18.5% (.EXE)	Win16 NE executable (generic) (5038/12/1)
7.4% (.EXE)	OS/2 Executable (generic) (2029/13)
7.3% (.EXE)	Generic Win/DOS Executable (2002/3)

FindCrypt	
FindCrypt	地址
Looks for big numbers 32:sized	0x355b08
Look for CRC32 [poly]	0x352580
Look for CRC32 table	0x352380
Look for MD5 constants	0x1d576 0xdb08f 0x1d57d 0xdb097 0x1d584 0xdb09f 0x1d58b

	0xdb0a7 0xda443
Look for Base64 table	0x33e900

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	6
LinkerVersion	11

PE版本信息

文件说明	PARQUET
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
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	NotSigned
------	-----------

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(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	0x002be000	0x00000400	0x002bd800	R-E	6.668526671905061	1e6428883876aa901ecd3f2ccdcbec6d
.adata	0x002bf000	0x00001000	0x002bdc00	0x00000600	R-E	3.860619706000931	829658b5dc4f0cd5c975d52f9ec439e
.rdata	0x002c0000	0x000ed000	0x002be200	0x000ec800	R--	6.403418181394305	75b74aab9f5275399a17ae97f25163d7
.data	0x003ad000	0x000ab000	0x003aa000	0x0000a200	RWL	5.729720166402808	91b99cb7f4b95243f682

PE资源(67)

资源名	资源类型	资源大小	偏移地址	语言	子语言
TEXT	ASCII text	0x000000f3	0x00458acc	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	UTF-8 Unicode text, with very long lines, with CRLF line terminators	0x0000ad7d	0x00458bc0	LANG_JAPANESE	SUBLANG_DEFAULT
TEXT	UTF-8 Unicode text, with very long lines, with CRLF line terminators	0x0000eef7	0x00463940	LANG_JAPANESE	SUBLANG_DEFAULT

文件内容

字符串

UnicodeASCII

输入搜索内容

Q

jjjjj

jjjjjh

TVPInvalidOperationFor8BPP

smj-no

FJ;mRh

files found

复制

下载

URLs

http://www.freetype.org

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

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

http://www.opensource.org/licenses/mit-license.php

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

沙箱动态检测

Win7(32bit,Office2013)

执行流程



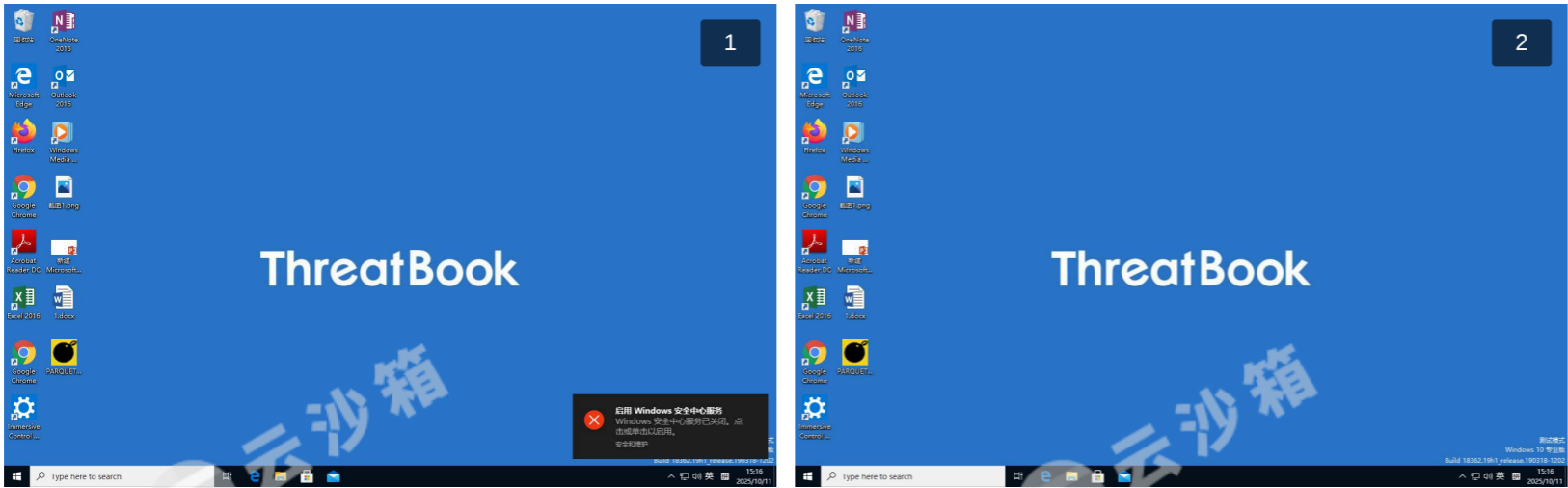


进程详情

共分析了1个进程

- PARQUET.exe (PID : 7120)
"C:\Users\Administrator\Desktop\PARQUET.exe"

运行截图 (2)



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