

一个反斜杠背后的玄机：未公开APT32样本的反沙箱绕过手法 | CTF导航

ctfiot.com/293464.html

```
seg000:00... 00000029 C received http/1.1 match not allowed
seg000:00... 00000024 C nsupported HTTP/1 subversion in response
seg000:00... 00000024 C nsupported HTTP version in response
seg000:00... 0000002A C nsupported response code in HTTP response
seg000:00... 0000002C C nsupported HTTP version (%u.%d) in response
seg000:00... 00000056 C http://62.76.234.33:80/users/89b159ce-6bcd-49e9-b048-4d3a14c5c31d/profile/information
seg000:00... 000000D C %HTTP_PROXY%
```

文章首发地址：<https://xz.aliyun.com/news/91352>文章首发作者：筱一

概述

近日，笔者基于技术手段关注到一款未被曝光的APT32样本，由于此样本的相关IOC信息均未被曝光，故将分析结果共享。

通过分析，梳理此样本的运行逻辑如下：

- 此样本是一款img镜像文件，运行后会挂载为虚拟光驱，虚拟光驱目录中有一个lnk文件；
- lnk文件运行后，会以-render 1440参数加载运行隐藏的normalimebiz.exe程序；
- 正常imebiz.exe程序运行后，会利用白加黑技术加载恶意browser_host.dll文件；
- browser_host.dll文件有多个运行逻辑：
 - 以“-render 1440”参数运行：利用进程注入技术向符合特定条件的进程注入shellcode1，shellcode1的功能为自启动配置及以“-render 2160”参数重新运行imebiz.exe程序；
 - 以“-render 2160”参数运行：利用代码注入技术加载shellcode2，此shellcode2是一款shellcode化的rust特马，运行后将向C&C发起HTTP外联请求；

反沙箱绕过手法

在分析过程中，笔者发现此样本在不同使用场景下，运行结果有很大差异：

- 在操作系统上，直接双击运行，以虚拟光驱的方式加载木马，此木马可正常运行；
- 在调试过程中，按照其默认逻辑进行调试，在释放docx文档的环节，即会因为路径错误导致木马进程退出；

起初，笔者还以为这是攻击者设计时的BUG。。。
- 在沙箱平台上，VT平台查杀率为5/62，微步平台查杀率为0/28，整体查杀率都不高；
- 在沙箱平台上，此样本均未能成功运行。

进一步分析，笔者发现此样本在对抗反沙箱和反调试角度其实是有不少对抗手段的，但在这里，我们着重对上述现象进行剖析。

通过分析，笔者发现，导致上述现象出现的本质原因是：在释放docx文档的时候，会调用GetCurrentDirectoryW函数：

- 当木马运行路径为普通目录时，则GetCurrentDirectoryW函数将「返回不带的路径」，在调用swprintf_s函数构造目录路径时，目录路径错误；
 例如：C:UsersadminDesktop1
- 当木马运行路径为根目录时，则GetCurrentDirectoryW函数将「返回带的路径」，在调用swprintf_s函数构造目录路径时，目录路径有效；
 例如：C:

结合上述情况对沙箱平台运行逻辑进行剖析，发现「大部分沙箱均不会将img内的文件放置于根目录运行，大多数沙箱会直接将img文件解压后运行。」

相关截图如下：

杀毒引擎结果

VT查杀结果如下：

微步查杀结果如下：

沙箱运行逻辑

微步沙箱

CAPE Sanbox沙箱

邀请函回执.docx.IMG

文件名称：邀请函回执.docx.IMG文件大小：2131968 字节MD5：
BE59979320EEE15EA7D1C3710EEEA774SHA1：
32563C9743F781DF71A943ED9D4C8704F9B799A5CRC32：2C8E2A58

虚拟光驱加载

由于系统默认把.img文件关联到资源管理器，因此，直接双击此img镜像文件，系统会将其挂载成虚拟光驱。

相关截图如下：

隐藏文件

在虚拟光驱中，默认只能看到一个快捷方式文件。

尝试关闭“隐藏受保护的操作系统文件”，则可看到当前目录下存在多个隐藏文件。

相关截图如下：

邀请函回执docx.lnk

文件名称：邀请函回执docx.lnk文件大小：389 字节MD5：
CADBB414E7A68C64D756C92740C16370SHA1：
B7BE9DFB17A29A76C5B66A18D80800F1A2C2842ACRC32：AEC31D58

加载正常imebiz.exe

此快捷方式的功能为加载当前目录下的imebiz.exe程序，提取快捷方式命令行指令如下：

C:\Users\admin\Documents\imebiz.exe -render 1440

相关截图如下：

正常imebiz.exe

文件名称：imebiz.exe文件大小：234816 字节文件版本：1.0.0.2760MD5：
E96E1418577AFBC354D3C162E27A1376SHA1：
94D9CCF74DD7A3A9751F6CB2481154EFB66CA7EDCRC32：72843547

正常文件

imebiz.exe文件是一款正常的搜狗输入法程序。

相关截图如下：

白加黑

imebiz.exe程序运行后，将利用白加黑技术加载并调用当前目录下browser_host.dll文件的GetBrowserManagerInstance函数。

相关代码截图如下：

恶意browser_host.dll

文件名称：browser_host.dll文件大小：1817600 字节MD5：
91C6080D291095C800782E1847F1AD76SHA1：
22C32A473A8BEB76F58EC5B71D56651ADB075DEBCRC32：CBC998BA

获取API函数地址

样本运行后，将根据API哈希获取对应API函数地址。

相关代码截图如下：

运行模式判断

样本运行后，将根据当前进程的命令行参数执行不同程序逻辑：

- 模式1：命令行参数为“-render 1440”
- 模式2：命令行参数为“-render 2160”
- 模式3：不携带参数，则直接退出程序

相关代码截图如下：

模式1-反安全工具

若样本进入模式1执行逻辑，则样本将遍历进程并计算进程名hash，判断进程名hash是否匹配内置的0xDFDD71B0、0x48323A80、0x76BC4427、0x11134B36、0xF904DA01值：

- 若匹配，则将直接调用ExitProcess函数退出程序；
- 若不匹配，则执行后续逻辑；

相关代码截图如下：

模式1-打开”邀请函回执.docx“

若样本进入模式1执行逻辑，则样本将调用ShellExecuteW或CreateProcessW函数打开”邀请函回执.docx“文档。

相关截图如下：

相关代码截图如下：

模式1-写imebiz.log

若样本进入模式1执行逻辑，则样本将在TEMP目录下写imebiz.log文件，imebiz.log文件内容为当前程序路径信息。

相关截图如下：

相关代码截图如下：

模式1-进程注入

若样本进入模式1执行逻辑，则样本将遍历系统进程，寻找符合特定条件（64位系统、非系统路径、未被调试）的进程注入shellcode。

寻找符合特定条件进程的代码截图如下：

注入shellcode代码截图如下：

模式2-互斥对象

若样本进入模式2执行逻辑，则样本将创建互斥对象，确保系统中只存在一个进程实例，互斥对象名为：WebViewInstance_03

相关代码截图如下：

模式2-解密shellcode2

若样本进入模式2执行逻辑，样本将调用AES算法对内置的加密shellcode进行解密。

AES算法代码截图如下：

模式2-代码注入

若样本进入模式2执行逻辑，则样本将加载d3d10warp.dll文件，将shellcode2写入d3d10warp.dll文件的.text节内存中，从而实现代码注入。

相关代码截图如下：

shellcode1

拷贝文件

此shellcode运行后，将按照如下逻辑将相关文件拷贝至C:\Users\admin\AppData\Local\imebiz\目录：

- 从TEMP目录下读取imebiz.log文件内容，获取当前程序路径信息；
- 调用CopyFileW函数将imebiz.exe和browser_host.dll文件拷贝至C:\Users\admin\AppData\Local\imebiz\目录；

相关截图如下：

相关代码截图如下：

以模式2运行

成功拷贝文件后，shellcode将调用CreateProcessW函数加载运行imebiz.exe程序，运行参数为：

C:\Users\admin\AppData\Local\imebiz\imebiz.exe" -render 2160

相关代码截图如下：

自启动

shellcode运行后，还将创建注册表实现自启动，注册表参数为：

C:\Users\admin\AppData\Local\imebiz\imebiz.exe" -render 2160

相关截图如下：

相关代码截图如下：

shellcode2

外联通信

通过分析，发现此shellcode实际即为APT32常用的shellcode化rust特马，运行后将向<http://62.76.234.33:80/users/89b159ce-6bcd-49e9-b048-4d3a14c5c31d/profile/information>地址发起外联通信。

相关截图如下：

IOCs

```
#邀请函回执.docx.IMGBE59979320EEE15EA7D1C3710EEEA774#邀请函回执
docx.lnkCADBB414E7A68C64D756C92740C16370#browser_host.dll91C6080D291095C800782E1847F1AD76#
IP归属地：意大利 西西里大区 巴勒莫http://62.76.234.33:80/users/89b159ce-6bcd-49e9-b048-
4d3a14c5c31d/profile/information
```

| 本篇文章来源于微信公众号: T0daySeeker

© 版权声明

文章版权归作者所有，未经允许请勿转载。