微步云沙箱

一站式文件分析平台，场景化专业云沙箱

S-221216-8ebea9

样本分析报告

文件名称：Windows全版本激活工具 底包9.0版本.exe

SHA256： 8ebea9839058bf1c11282b4c43d1ab0f11ce4f3c8185b4c4524d32f48356e0b3

文件大小：10.32 MB

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

分析环境：Win10(1903 64bit,Office2016) Win7(32bit,Office2013)

微步判定：安全

目录

Windows全版本激活工具 底包9.0版本.exe

安全

首次提交: 2022/08/31　末次提交: 2022/11/24　末次分析: 2022/11/24 11:45:21

文件大小： 10.32 MB　文件类型： PE32 executable (console) Intel 80386, for MS Windows

引擎检出： 1 / 22　分析环境： Win7(32bit,Office2013) Win10(1903 64bit,Office2016)

HASH

SHA256: 8ebea9839058bf1c11282b4c43d1ab0f11ce4f3c8185b4c4524d32f48356e0b3

MD5: 77ff884221273994cc7c8016b36fe1de

SHA1: 5285bcb3731c2db3bffa1f7265df852ecbaa4759

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

全部分析环境签名

高危行为（4）

网络相关	连接IRC服务，可能是僵尸网络（botnet）	Win7(32bit,Office2013)
一般行为	创建并运行批处理文件以删除原始二进制文件	2 个分析环境
系统敏感操作	创建一个或多个可疑进程	Win7(32bit,Office2013)
	在用户目录下创建可执行文件	2 个分析环境

可疑行为（8）

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	2 个分析环境
网络相关	进程wget.exe下载了一个可执行文件到本地	Win7(32bit,Office2013)
	连接到无应答的IP地址	Win7(32bit,Office2013)
一般行为	感知时区，常用于躲避恶意软件分析系统	Win7(32bit,Office2013)
	将文件属性设置为删除	2 个分析环境
	释放了一个二进制文件并执行	Win7(32bit,Office2013)
系统敏感操作	访问系统的证书存储区域	Win7(32bit,Office2013)
	使用windows实用程序代替windows的基础功能	Win7(32bit,Office2013)

通用行为（8）

静态文件特征	PE文件的节大小异常	2 个分析环境
系统环境探测	包含查询计算机时区的功能	Win7(32bit,Office2013)

网络相关	发起了HTTP请求	2 个分析环境
一般行为	在临时目录中创建文件	2 个分析环境
	命令行控制台有数据输出	2 个分析环境
	读写ini文件	Win7(32bit,Office2013)
系统敏感操作	在文件系统上创建脚本文件	2 个分析环境
	在文件系统上创建可执行文件	2 个分析环境

多引擎检测

检出率：1 / 22

最近检测时间：2022-09-01 10:20:01

引擎	检出	引擎	检出
GDATA	Gen:Variant.Strictor.200365	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	K7	无检出
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

收起全部

静态分析

基础信息

文件名称	8ebea9839058bf1c11282b4c43d1ab0f11ce4f3c8185b4c4524d32f48356e0b3
文件格式	EXEx86
文件类型(Magic)	PE32 executable (console) Intel 80386, for MS Windows
文件大小	10.32MB
SHA256	8ebea9839058bf1c11282b4c43d1ab0f11ce4f3c8185b4c4524d32f48356e0b3
SHA1	5285bcb3731c2db3bffa1f7265df852ecbaa4759
MD5	77ff884221273994cc7c8016b36fe1de
CRC32	884B30B0
SSDEEP	196608:Y/nuE+3TaTw4iigxohK0cSopezHbDhZk/nOzsA+y0zrN5mdG1j:Y/utTaTwYgxoUoopUhZk/nOwpzR5mi

TLSH	T1D6B6335071D08AE5E2A0863850D5B0F89FDC6F2AA3315E83D75E3D11C5AF7AE83B914B
AuthentiHash	CB3122F12D71B8BE2AA467B94B16EF64AE05CFD0D958EB9781956A87A3F86E69
peHashNG	867fced926f8b82a46e84b3ee118f421a25bee37f0a0c6d9d9da3af9e344f3e0
impfuzzy	48:YMuGno3GrCpb1HqJOI40EdXIqSZ/g/KA/kEUEk1WSY+09AEFXolvyAobFzGJ6tnm:Y7qo3qCpb1KJh400XIZW4wvIow
ImpHash	2c5f2513605e48f2d8ea5440a870cb9e
ICON SHA256	4301dea771581abc8bb6b52bec2c59a72b39f5f4cac7be7ea83bb27438fc5ad3
ICON DHash	fb1b5a5a5a5a5bfb
Tags	exe,lang_neutral,encrypt_algorithm

元数据

ExifTool

FileType	Win32 EXE
FileTypeExtension	exe
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
TimeStamp	2018:02:02 04:18:05+08:00
ImageFileCharacteristics	No relocs, Executable, No line numbers, No symbols, 32-bit
PEType	PE32
LinkerVersion	2.5
CodeSize	70144
InitializedDataSize	10750464
UninitializedDataSize	0
EntryPoint	0x1000
OSVersion	4
ImageVersion	0
SubsystemVersion	4
Subsystem	Windows command line
FileVersionNumber	0.0.0.0
ProductVersionNumber	0.0.0.0
FileFlagsMask	0x003f
FileFlags	Debug, Pre-release, Private build
FileOS	Windows 16-bit
ObjectFileType	Executable application
FileSubtype	0
LanguageCode	English (U.S.)
CharacterSet	Windows, Latin1

TrID

37.8% (.EXE)	Win32 Executable MS Visual C++ (generic) (31206/45/13)
20.0% (.EXE)	Microsoft Visual C++ compiled executable (generic) (16529/12/5)
12.7% (.EXE)	Win64 Executable (generic) (10523/12/4)
7.9% (.DLL)	Win32 Dynamic Link Library (generic) (6578/25/2)
6.1% (.EXE)	Win16 NE executable (generic) (5038/12/1)

DIE

Compiler	PureBasic(4.X)[-]
Linker	Polink(2.50*)[Console32,console,admin]
字节序	LE
模式	32
程序类型	Console
文件类型	PE32
熵	7.999547230607807

FindCrypt

FindCrypt	地址
Looks for big numbers 32:sized	0x1607a 0x162be 0x163a4
Look for CRC32 [poly]	0xfac9 0x129d0
Look for CRC32 table	0x127d0
Look for MD5 constants	0xa743 0xbc9e 0xa74a 0xbca5 0xa751 0xbcac 0xa758 0xbcb3 0xbd29
Look for RIPEMD-160 constants	0xa743 0xbc9e 0xa74a 0xbca5 0xa751 0xbcac 0xa758 0xbcb3 0xa75f
Look for SHA1 constants	0xa743 0xbc9e 0xa74a 0xbca5 0xa751 0xbcac 0xa758 0xbcb3 0xa75f 0xb619 0xb654 0xb68a 0xb6b5 0xb6ec 0xb6fd 0xb76a 0xb7a2 0xb7ed 0xb817 0xb843 0xb84f 0xb8b2 0xb8e9 0xb926 0xb95d 0xb99b 0xb9ca 0xb9fa 0xba02

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 character-mode user interface (CUI) subsystem
编译时间戳	2018-02-02 04:18:05
入口点(OEP)	0x1000
入口所在段	.code
镜像基地址	0x400000
节区数量	5
LinkerVersion	2

PE版本信息

语言	0x0000 0x04e4

签名信息

签名验证	NotSigned

导入表(9)

DLL	DLL描述	函数数量	
MSVCRT.dll	-	16	展开
KERNEL32.dll	-	72	展开
USER32.DLL	-	33	展开
GDI32.DLL	-	1	展开
COMCTL32.DLL	-	1	展开

查看全部

PE节区(5)

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
.code	0x00001000	0x0000387e	0x00000400	0x00003a00	R-E	5.527969468191716	da73045b586ab1e28e607f483a0c2ce0
.text	0x00005000	0x0000d642	0x00003e00	0x0000d800	R-E	6.546149830415049	45a4903077d6f7155f4006b168c87dca
.rdata	0x00013000	0x000033a8	0x00011600	0x00003400	R--	7.110334372906 4665	fc9dcbeb475affc5d4c8d32f8314c9b3

PE资源(21)

资源名	资源类型	资源大小	偏移地址	语言	子语言
RT_ICON	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294901502, next used block 4294901758	0x000010a8	0x00019980	LANG_NEUTRAL	SUBLANG_NEUTRAL
RT_RCDATA	zlib compressed data	0x00000012	0x0001aa28	LANG_NEUTRAL	SUBLANG_NEUTRAL
RT_RCDATA	very short file (no magic)	0x00000001	0x0001aa3c	LANG_NEUTRAL	SUBLANG_NEUTRAL

文件内容

字符串

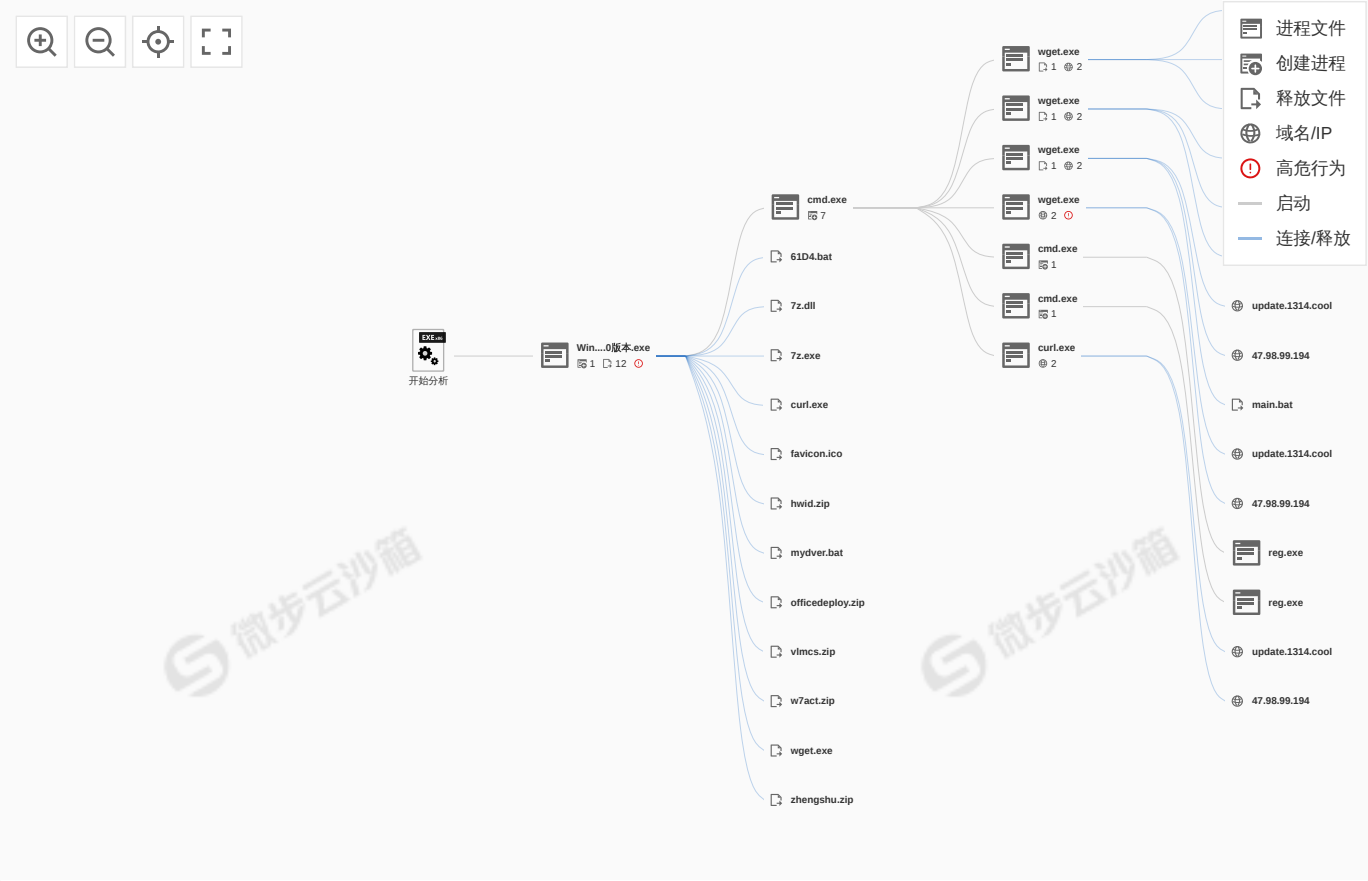
Unicode ASCII

```
Inexact floating-point result
Array bounds exceeded
Privileged instruction
Shell32.DLL
Kernel32.dll
```

沙箱动态检测

Win7(32bit,Office2013)

执行流程



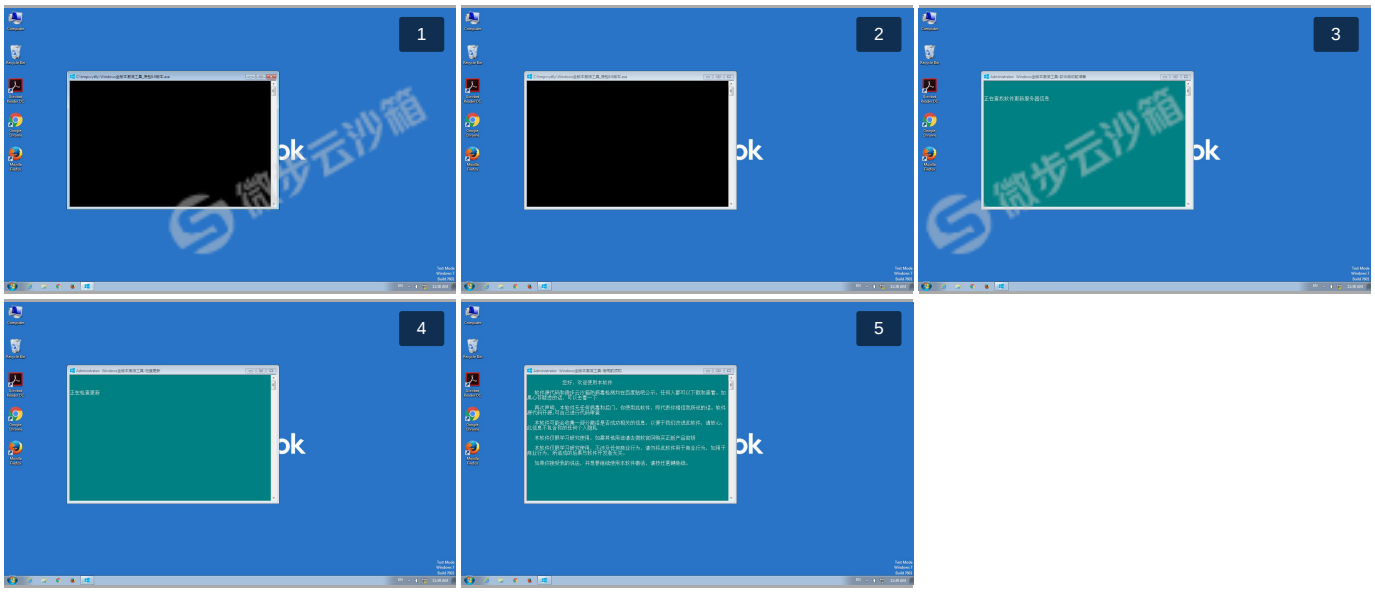
进程详情

共分析了11个进程

- Windows全版本激活工具_底包9.0版本.exe（PID：2144）
  "C:\tmpcvyt0y\Windows全版本激活工具_底包9.0版本.exe"
  - cmd.exe（PID：2236）
    "C:\Windows\system32\cmd" /c "C:\Users\Admin\AppData\Local\Temp\61D2.tmp\61D3.tmp\61D4.bat C:\tmpcvyt0y\Windows全版本激活工具_底包9.0版本.exe"
    - wget.exe（PID：2340）
      wget -q http://chenchuanrui.gitee.io/services/actsev.bat
    - wget.exe（PID：2080）
      wget -q http://update.1314.cool/update/act/ver.bat
    - wget.exe（PID：2532）
      wget -q http://update.1314.cool/update/act/main.bat
    - wget.exe（PID：3052）
      wget -q "http://update.1314.cool/update/act/curl.exe"
    - cmd.exe（PID：3140）
      C:\Windows\system32\cmd.exe /c REG QUERY "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion" /v ProductName
      - reg.exe（PID：3260）
        REG QUERY "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion" /v ProductName
    - cmd.exe（PID：3180）
      C:\Windows\system32\cmd.exe /c REG QUERY "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion" /v CurrentBuildNumber
      - reg.exe（PID：3292）
        REG QUERY "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion" /v CurrentBuildNumber
    - curl.exe（PID：2956）

curl.exe "http://update.1314.cool/update/act/counter/counter.php?system=Windows 7 Ultimate&status=start"

运行截图（5）



网络行为

指纹	域名	DNS	HTTP	HTTPS	TCP	IRC	Hosts	UDP	SMTP	ICMP	Dead-Hosts
12	2	2	4	1	3	2	2	0	0	0	0

指纹：12

协议	地址	指纹类型	指纹哈希	详情
HTTP	目的 IP 212.64.63.215:80	clientHeaderHash	d3a85c232b0a1ba9736e0fa9bd64cf35	host,user_agent,accept,accept_encoding,connection
HTTP	目的 IP 212.64.63.215:80	hfingerHash	b0f17740a7aeee91eed573cdeef038aa	1.3|2|1.0|bat|||GE|1|ho,us-ag,ac,ac-en,co|us-ag:af68cc82/ac:as-as/ac-en:id/co:Ke-Al|||
HTTP	源 IP 212.64.63.215:80	serverHeaderHash	186c7cdba181dd3071940b35bf7cea66	date,content_type,content_length,connection,server,location,cache_control
TLS	目的 IP 212.64.63.215:443	JA3	b9c865e0f840d0946a3b80a0e142610c	771,4866-4867-4865-49196-49200-163-159-52393-52392-52394-49327-49325-49315-49311-49245-49249-49239-49235-49195-49199-162-158-49326-49324-49314-49310-49244-49248-49238-49234-49188-49192-107-106-49267-49271-196-195-49187-49191-103-64-49266-49270-190-189-49162-49172-57-56-136-135-49161-49171-51-50-69-68-157-49313-49309-49233-156-49312-49308-49232-61-192-60-186-53-132-47-65-255,0-11-10-35-22-23-49-13-43-45-51,29-23-30-25-24,0-1-2
TLS	源 IP 212.64.63.215:443	JA3S	a9e3ed16ee3208291487c8d2aa2ad924	771,49200,0-65281-11

1 / 3 每页显示 5条

域名：2

域名	微步判定	情报内容	当前解析IP
update.1314.cool	未知	-	47.98.99.194

域名	微步判定	情报内容	当前解析IP
chenchuanrui.gitee.io	安全	白名单	212.64.63.215

DNS：2

域名	请求	应答
chenchuanrui.gitee.io	A	CNAME → aoufnebg.dayugslb.com A → 212.64.63.215 212.64.63.190
update.1314.cool	A	A → 47.98.99.194

HTTP：4

Timeshift	进程	响应头	URL	目标地址	内容
45ms	-	GET | 301	http://chenchuanrui.gitee.io:80/services...actsev.bat	212.64.63.215:80	0 B ↑ empty 182 B ↓ HTML doc...
46ms	-	GET | 200	http://update.1314.cool:80/update/act/ver.bat	47.98.99.194:80	0 B ↑ empty 37 B ↓ ASCII te...
47ms	-	GET | 200	http://update.1314.cool:80/update/act/main.bat	47.98.99.194:80	0 B ↑ empty 69.94 KB ↓ DOS batc...
48ms	-	GET | 200	http://update.1314.cool:80/update/act/curl.exe	47.98.99.194:80	0 B ↑ empty 272.5 KB ↓ PE32 exe...

HTTPS：1

Timeshift	进程	响应头	URL	目标地址	内容
45ms	-	GET | 200	https://chenchuanrui.gitee.io:443/servic...actsev.bat	212.64.63.215:443	0 B ↑ empty 62 B ↓ ASCII te...

TCP：3

源地址	目标地址
192.168.7.176	212.64.63.215
192.168.7.176	212.64.63.215
192.168.7.176	47.98.99.194

IRC：2

Timeshift	进程ID	目标地址	IRC类型	IRC命令	IRC参数
1669261184ms	-	47.98.99.194:80	server	add	"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Polic…
1669261184ms	-	47.98.99.194:80	server	add	"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Polic…

Hosts：2

IP地址	微步判定	情报内容	地理信息	ASN	使用场景
47.98.99.194	未知	阿里云主机 IDC服务器	China Zhejiang Hangzhou City	37963(CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd., CN)	Hosting
212.64.63.215	安全	白名单 腾讯云主机 IDC服务器	China Shanghai Shanghai City	45090(CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN)	Hosting

释放文件（15）

释放样本	进程	多引擎检出	威胁类型/木马家族	微步判定	操作
c6421758962dd335_61d4.bat(1.03 KB) 文件类型： ISO-8859 text, with CRLF line terminators 文件路径： C:\Users\Admin\AppData\Local\Temp\61D2.tmp\61D3.tmp\61D4.bat SHA256： c6421758962dd335fdee19ba21ecd64e7b4e2da66c193cd85e8863e67aa3df8d	（2144）Windows全版本激…	0/24	-	安全	
ca8ab5aeef734f24_7z.dll(1.18 MB) 文件类型： PE32 executable (DLL) (GUI) Intel 80386, for MS Windows 文件路径： C:\Users\Admin\AppData\Local\Temp\61D2.tmp\7z.dll SHA256： ca8ab5aeef734f24a3c58bf10b3f0152c2ea1329b02d2730448693df563b4c6a	（2144）Windows全版本激…	0/22	-	安全	
59cbfba941d3ac02_7z.exe(329.5 KB) 文件类型： PE32 executable (console) Intel 80386, for MS Windows 文件路径： C:\Users\Admin\AppData\Local\Temp\61D2.tmp\7z.exe SHA256： 59cbfba941d3ac0238219daa11c93969489b40f1e8b38fabdb5805ac3dd72bfa	（2144）Windows全版本激…	0/22	-	安全	
26792fcaca5109ed_actsev.bat(62 B) 文件类型： ASCII text, with CRLF line terminators 文件路径： C:\Users\Admin\AppData\Local\Temp\61D2.tmp\actsev.bat SHA256： 26792fcaca5109ed6e315b65c1924eea730f7b24e20c714aef1dff7ade1808b3	（2340）wget.exe	0/25	-	安全	
44f1669e08666b26_curl.exe(272.5 KB) 文件类型： PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows 文件路径： C:\Users\Admin\AppData\Local\Temp\61D2.tmp\curl.exe SHA256： 44f1669e08666b26c47edda9a79ec993a5bfcf262cd7f2c71155257f8a00af96	（2144）Windows全版本激…	0/22	-	安全	

Win10(1903 64bit,Office2016)

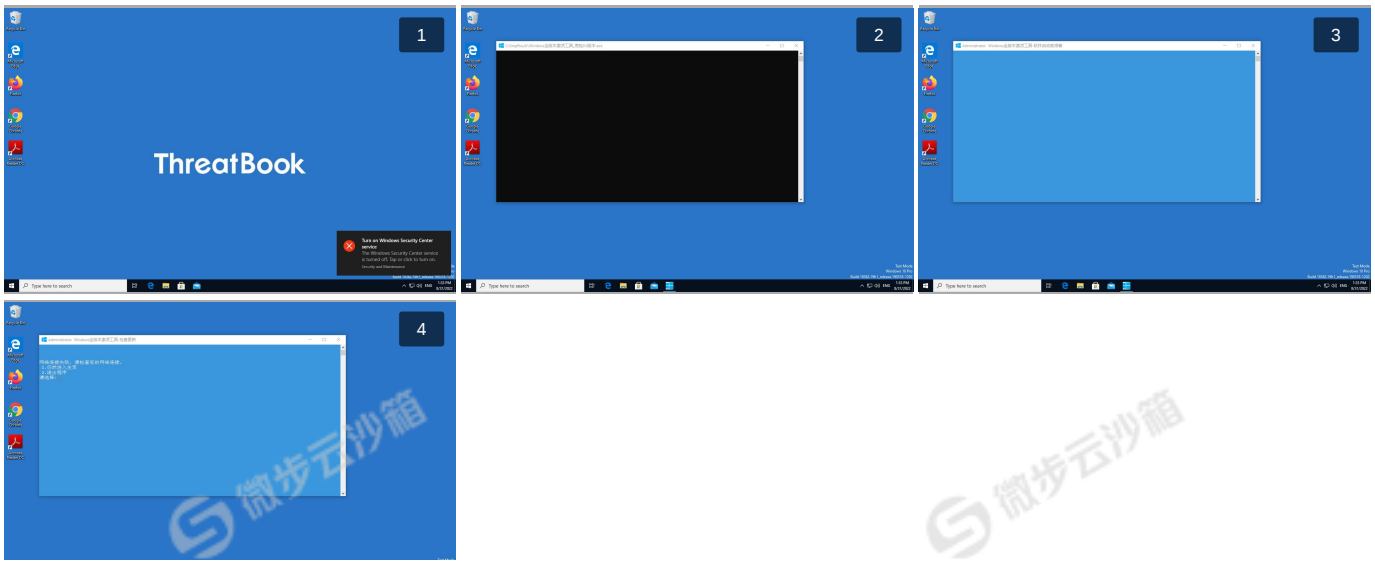
执行流程

进程详情

共分析了4个进程

- Windows全版本激活工具_底包9.0版本.exe（PID：7000）
  "C:\tmpflwy5r\Windows全版本激活工具_底包9.0版本.exe"
  - cmd.exe（PID：2368）
    "C:\Windows\sysnative\cmd" /c "C:\Users\Administrator\AppData\Local\Temp\CC24.tmp\CC25.tmp\CC26.bat "
    - wget.exe（PID：6640）
      wget -q http://chenchuanrui.gitee.io/services/actsev.bat
    - choice.exe（PID：6888）
      choice /c 12 /n /m "请选择: "

运行截图（4）



网络行为

指纹	域名	DNS	HTTP	TCP	Hosts	HTTPS	UDP	SMTP	ICMP	IRC	Dead-Hosts
3	1	1	1	1	1	0	0	0	0	0	0

指纹：3

协议	地址	指纹类型	指纹哈希	详情
HTTP	目的 IP 212.64.63.190:80	clientHeaderHash	d3a85c232b0a1ba9736e0fa9bd64cf35	host,user_agent,accept,accept_encoding,connection
HTTP	目的 IP 212.64.63.190:80	hfingerHash	b0f17740a7aeee91eed573cdeef038aa	1.3|2|1.0|bat|||GE|1|ho,us-ag,ac,ac-en,co|us-ag:af68cc82/ac:as-as/ac-en:id/co:Ke-Al|||
HTTP	源 IP 212.64.63.190:80	serverHeaderHash	186c7cdba181dd3071940b35bf7cea66	date,content_type,content_length,connection,server,location,cache_control

域名：1

域名	微步判定	情报内容	当前解析IP
chenchuanrui.gitee.io	安全	白名单	212.64.63.190

DNS：1

域名	请求	应答
chenchuanrui.gitee.io	A	CNAME → aoufnebg.dayugslb.com A → 212.64.63.190 212.64.63.215

HTTP：1

Timeshift	进程	响应头	URL	目标地址	内容
49ms	（6640）wget.exe	GET | 301	http://chenchuanrui.gitee.io:80/services...actsev.bat	212.64.63.190:80	0 B empty 182 B HTML doc...

TCP：1

Timeshift	进程	目标地址	微步判定	情报内容	流量
49ms	（6640）wget.exe	212.64.63.190:80	安全	白名单 腾讯云主机 IDC服务器	151 B 471 B

Hosts：1

IP地址	微步判定	情报内容	地理信息	ASN	使用场景
212.64.63.190	安全	白名单 腾讯云主机 IDC服务器	China Shanghai Shanghai City	45090(CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN)	Hosting

释放文件（13）

释放样本	进程	多引擎检出	威胁类型/木马家族	微步判定	操作
ca8ab5aeef734f24_7z.dll(1.18 MB) 文件类型： PE32 executable (DLL) (GUI) Intel 80386, for MS Windows 文件路径： C:\Users\Administrator\AppData\Local\Temp\CC24.tmp\7z.dll SHA256： ca8ab5aeef734f24a3c58bf10b3f0152c2ea1329b02d2730448693df563b4c6a	（7000）Windows全版本激…	0/22	-	安全	
59cbfba941d3ac02_7z.exe(329.5 KB) 文件类型： PE32 executable (console) Intel 80386, for MS Windows 文件路径： C:\Users\Administrator\AppData\Local\Temp\CC24.tmp\7z.exe SHA256： 59cbfba941d3ac0238219daa11c93969489b40f1e8b38fabdb5805ac3dd72bfa	（7000）Windows全版本激…	0/22	-	安全	
2171a75881e7800a_cc26.bat(1.13 KB) 文件类型： Unicode text, UTF-8 text, with CRLF line terminators 文件路径： C:\Users\Administrator\AppData\Local\Temp\CC24.tmp\CC25.tmp\CC26.bat SHA256： 2171a75881e7800ac8134bca2c3b355704fd2c603aa383430df52e93ca37c241	（7000）Windows全版本激…	0/22	-	安全	
44f1669e08666b26_curl.exe(272.5 KB) 文件类型： PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows 文件路径： C:\Users\Administrator\AppData\Local\Temp\CC24.tmp\curl.exe SHA256： 44f1669e08666b26c47edda9a79ec993a5bfcf262cd7f2c71155257f8a00af96	（7000）Windows全版本激…	0/22	-	安全	
ed23cf2f7ca6c126_favicon.ico(4.19 KB) 文件类型： MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel 文件路径： C:\Users\Administrator\AppData\Local\Temp\CC24.tmp\favicon.ico SHA256： ed23cf2f7ca6c126523e83be8007e10f0ead6f62f6ba16828b39044763afdc13	（7000）Windows全版本激…	0/25	-	安全	