這幾招技術，病毒木馬經常用!

SpyGOD 黑客技術與網絡安全 2021-12-22 08:30

> **來自公眾號：小白學黑客**

惡意代碼的分類包括計算機病毒、蠕蟲、木馬、後門、Rootkit、流氓軟件、間諜軟件、廣告軟件、殭屍(bot) 、Exploit等等，雖然功能不同，形態各異，但有些技術是它們基本都會使用的，這篇文章就來簡單聊一聊。

惡意代碼常見功能技術如下：

- 進程遍歷
- 文件遍歷
- 按鍵記錄
- 後門
- 桌面截屏
- 文件監控
- 自刪除
- U盤監控

知己知彼，百戰不殆。這裡旨在給反病毒工程師提供參照，切勿從事違法事情，病毒作者請繞過。

0x01 進程遍歷

進程遍歷獲取計算機上所有進程的信息（用戶進程，系統進程），通常是為了檢索受害進程，檢測是否運行在虛擬機中，以及是否存在殺軟等，有時候反調試技術也會檢測進程名，所以在惡意代碼中進程遍歷很常見。

具體流程

1 調用CreateToolhelp32Snapshot獲取所有進程的快照信息之所以稱為快照是因為保存的是之前的信息，該函數返回進程快照句柄。

2 調用Process32First獲取第一個進程的信息，返回的進程信息保存在PROCESSENTRY32結構體中，該函數的第一個參數是CreateToolhelp32Snapshot返回的快照句柄。

3 循环调用Process32Next从进程列表中获取下一个进程的信息，直到Process32Next函数返回FALSE，GetLastError的错误码为ERROR_NO_MORE_FILES,则遍历结束

4 关闭快照句柄并释放资源

遍历线程和进程模块的步骤和上面的相似，线程遍历使用Thread32First和Thread32Next,模块遍历使用Module32First和Module32Next

0x02 文件遍历

文件操作几乎是所有恶意代码必备的功能，木马病毒窃取机密文件然后开一个隐秘端口，就算是在内核模式下，也经常会创建写入读取文件，文件功能经常用到。

文件搜索功能主要是通过调用FindFirstFile和FindNextFile来实现

具体流程

1 调用FindFirstFile函数，该函数接收文件路径，第二个参数指向WIN32_FIND_DATA结构的指针。若函数成功则返回搜索句柄。该结构包含文件的名称，创建日期，属性，大小等信息。该返回结构中的成员dwFileAttributes为FILE_ATTRIBUTE_DIRECTORY时表示返回的是一个目录，否则为文件，根据cFileName获取搜索到的文件名称。如果需要重新对目录下的所有子目录文件都再次进行搜索的话，则需要对文件属性进行判断。若文件属性是目录，则继续递归搜索，搜索其目录下的目录和文件。

2 调用FindNextFile搜索下一个文件，根据返回值判断是否搜索到文件，若没有则说明文件遍历结束。

3 搜索完毕后，调用FindClose函数关闭搜索句柄，释放资源缓冲区资源。

0x03 按键记录

收集用户的所有按键信息，分辨出哪些类似于账号，密码等关键信息进行利用，窃取密码，这里用原始输入模型直接从输入设备上获取数据，记录按键信息。

要想接收设备原始输入WM_INPUT消息，应用程序必须首先使用RegisterRawInputDevice注册原始输入设备，因为在默认情况下，应用程序不接受原始输入。

具体流程

1 注册原始输入设备

一个应用程序必须首先创建一个RAWINPUTDEVICE结构，这个结构表明它所希望接受设备的类别，再调用RegisterRawInputDevices注册该原始输入设备。将RAWINPUTDEVICE结构体成员dwFlags的值设置为RIDEV_INPUTSINK,即使程序不处于聚焦窗口，程序依然可以接收原始输入。

2 获取原始输入数据

消息过程中调用GetInputRawData获取设备原始输入数据。在WM_INPUT消息处理函数中，参数lParam存储着原始输入的句柄。此时可以直接调用GetInputRawData函数，根据句柄获取RAWINPUT原始输入结构体的数据。dwType表示原始输入的类型，RIM_TYPEKEYBOARD表示是键盘的原始输入，Message表示相应的窗口消息。WM_KEYBOARD表示普通按键消息，WM_SYSKEYDOWN表示系统按键消息，VKey存储键盘按键数据。

3 保存按键信息

GetForegroundWindow获取按键窗口的标题,然后调用GetWindowText根据窗口句柄获取标题，存储到本地文件。

0x04 后门

后门常以套件的形式存在，用于将受害者信息发送给攻击者或者传输恶意可执行程序（下载器），最常用的功能是接收攻击端传送过来的命令，执行某些操作。

Windows系统中有很多WIN32 API可以执行CMD命令，例如system Winexe CreateProcess等。这里介绍通过匿名管道实现远程CMD

具体过程

1 调用CreatePipe创建匿名管道，获取管道数据读取句柄和写入句柄

2 初始化STARTUPINFO结构体，隐藏进程窗口，并把管道数据写入句柄赋值给新进程控制台窗口的缓存句柄

3 调用CreateProcess函数创建进程，执行CMD命令并调用WaitForSingleObject等待命令执行完

4 调用ReadFile根据匿名管道的数据读取句柄从匿名管道的缓冲区中读取数据

5 关闭句柄，释放资源

0x05 文件监控

全局钩子可以实现系统监控，Windows提供了一个文件监控接口函数ReadDirectoryChangesW，该函数可以对计算机上所有文件操作进行监控。

在调用 ReadDirectoryChangesW设置监控过滤条件之前，需要通过CreateFile函数打开监控目录，获取监控目录的句柄，之后才能调用ReadDirectoryChangesW函数设置监控过滤条件并阻塞，直到有满足监控过滤条件的操作，ReadDirectoryChangesW才会返回监控数据继续往下执行。

具体过程

1 打开目录，获取文件句柄，调用CreateFile获取文件句柄，文件句柄必须要有FILE_LIST_DIRECTORY权限

2 调用ReadDirectoryChangesW设置目录监控

3 判断文件操作类型，只要有满足过滤条件的文件操作，ReadDirectoryChangesW函数会立马返回信息，并将其返回到输出缓冲区中，而且返回数据是按结构体FILE_NOTIFY_INFORMATION返回的

调用一次ReadDirectoryChangesW函数只会监控一次，要想实现持续监控，则需要程序循环调用来设置监控并获取监控数据，由于持续的目录监控需要不停循环调用会导致程序阻塞，为了解决主线程阻塞的问题，可以创建一个文件监控子线程，把文件监控的实现代码放到子线程中

0x06 自删除

自删除功能对病毒木马来说同样至关重要，它通常在完成目标任务之后删除自身，不留下任何蛛丝马迹，自删除的方法有很多种，常见的有利用MoveFileEx重启删除和利用批处理删除两种方式

MoveFileEx重启删除

MOVEFILE_DELAY_UNTIL_REBOOT这个标志只能由拥有管理员权限的程序或者拥有本地系统权限的程序使用，而且这个标志不能MOVEFILE_COPY_ALLOWED一起使用，并且，删除文件的路径开头需要加上“?"前缀

利用批处理命令删除

del %0 批处理命令会将自身批处理文件删除而且不放进回收站

具体流程

1 构造自删除批处理文件，该批处理文件的功能就是先利用choice或ping命令延迟一定的时间，之后才开始执行删除文件操作，最后执行自删除命令

2 在程序中创建一个新进程并调用批处理文件，程序在进程创建成功后，立刻退出整个程序

> 以上文章来自看雪论坛，经过小白修改校正：
>
> 原文链接：https://bbs.pediy.com/thread-263545.htm

看完这篇文章，你有什么收获吗，欢迎转发分享哦~

--- EOF ---

推荐↓↓↓

Linux学习

专注分享Linux/Unix相关内容，包括Linux命令、Linux内核、Linux系统开发、Linu...

公众号

喜欢此内容的人还喜欢

Linus 全身每一个细胞都在拒绝 GPLv3

开源前线

自动化分析Windows系统缺失的补丁及对应的漏洞情况(上)

嘶吼专业版

炸锅了！Apache Log4j2 核弹级漏洞公开

程序員書庫