样本分析报告

文件名称： 潜水艇.exe

SHA256： ab0594e8761a0d259b2ec4415a0c7a6835e4ba83ac44cfffee7ec57e738f3c11

文件大小： 69.92 MB

文件类型： PE32+ executable (GUI) x86-64, for MS Windows

分析环境： Win10(1903 64bit,Office2016)

微步判定： 安全

云沙箱

目录

安全

潜水艇.exe

首次提交: 2025/02/19　末次提交: 2025/02/19　末次分析: 2025/02/19 20:29:32

文件大小： 69.92 MB　文件类型： PE32+ executable (GUI) x86-64, for MS Windows

引擎检出： 0 / 28　分析环境： Win10(1903 64bit,Office2016)

HASH

SHA256: ab0594e8761a0d259b2ec4415a0c7a6835e4ba83ac44cfffee7ec57e738f3c11

MD5: f465e825f9c5535e862cd4ff32dfb882

SHA1: 8f376ec5c1696f48b2bad5e6a063c73421720bb5

行为检测

MITRE ATT&CK™ 矩阵（技术）检测到 **3** 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	Win10(1903 64bit,Office2016)

可疑行为 (3)

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	Win10(1903 64bit,Office2016)
静态文件特征	样本使用了PyInstaller打包器	Win10(1903 64bit,Office2016)
一般行为	感知时区，常用于躲避恶意软件分析系统	Win10(1903 64bit,Office2016)

通用行为 (4)

系统环境探测	查询计算机名	Win10(1903 64bit,Office2016)
	包含查询计算机时区的功能	Win10(1903 64bit,Office2016)
一般行为	在临时目录中创建文件	Win10(1903 64bit,Office2016)
系统敏感操作	在文件系统上创建可执行文件	Win10(1903 64bit,Office2016)

多维检测

Yara 规则　Win10(1903 64bit,Office2016)

初始样本：2

规则	描述	SHA256	匹配项	源	分析环境
PyInstaller	(no description)	ab0594e8761a0d259b2ec4415a0c7a6835e4ba83…	查看	General	Win10(1903 …
MachO_File_pyinstaller	Detect Mach-O file produced by pyinstaller	ab0594e8761a0d259b2ec4415a0c7a6835e4ba83…	查看	Github	Win10(1903 …

释放文件：1

规则	描述	路径	匹配项	源	分析环境
vmdetect	Possibly employs anti-virtualization techniques	C:\Users\Administrator\AppData\Local\Temp_ME…	查看	General	Win10(1903 …

Sigma 规则 (2)　Win10(1903 64bit,Office2016)

标题	描述	标签	危险等级	匹配项	源	分析环境
Autorun Keys Modification	Detects modification of autostart extensibility point (ASEP) in …	persistence; t1547.001; t1060	中	查看	SigmaHQ	Win10(1903 …
New Application in AppCompat	A General detection for a new application in AppCompat. Thi…	execution; t1204.002	info	查看	SigmaHQ	Win10(1903 …

多引擎检测

检出率：**0** / 28　最近检测时间：2025-02-19 20:27:29

引擎	检出	引擎	检出
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

引擎	检出	引擎	检出
安天（Antiy）	无检出	江民（JiangMin）	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	ab0594e8761a0d259b2ec4415a0c7a6835e4ba83ac44cfffee7ec57e738f3c11
文件格式	EXEx64
文件类型(Magic)	PE32+ executable (GUI) x86-64, for MS Windows
文件大小	69.92MB
SHA256	ab0594e8761a0d259b2ec4415a0c7a6835e4ba83ac44cfffee7ec57e738f3c11
SHA1	8f376ec5c1696f48b2bad5e6a063c73421720bb5
MD5	f465e825f9c5535e862cd4ff32dfb882
CRC32	C38ABB7F
SSDEEP	1572864:kh9xTBYSeUqAtN2UDOz5FyWC9rCiaQoSBvzy+Wx3CRrycQ2hPygIhCwarKPqaiVa:gOdtyTrCHTSBO+YCRJBhPQnaWC36
TLSH	T19BF73308ABD43087E8952679C5E7DC25AFD1BCBB4FA2C45A29F54655048B0C0FF392EB
AuthentiHash	1121505BAAEB7091C318B961040EB4A91215E424900F77B91C214B74B3E64B9D
peHashNG	de7b513449a1c168d50f6a041f90b2be162fa1a1922b99200e94adb0a2f2fb0e
RichHash	66a3d2fc5ff0010149c3be0b1b99c500
impfuzzy	48:tVYEK/0W/KA4JGn6gF/gub6EwoQ54rzSv6xviAYd9pUJOyIx0LwitN1MEc+pIuCP:D/sTfh18gJtIx0LZtN1MEc+pIuYQ9HS
ICON SHA256	93abf7a390b6ba741dfa909fe00cd55da218d7d6c0d60fbc4c98caf0d7d041fe
ICON DHash	46b3b0a6a4e8f088
Tags	exe,lang_neutral,encrypt_algorithm

元数据

ExifTool

FileType	Win64 EXE
FileTypeExtension	exe
MIMEType	application/octet-stream
MachineType	AMD AMD64
TimeStamp	2025:02:19 15:07:59+08:00
ImageFileCharacteristics	Executable, Large address aware
PEType	PE32+
LinkerVersion	14.41
CodeSize	172032
InitializedDataSize	193536
UninitializedDataSize	0
EntryPoint	0xce20
OSVersion	6.0
ImageVersion	0.0
SubsystemVersion	6.0
Subsystem	Windows GUI
FileVersionNumber	0.2.3.4
ProductVersionNumber	0.2.3.4
FileFlagsMask	0x003f
FileFlags	(none)
FileOS	Windows NT 32-bit
ObjectFileType	Executable application
FileSubtype	0
LanguageCode	Chinese (Simplified)
CharacterSet	Unicode
CompanyName	狗头包匪
FileDescription	深海潜水艇
FileVersion	0.2.3.4
InternalName	submarine
LegalCopyright	Copyright (C) 2025 狗头包匪
OriginalFileName	潜水艇.exe
ProductName	深海潜水艇
ProductVersion	0.2.3.4

TrID

44.4% (.EXE)	Win64 Executable (generic) (10523/12/4)
21.3% (.EXE)	Win16 NE executable (generic) (5038/12/1)
8.7% (.ICL)	Windows Icons Library (generic) (2059/9)
8.5% (.EXE)	OS/2 Executable (generic) (2029/13)
8.4% (.EXE)	Generic Win/DOS Executable (2002/3)

DIE

链接器	Microsoft Linker(14.36.34123)
编译器	Microsoft Visual C/C++(19.36.34123)[C]
工具	Visual Studio(2022 version 17.6)
字节序	LE
模式	64
程序类型	GUI
文件类型	PE64
熵	7.997264597205232
语言	C/C++
操作系统	Windows(Vista)[AMD64, 64位, GUI]

FindCrypt

FindCrypt	地址
Look for CRC32 [poly]	0x2d1b0
Look for CRC32 table	0x2cfb0

Magika

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

格式深度分析

文档分析

PE头信息

平台	AMD64 (K8)
子系统	Windows graphical user interface (GUI) subsystem
编译时间戳	2025-02-19 15:07:59
入口点(OEP)	0xce20
入口所在段	.text
镜像基地址	0x140000000
节区数量	6
LinkerVersion	14

PE版本信息

文件说明	深海潜水艇
文件版本	0.2.3.4
产品名称	深海潜水艇
产品版本	0.2.3.4
内部名称	submarine
原始文件名	潜水艇.exe
语言	0x0804 0x04b0
版权	Copyright (C) 2025 狗头包匪

签名信息

签名验证	Unsigned

导入表(5)

DLL	DLL描述	函数数量	
USER32.dll	-	28	展开
COMCTL32.dll	-	1	展开
KERNEL32.dll	-	107	展开
ADVAPI32.dll	-	4	展开
GDI32.dll	-	3	展开

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	0x00029f70	0x00000400	0x0002a000	R-E	6.489205819736506	b8c3814c5fb0b18492ad4ec2ffe0830a
.rdata	0x0002b000	0x00012a28	0x0002a400	0x00012c00	R--	5.75078293605444	0339edd69efae6ba968d5c051a6bec48
.data	0x0003e000	0x000053f8	0x0003d000	0x00000e00	RW-	1.8392217063172436	dba0caeecab624a0ccc0d577241601d1
.pdata	0x00044000	0x00002238	0x0003de00	0x00002400	R--	5.2645170849678795	9cd1eac931545f28ab0

PE资源(10)

资源名	资源类型	资源大小	偏移地址	语言	子语言
RT_ICON	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced	0x000002be	0x00047250	LANG_NEUTRAL	SUBLANG_NEUTRAL

RT_ICON	PNG image data, 24 x 24, 8-bit/color RGBA, non-interlaced	0x000005b9	0x00047510	LANG_NEUTRAL	SUBLANG_NEUTRAL
RT_ICON	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced	0x00000926	0x00047acc	LANG_NEUTRAL	SUBLANG_NEUTRAL
RT_ICON	PNG image data, 48 x 48, 8-bit/				

文件内容

字符串

Unicode ASCII

```
#+3;CScs
smn-FI
sma-SE
az-az-latn
Monday
quz-PE
```

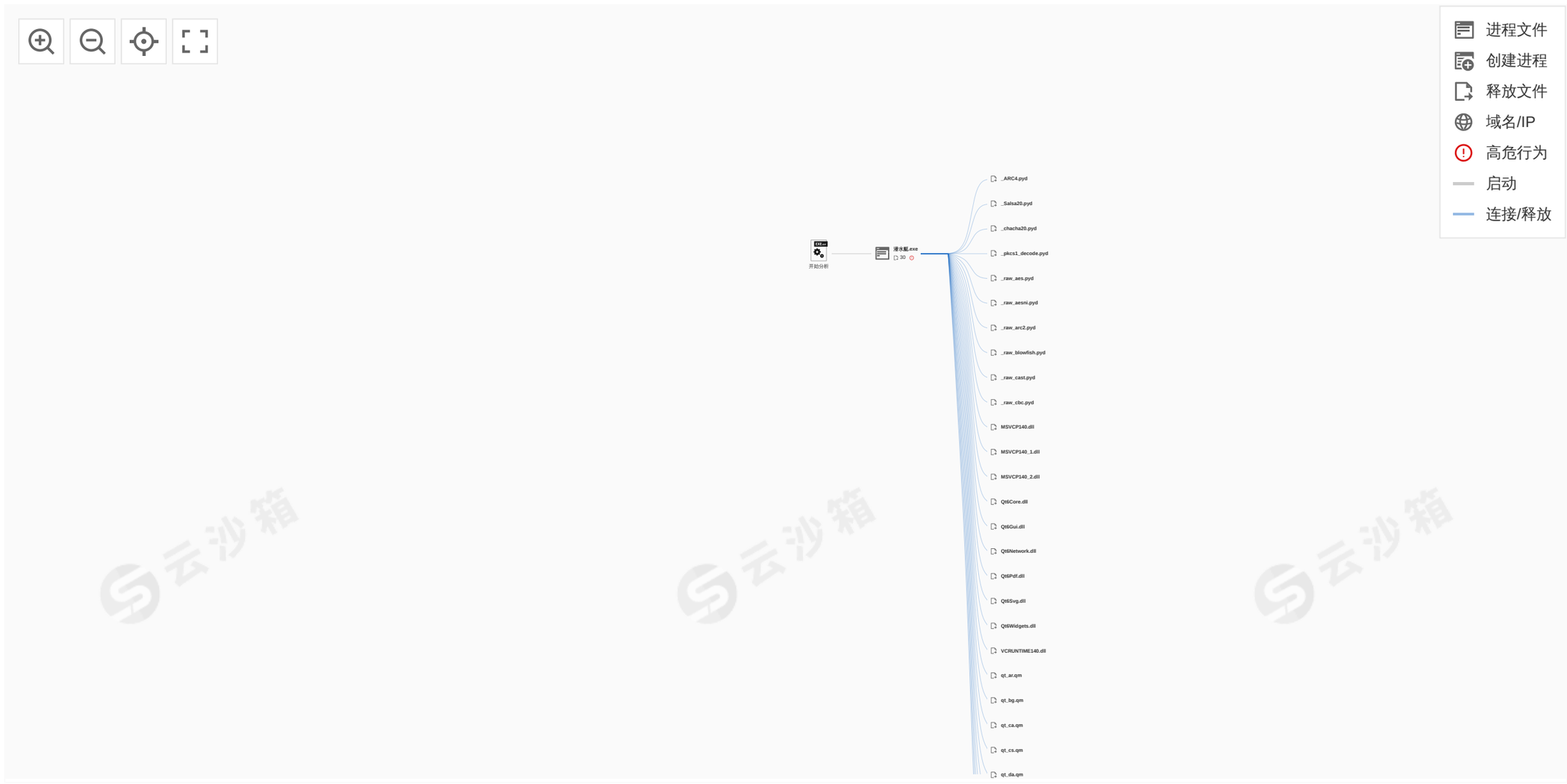
URLs

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

潜水艇.exe（PID：6864）

"C:\Users\Administrator\Desktop\潜水艇.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（30）

释放样本	进程	多引擎检出	威胁类型/木马家族	微步判定
_ARC4.pyd(11 KB) 文件类型： PE32+ executable (DLL) (GUI) x86-64, for MS Windows 文件路径： C:\Users\Administrator\AppData\Local\Temp_MEI68642\Crypto\Cipher_ARC4.pyd SHA256： 78725d2f55b7400a3fcafecd35af7aeb253fbc0ffcdf1903016eb0aabd1b4e50	（6864）潜水艇.exe	0/28	-	安全
_Salsa20.pyd(13.5 KB) 文件类型： PE32+ executable (DLL) (GUI) x86-64, for MS Windows 文件路径： C:\Users\Administrator\AppData\Local\Temp_MEI68642\Crypto\Cipher_Salsa20.pyd SHA256： 1ece1dc94471d6977dbe2ceeba3764adf0625e2203d6257f7c781c619d2a3dad	（6864）潜水艇.exe	0/28	-	安全
_chacha20.pyd(13 KB) 文件类型： PE32+ executable (DLL) (GUI) x86-64, for MS Windows 文件路径： C:\Users\Administrator\AppData\Local\Temp_MEI68642\Crypto\Cipher_chacha20.pyd SHA256： 68f081e96ae08617cf111b21eded35c1774a5ef1223df9a161c9445a78f25c73	（6864）潜水艇.exe	0/28	-	安全
_pkcs1_decode.pyd(14 KB) 文件类型： PE32+ executable (DLL) (GUI) x86-64, for MS Windows 文件路径： C:\Users\Administrator\AppData\Local\Temp_MEI68642\Crypto\Cipher_pkcs1_decode.pyd SHA256： 8a1b751db47ce7b1d3bd10bebffc7442be4cfb398e96e3b1ff7fb83c88a8953d	（6864）潜水艇.exe	0/28	-	安全
_raw_aes.pyd(35.5 KB) 文件类型： PE32+ executable (DLL) (GUI) x86-64, for MS Windows 文件路径： C:\Users\Administrator\AppData\Local\Temp_MEI68642\Crypto\Cipher_raw_aes.pyd SHA256： 6ce8a60d1ab5adc186e23e3de864d7adf6bdd37e3b0c591fa910763c5c26af60	（6864）潜水艇.exe	0/28	-	安全