

病毒分析 | 一只“蜗牛”偷梁换柱，靠锁主页进行牟利

 渔村安全 

 2018-01-12

共50187人围观，发现 5 个不明物体

[安全报告](#)

一、概述

众所周知，导航推广、淘宝客劫持可以给渠道商带来巨大的利益，使得木马病毒制造者纷纷变成推广渠道商。一些明的病毒制造者利用锁页生成器，以“造福”推广技术人员为由，让其助力进行木马传播。在这期间，病毒制造者再行偷梁换柱，通过云配替换成自己的推广链接，并对国美，京东，苏宁，淘宝等电商进行劫持。据统计，截至到目共有438397位网民中招。



图1：蜗牛锁页QQ 群

1.母体分析

蜗牛主页是一套很全的主页锁定木马，模块和功能也比较多，整体的模块和功能说明如下：

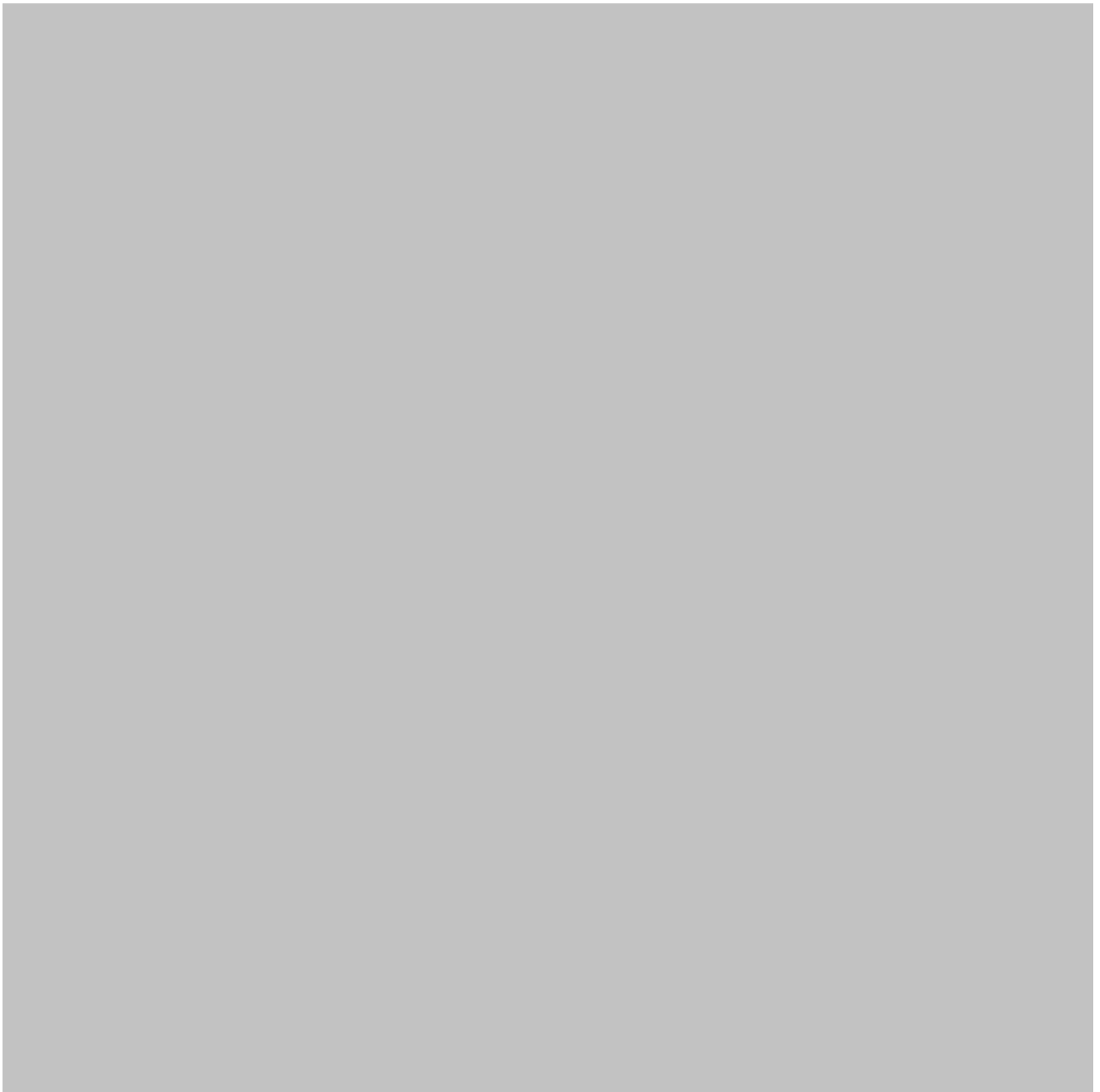


图2：蜗牛锁页框架



图3：蜗牛锁页生成器

木马制作者会向推广人员提供一个生成器（如上图），当推广人员填写完推广id和锁定的链接并点击“生成静默包”会在当前目录下生成名叫LockPage.exe的文件，该文件就是用于传播的母体，其主要负责工作如下：

a.解密释放配置文件sss.dat，该文件用于保存“插件模块”的存放目录信息，创建com组件注册表的路径等信息。



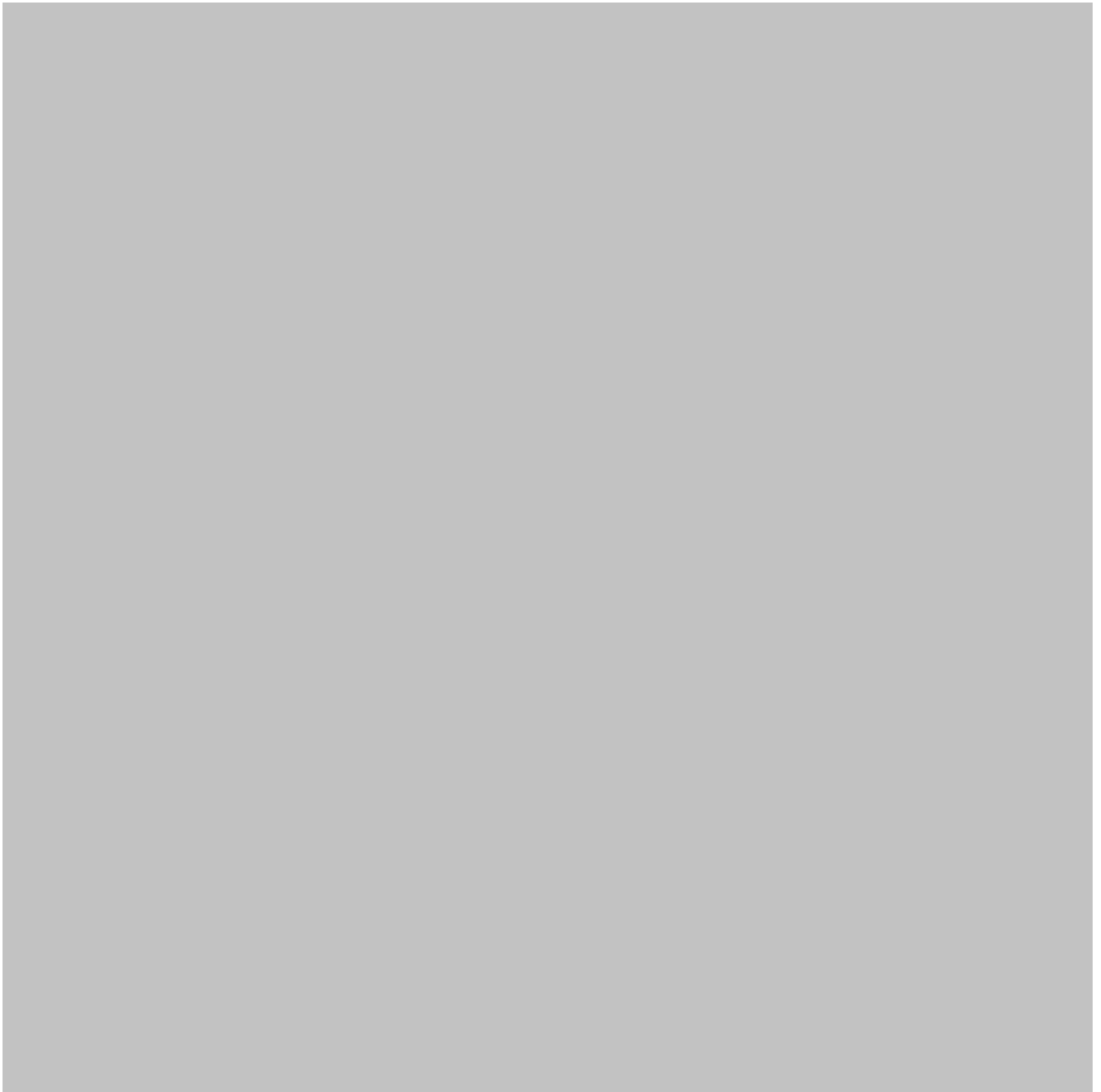


图4：蜗牛锁页sss.dat配置

b.解密释放文件config.dat到%temp%和C:\ProgramFiles\Common Files\System 目录下，该文件保存导航主页的配置信息。





图5：蜗牛锁页主页配置文件

c.根据系统版本数位不同，释放safe32.dat或者safe64.dat命名为safe.zip，并将文件生成到”%temp%”和 C:\ProgramFiles\Common Files\System\目录下，safe32.dat 和safe64.dat是主页劫持的核心模块。



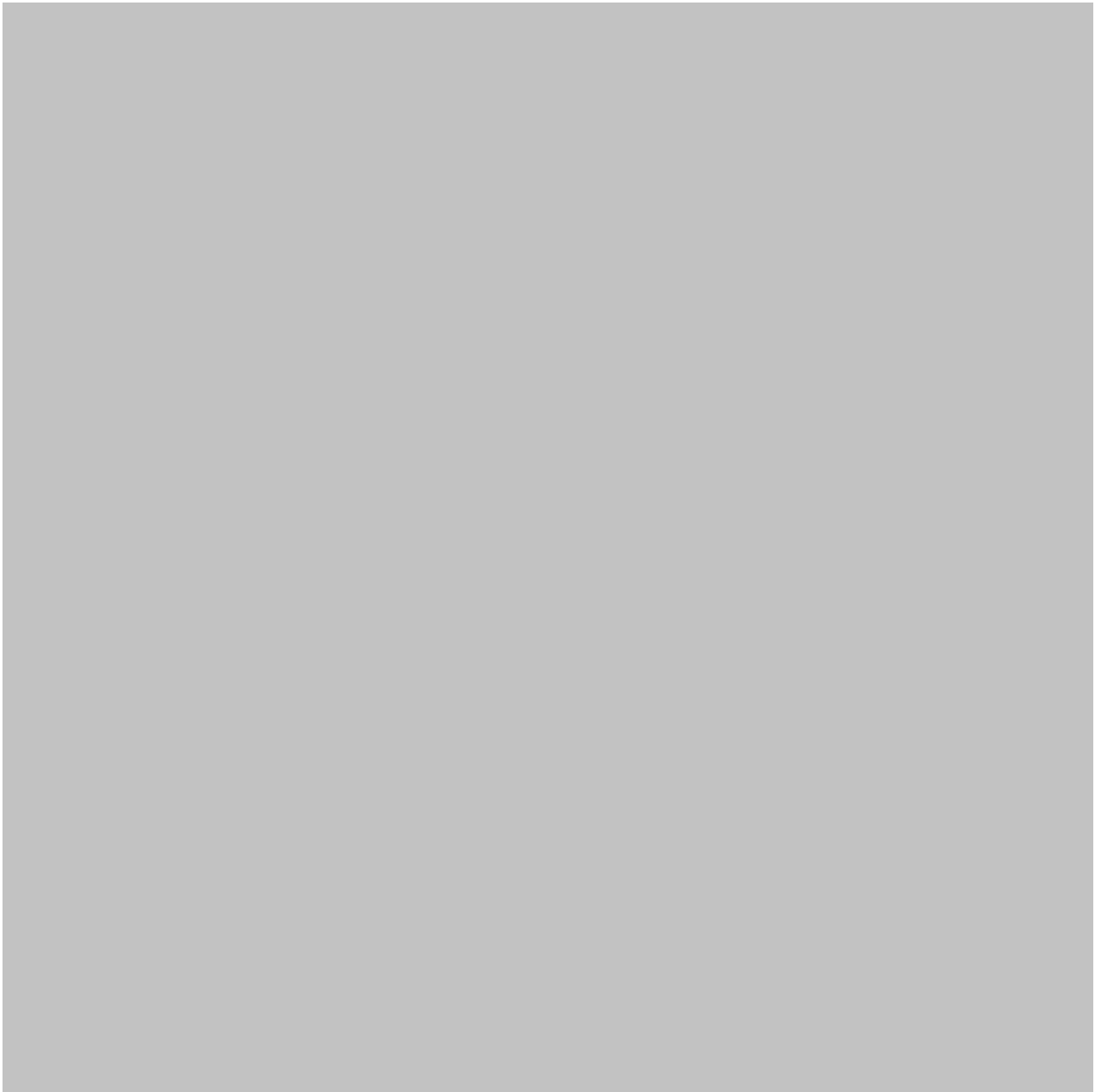


图6：释放safe32.zip和 safe64.zip

d. 木马通过该创建COM组件接口的方式将safemonn.dll进行注入explorer中

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlays\1\IconHandlerList\{8D6E9E7B-57C4-4080-AAAE-5DC03C45B9D7}\InProcServer32
```

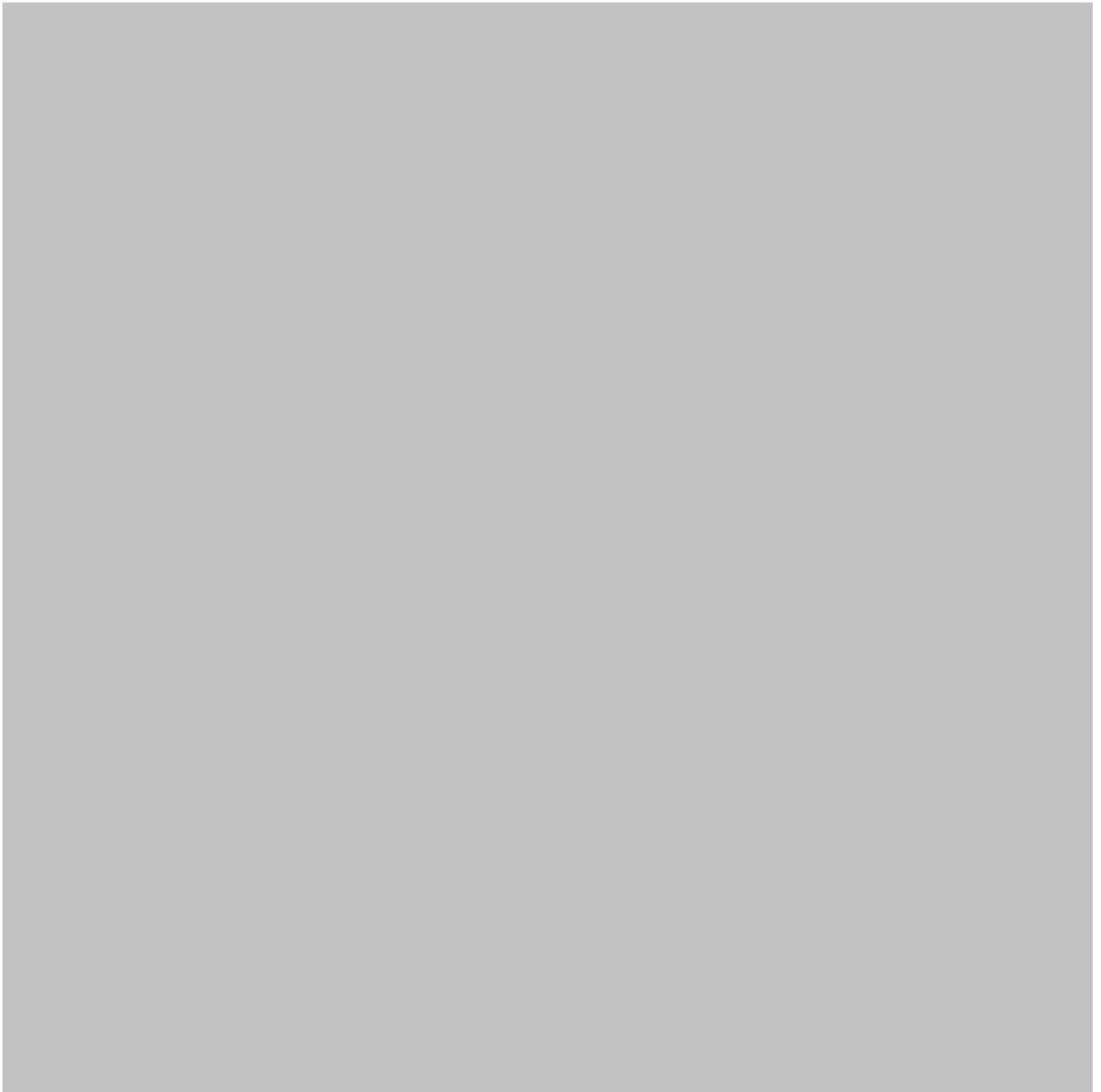


图7：添加com组件

e.根据不同版本位数的系统解密释放safemonn32.dll或者safemonn64.dll文件到C:\ProgramFiles\Common Files\System\Inf下。



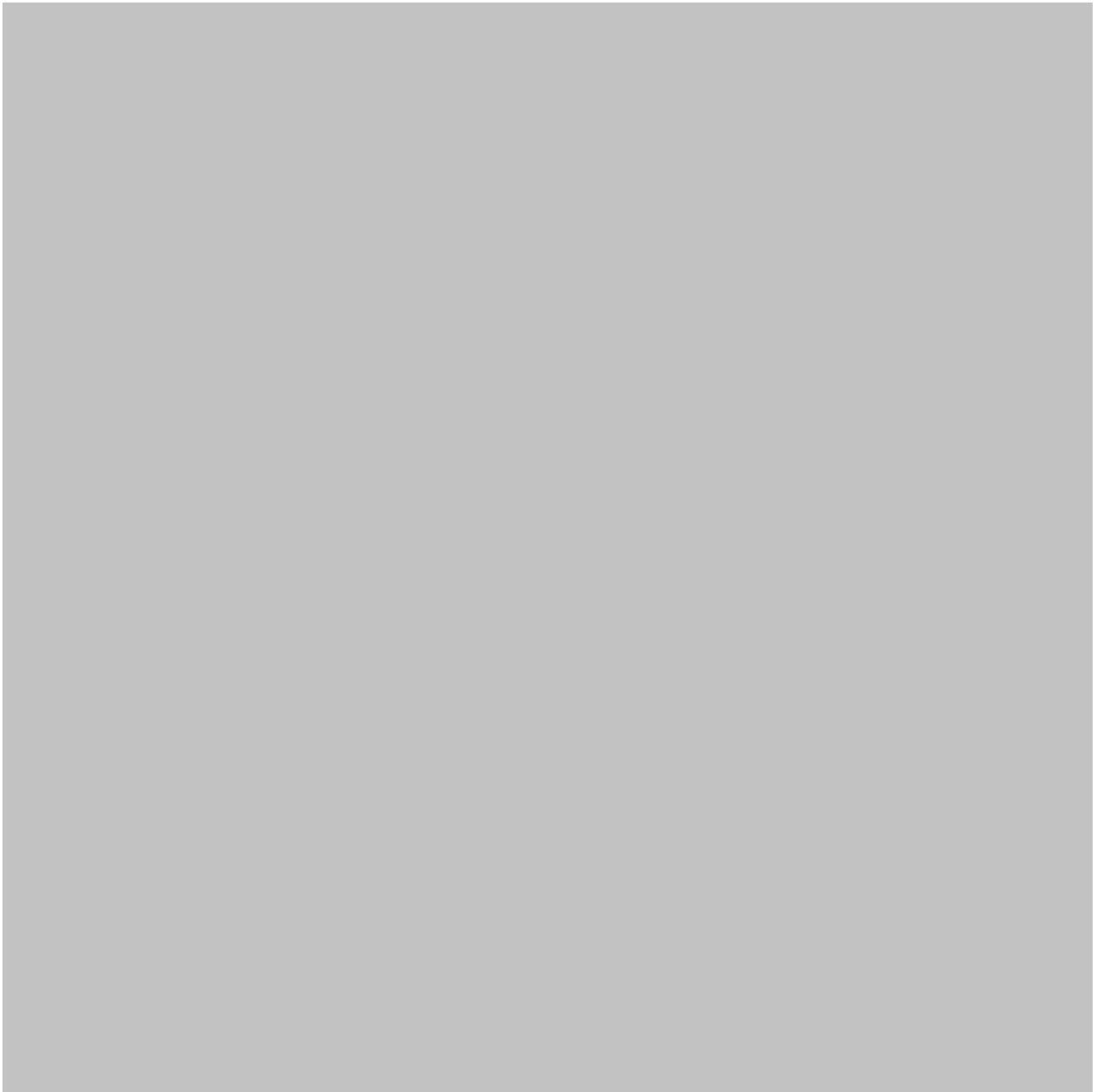


图8：释放safemonn32.dll或safemonn64.dll

f.做完以上操作后，木马会重启Explorer进程，并自删除。这时safemonn.dll将被explorer自动加载启动。



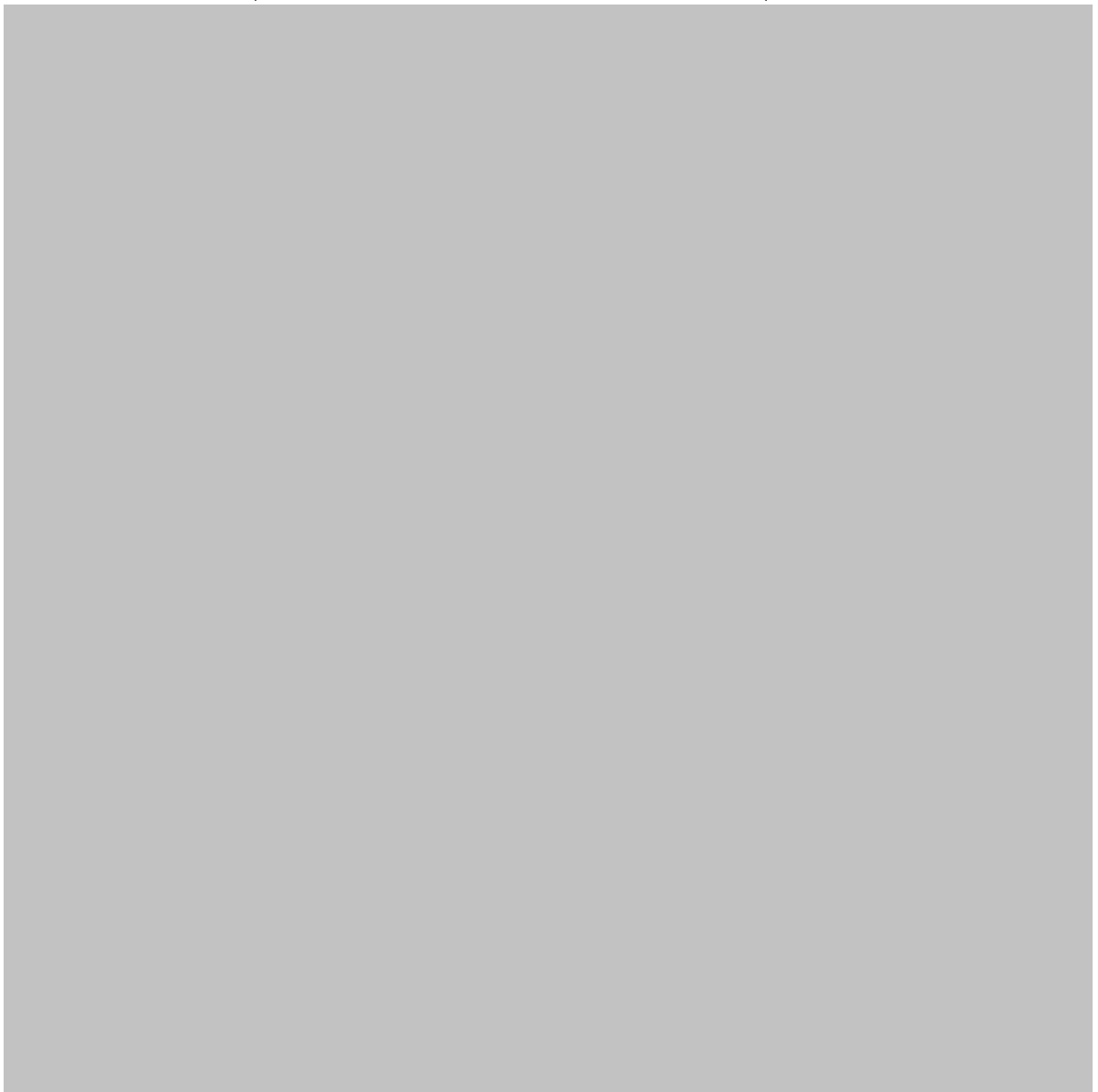


图9：重启Explorer

2.safemonn分析

Safemonn它的在整个模块中扮演的loader的”角色”，负责加载safe32.dat或者safe64.dat和卸载自身。首先safemonn会判断当前模块名是否为空，如果不是就在当前进程开辟一段内存空间并将自己拷贝到该内存中，然后进行PE文件重定位复等工作，最后调用自身DLLMAIN。



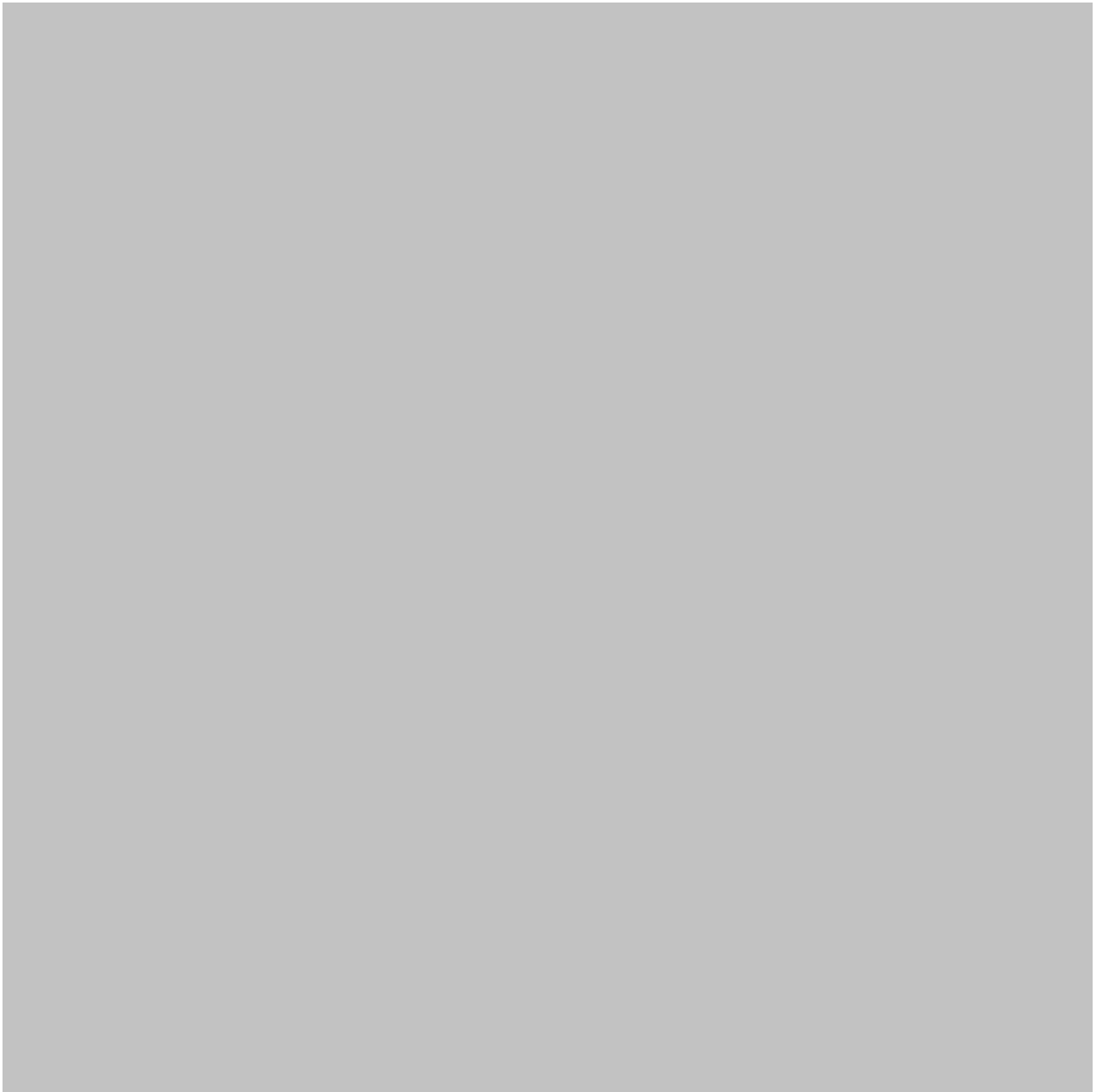


图10：内存加载自身

自身DLLMAIN被调用后，接下来木马会尝试对LdrLoadDll函数进行 inline Hook，如果LdrLoadDll函数地址获取不成功，则获取LoadLibraryW函数的地址进行inline Hook，作者的目的是为了让自己的运行在当前进程内存中，并卸载当前进程的自身模块，不让分析人员发现有可疑DLL的存在。



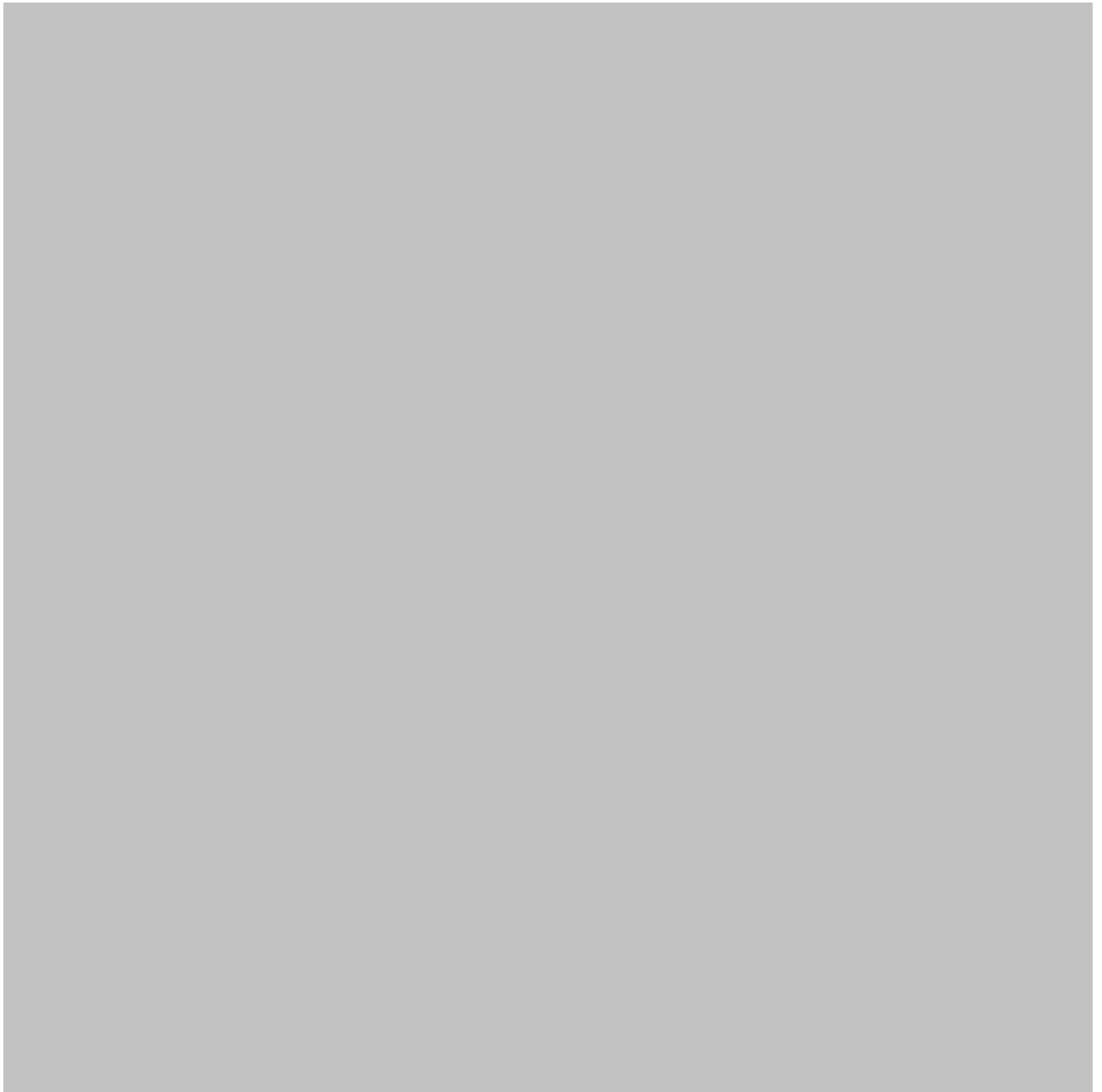


图11：HookLdrLoadDll



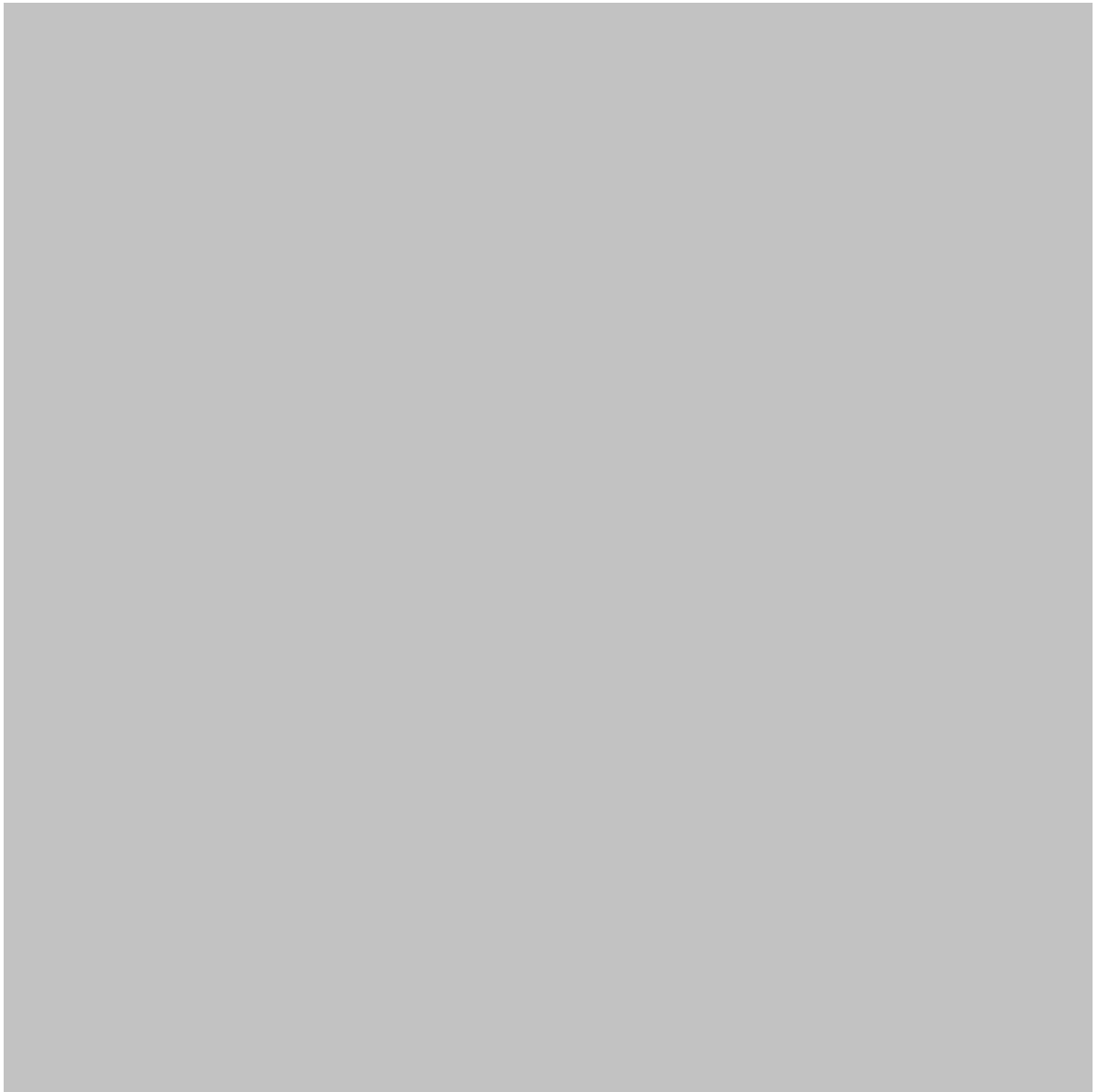


图12:卸载模块

做完以上的步骤后，接下来创建一个隐藏的Dialog，当Dialog被初始化时（MSG= WM_INITDIALOG）将会启动一·线程，该线程主要完成对C:\Program Files\Common Files\System\目录下的safe32.dat或者safe64.dat文件进行解密并内加载(ps:如果safe32.dat或者safe64.dat不存在，那么将会从服务器上下载进行解密加载)





图13:加载safe32.dat或者safe64.dat

3.safe32.dat分析

Safe32.dat它被保存在C:\ProgramFiles\Common Files\System目录下并以safe.dat命名，该样本在整个模块中负责主页劫持，加载模块safe32.dll(ps：与safe32.dat同名而已)，nline hook CreateProcessW，配置环境检测还原，信息上报，主页配置文件更新等。



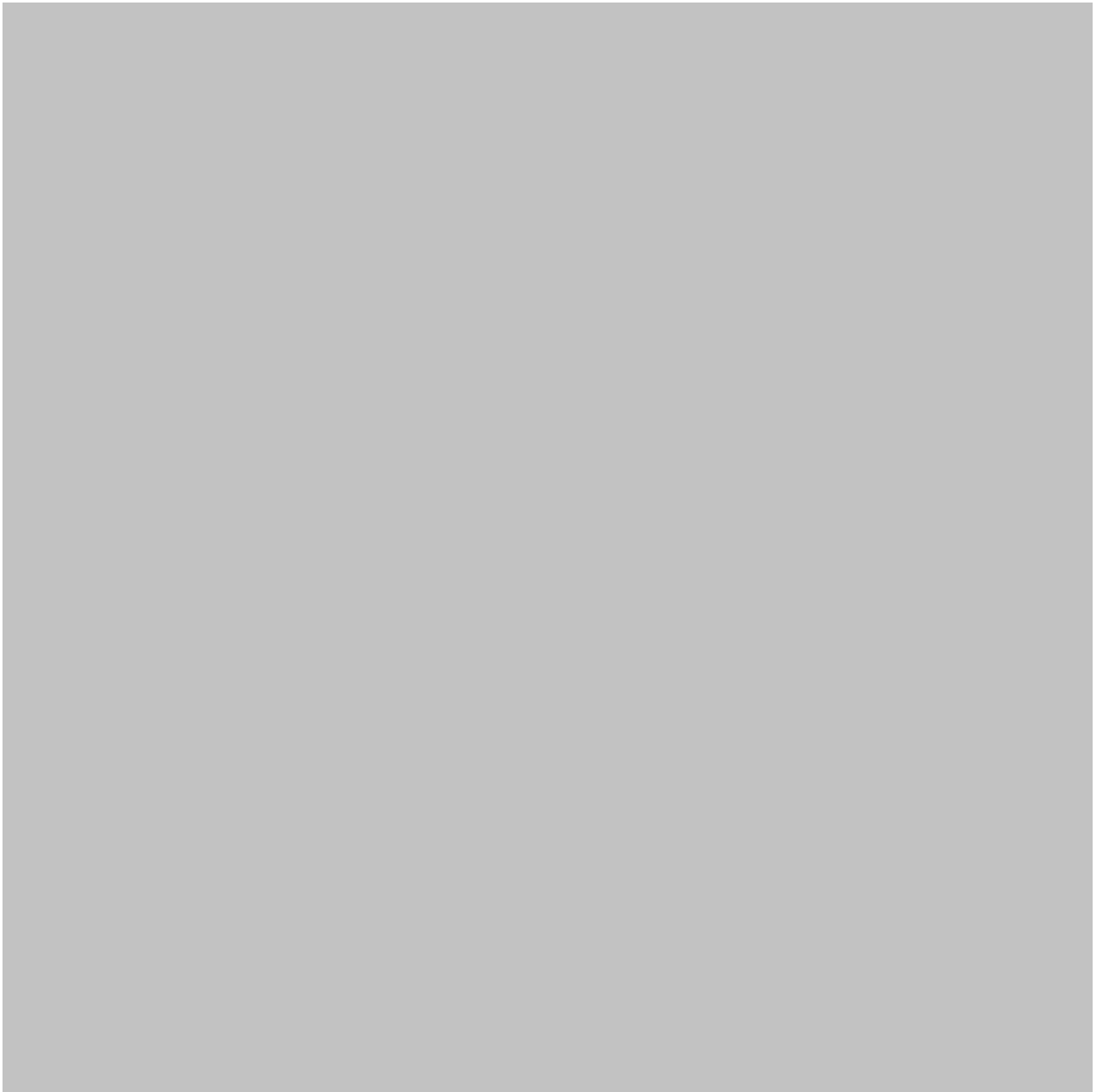


图14 资源

a、从资源中读取safe32.dll，进行异或0xA加密后保存在C:\\ProgramFiles\\Common Files\\System\\ado\\ hehe.dat做一份，然后创建sort.exe进程做为傀儡进程，通过枚举safe32.dll导出表找到导出函数Loadpe地址，传递safe32.dll(自身)为参数，以远程线程的方式注入到傀儡进程sort.exe中。





图15:傀儡进程

b、从资源中释放reload.sys，进行异或0xA加密后保存在C:\\ProgramFiles\\Common Files\\System\\ado\\uiprotect.dat做次备份，然后检测reload.sys驱动是否已经被加载，如果没有加载，则进行驱动的加载。并生成一份未加密的在C:\\Program Files\\Common Files\\System\\uiprotect.sys，最后加载驱动。



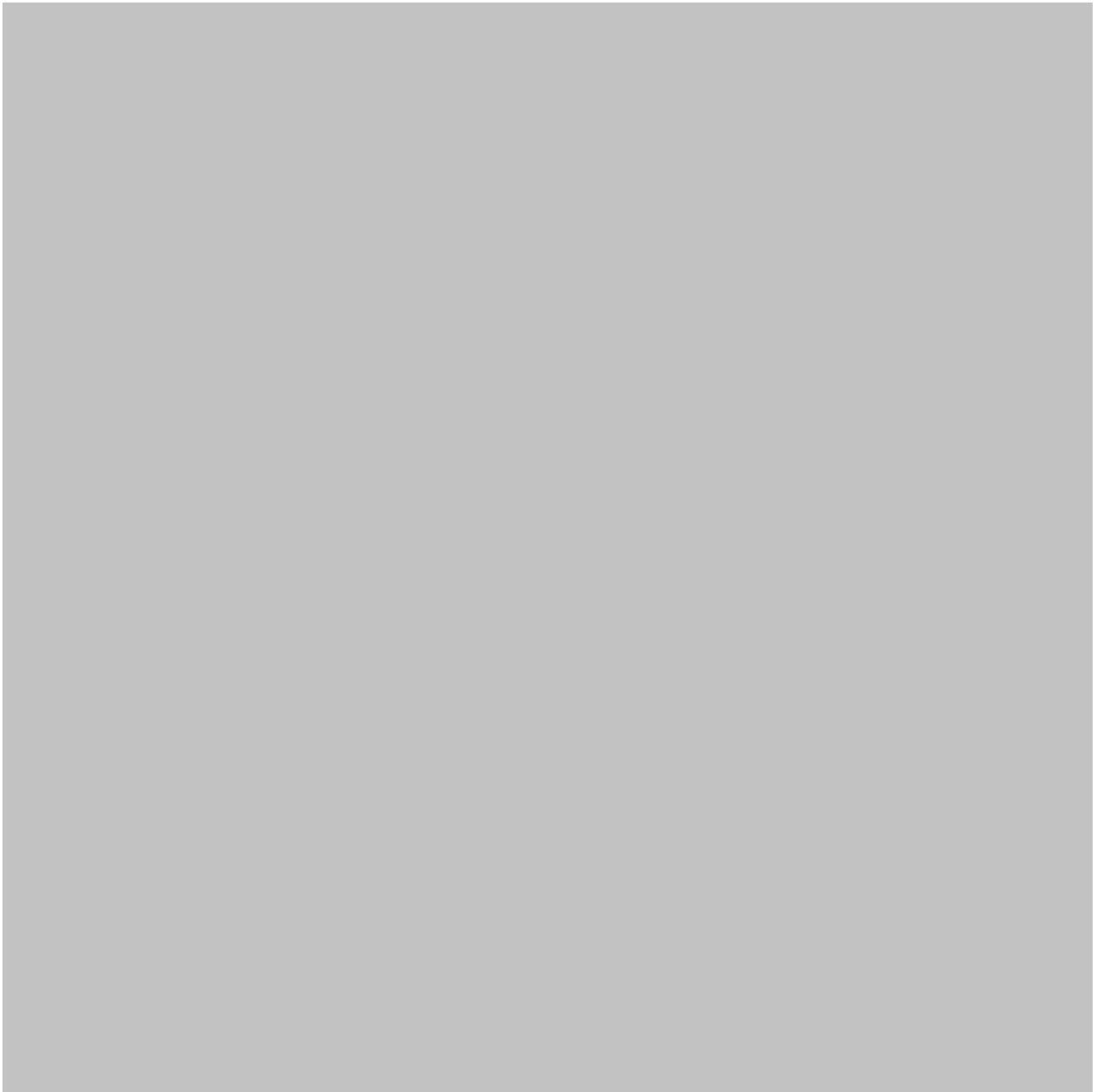


图16：木马驱动注册表

C、作者为了起到双保险效果，对CreateProcessW函数进行inlinehook，在浏览器启动后，在浏览器后面添加参数，到劫持的主页的效果。



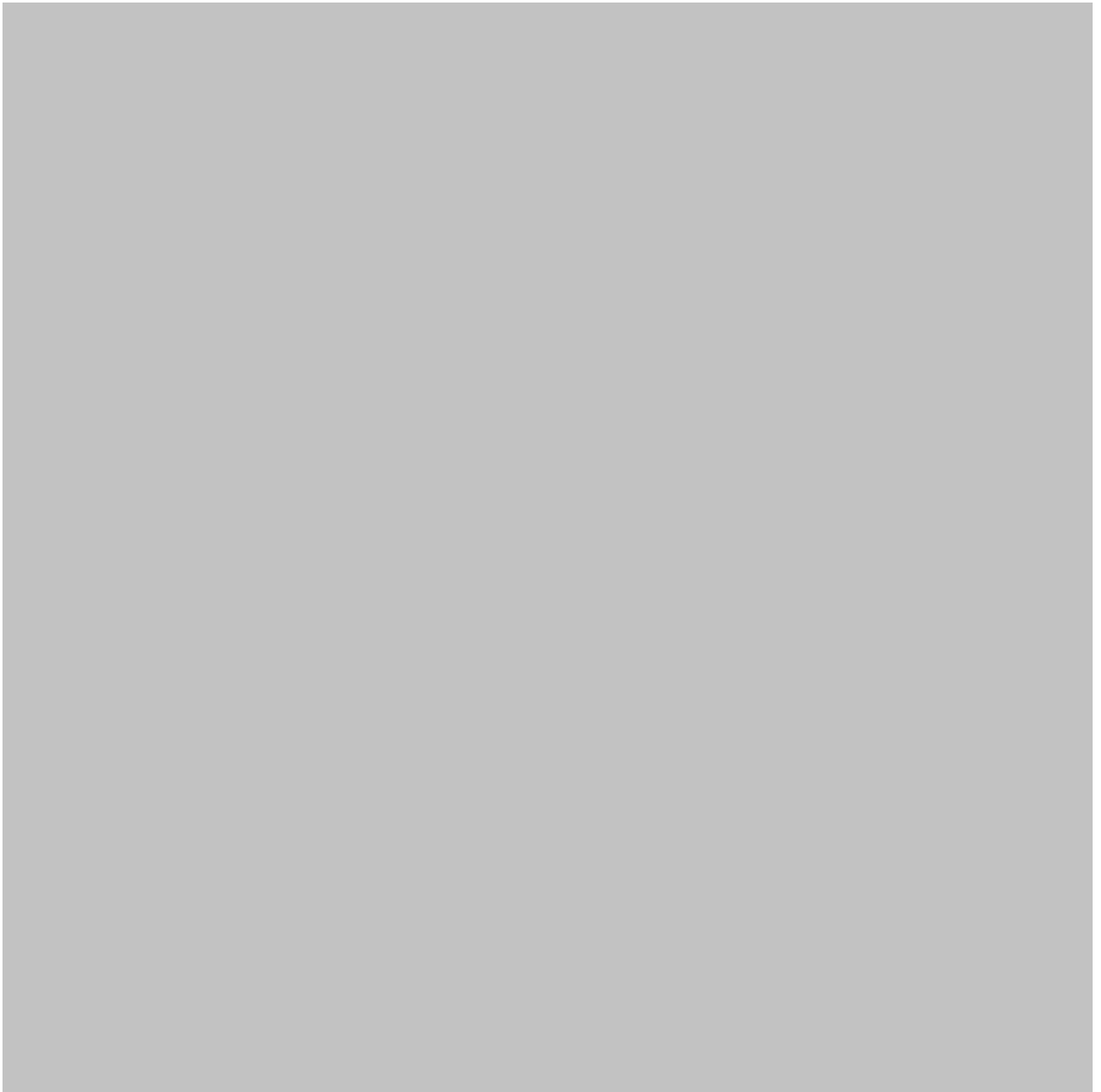


图17：Hook CreateProcessW

劫持的浏览器列表如下：

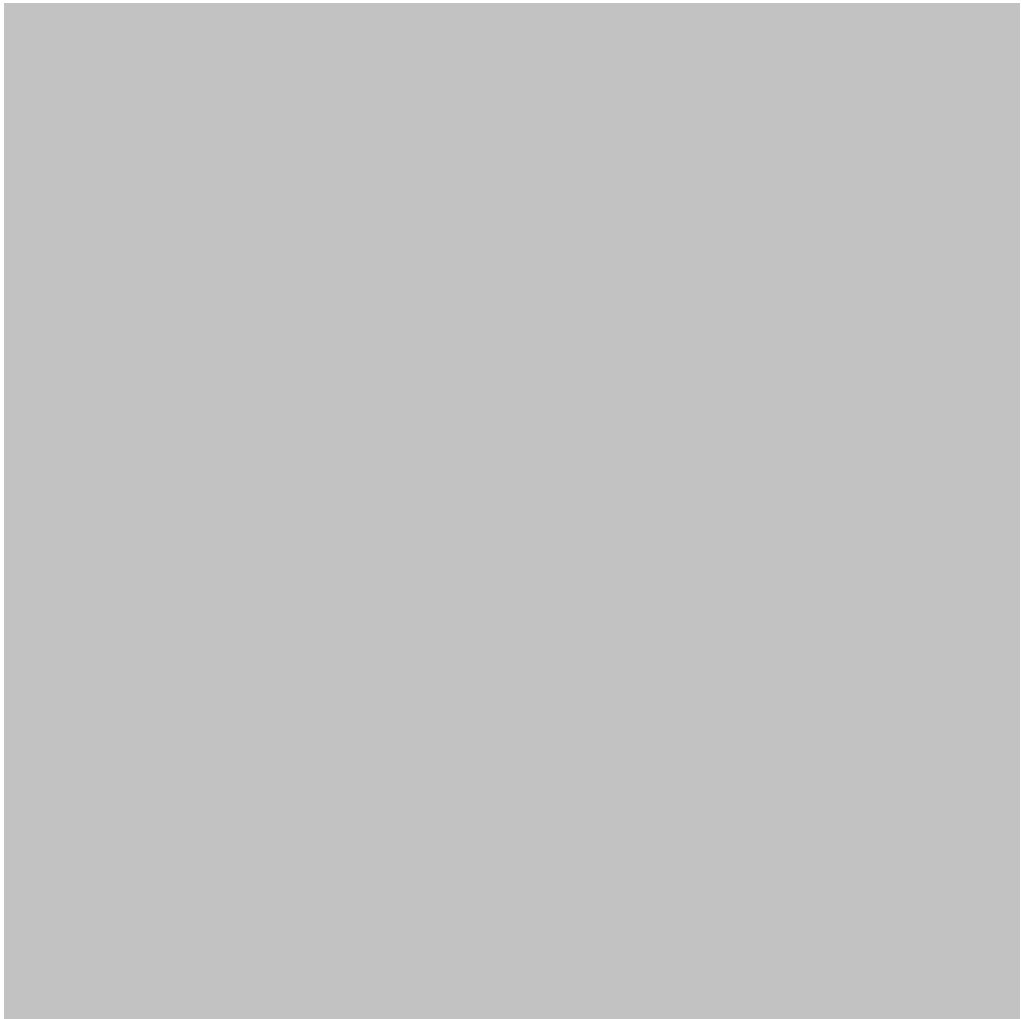


图18:被劫持的浏览器

木马还会对桌面上的浏览器快捷方式做劫持。





图19:浏览器快捷方式被劫持

d、木马会检测自己的配置文件是否已经被删除，如果文件不存在。则发控制码0×222024给驱动，准备还原配置文件。



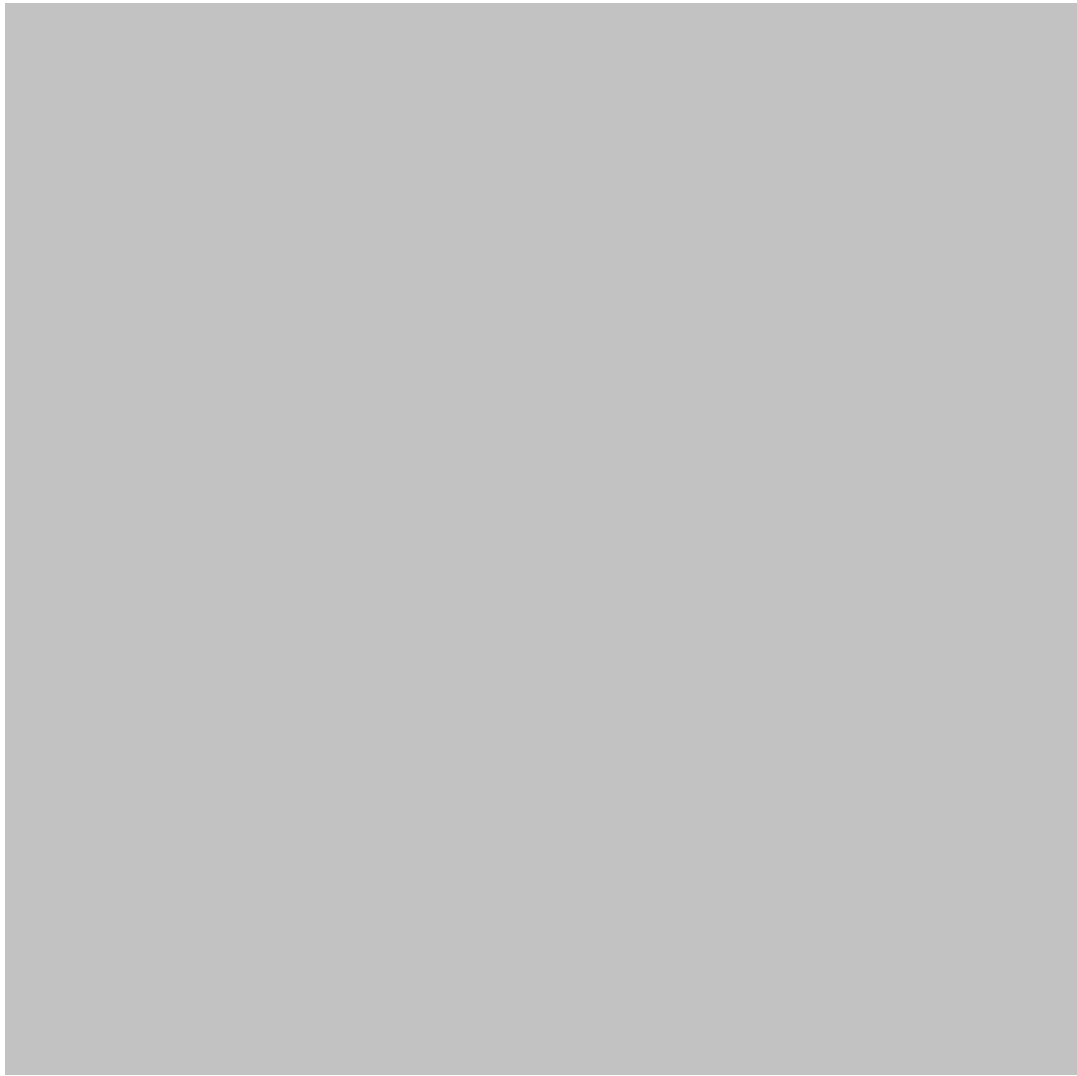


图20:恢复配置文件

e、访问<http://www.woniulock.com/taobaoke.php?domain=http://www.woniulock.com/>获取淘宝客配置文件,并发送控制0x222018把内容交给驱动。





图21：淘宝客内容

f、统计用户电脑信息以http方式向服务端发送格式如下：

www.woniulock.com/getwinmm.php?type=1&compName=&visiteNow=&code=&ip=&sys=&ver=&setuptime=&qq=&md5=

g、木马根据用户机器名计机码进行一次md5计算，然后向服务端发送请求进行md5查寻，如果服务端配置好机器码md5和客户端请求的md5值一致，那么就会新返回id号，url等等值，然后去修改config.dat（主页配置文件）的id、url等等字段（作者想黑吃黑）。



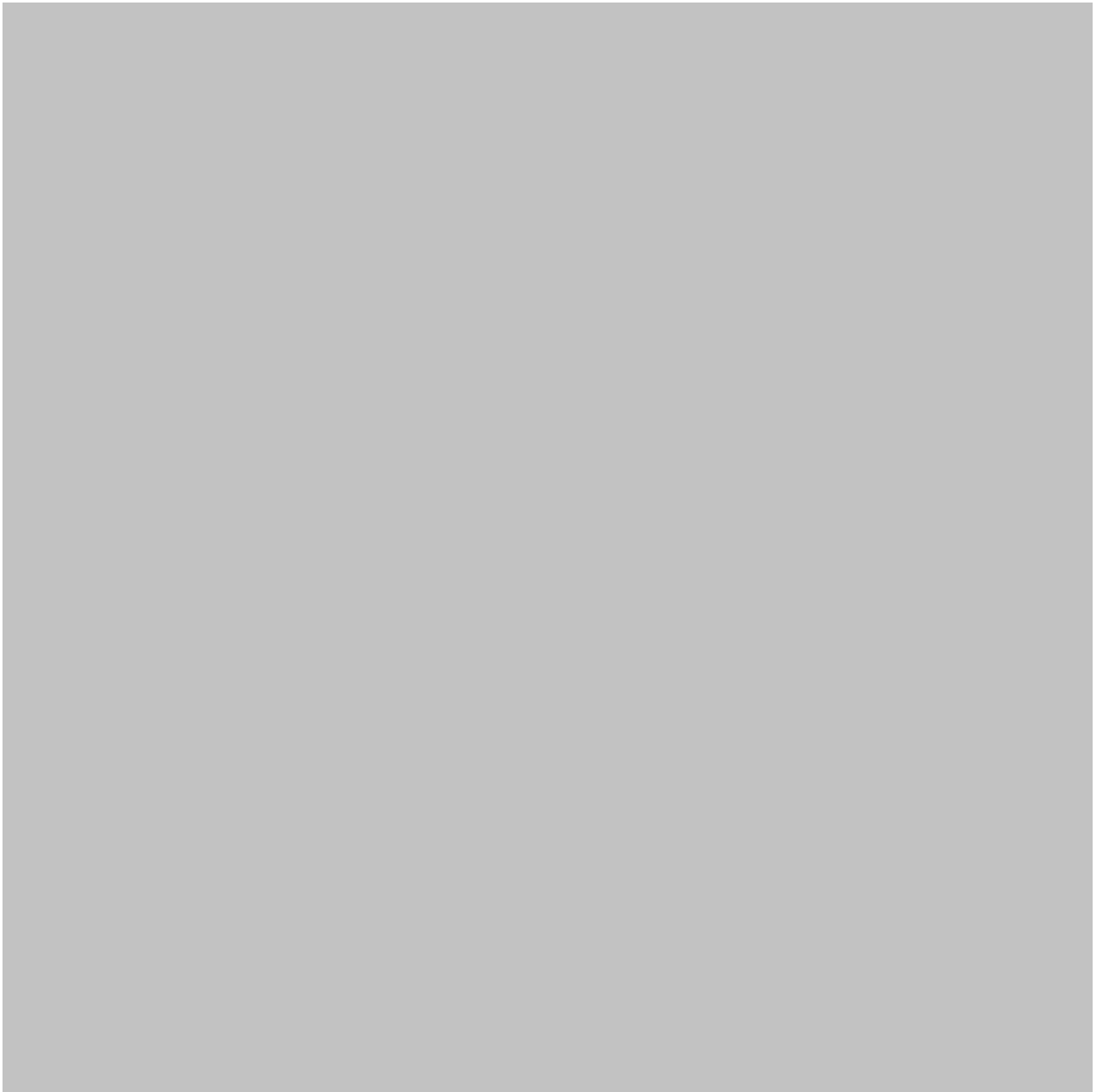


图22：修改config.dat配置文件

h、根据机器码查询获取广告配置，不过根据病毒后台显示该功能目前疑似暂未启用。



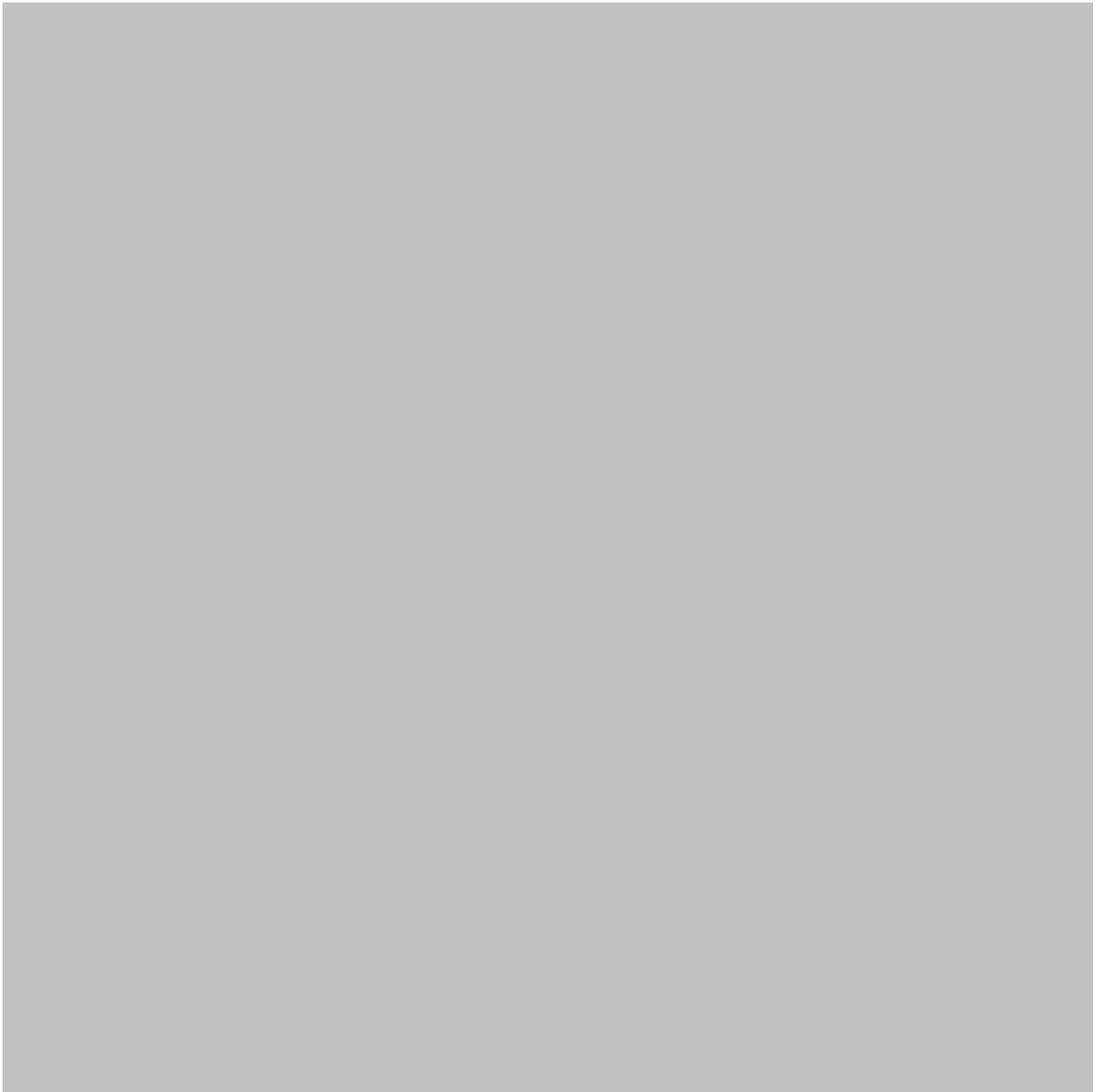




图23：广告模拟点击

4.safe32.dll(hehe.dat)分析

Safe32.dll(hehe.dat) 是浏览器劫持模块它被内核层注入到浏览器中，通过读取config.dat中的url字段获取主页信息。

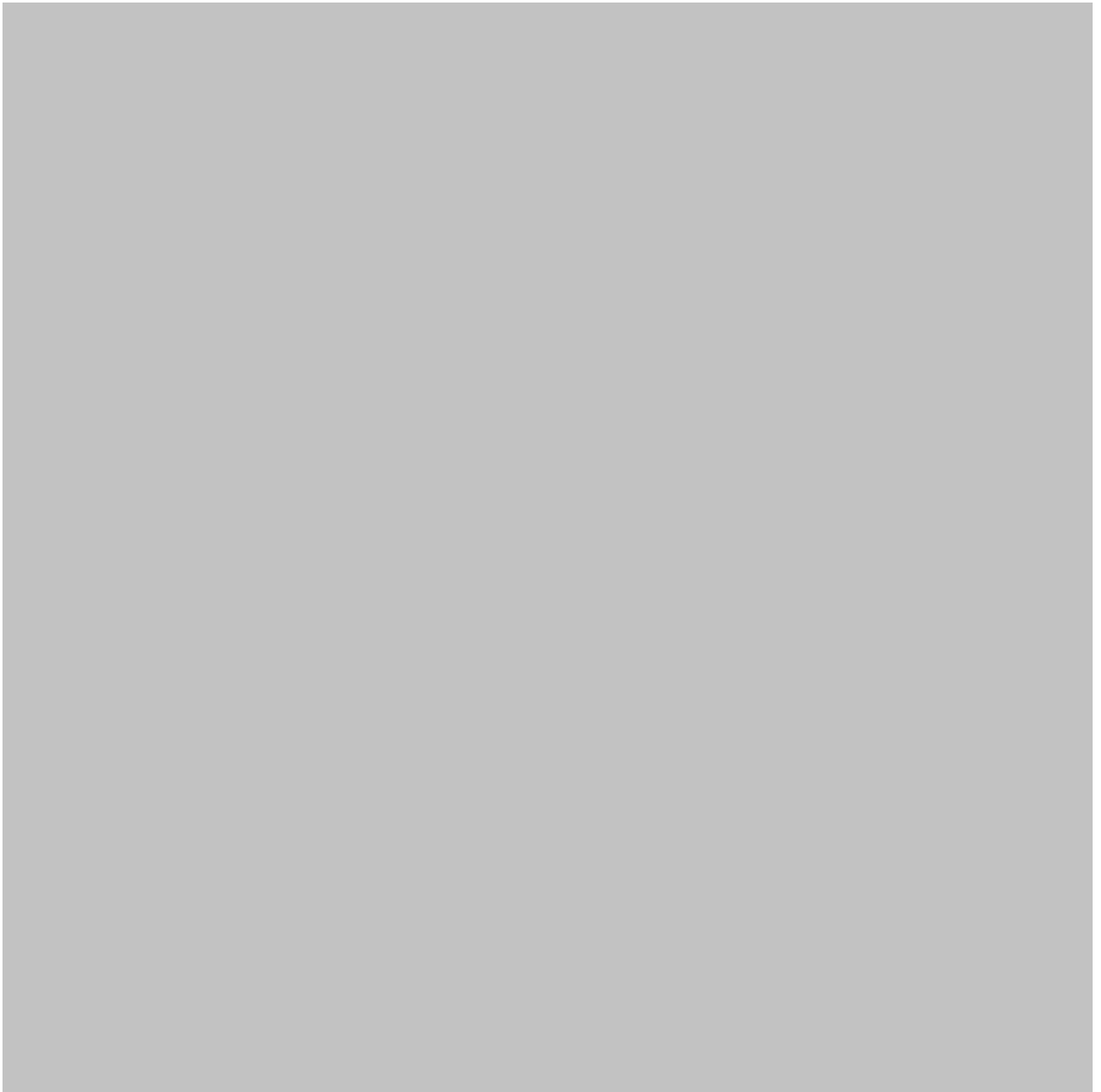


图24：读取config.dat文件

通过对GetCommandLineW函数进行inline hook，检测浏览器参数中是否包含电商类网站（如淘宝、京东、苏宁、国美）进行电商和导航的劫持。



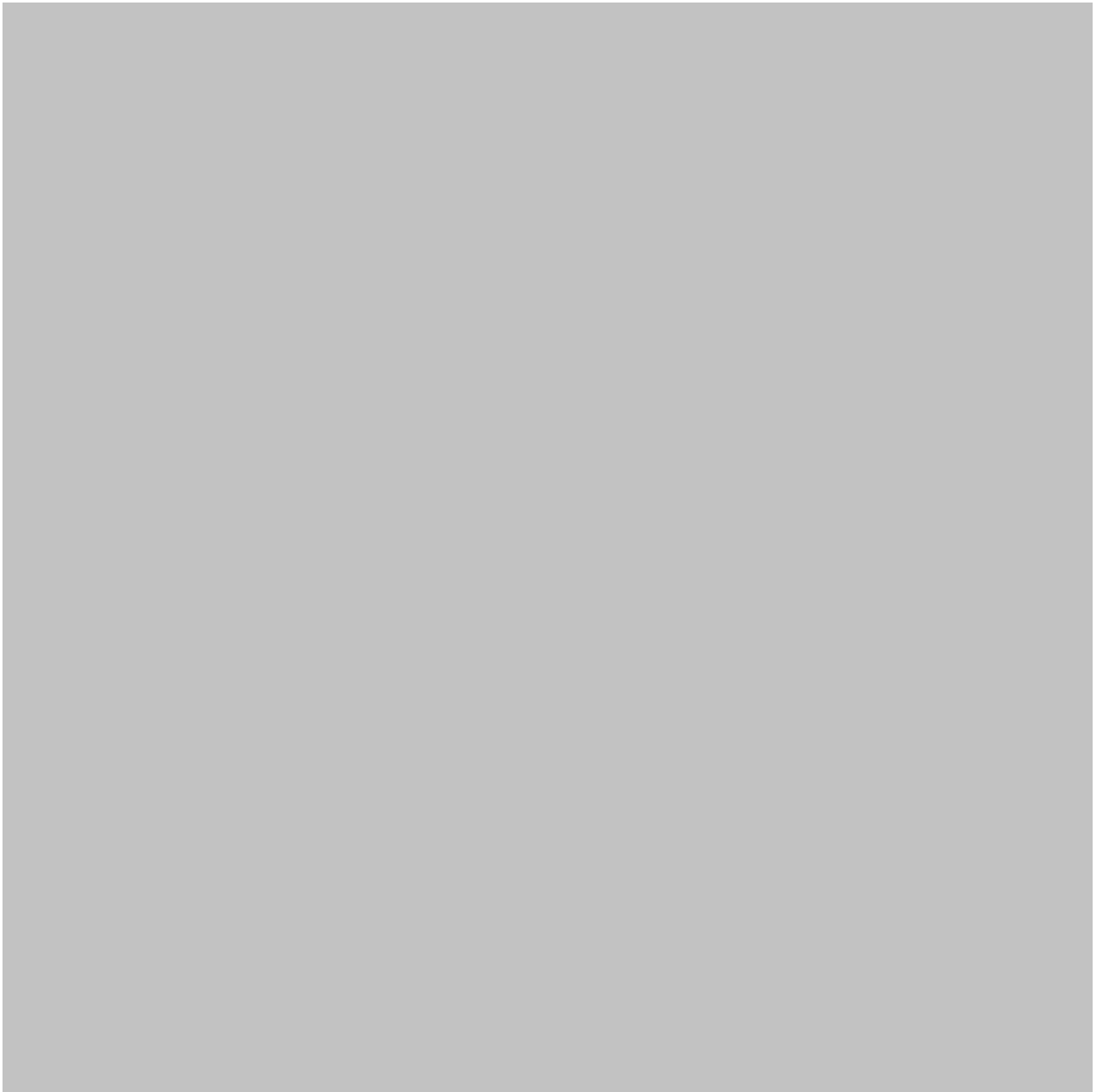


图25：HOOK GetCommandLineW函数：



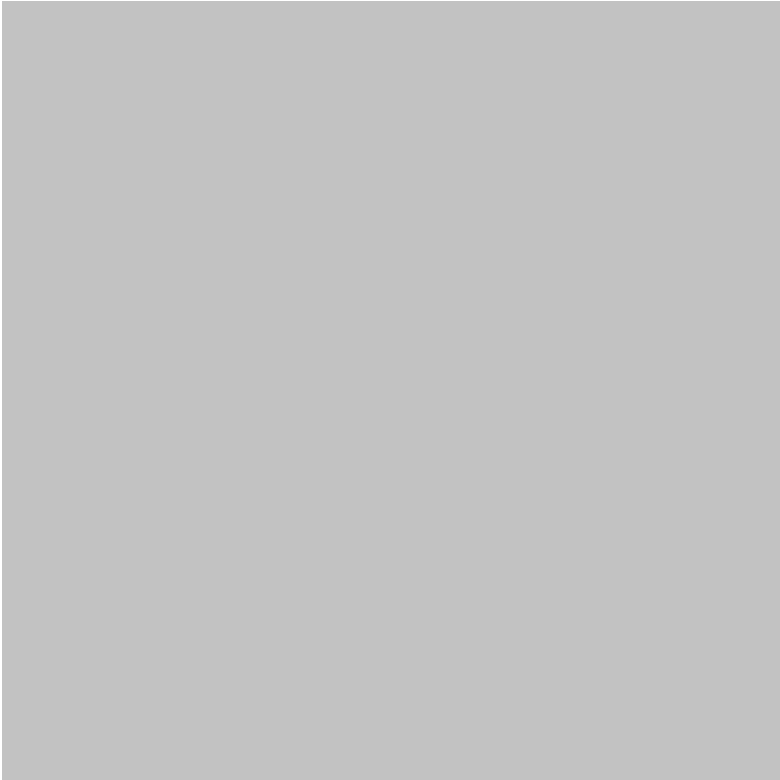


图26: 淘宝客劫持

5.驱动分析

蜗牛锁页的驱动主要起到保护注册表、对抗安全厂商主页锁定模块、淘宝客劫持、主页劫持、关机修复等功能。

5.1控制码对应功能:

木马的驱动控制码功能对应如下:

控制码	功能说明
0×222000	未实现功能
0×222004	未实现功能
0×222018	接收R3传递过来的淘宝客劫持pid
0×222024	清楚FSD Hook
0×222028	删除文件
0x22202C	未实现功能
0×222048	恢复注册表

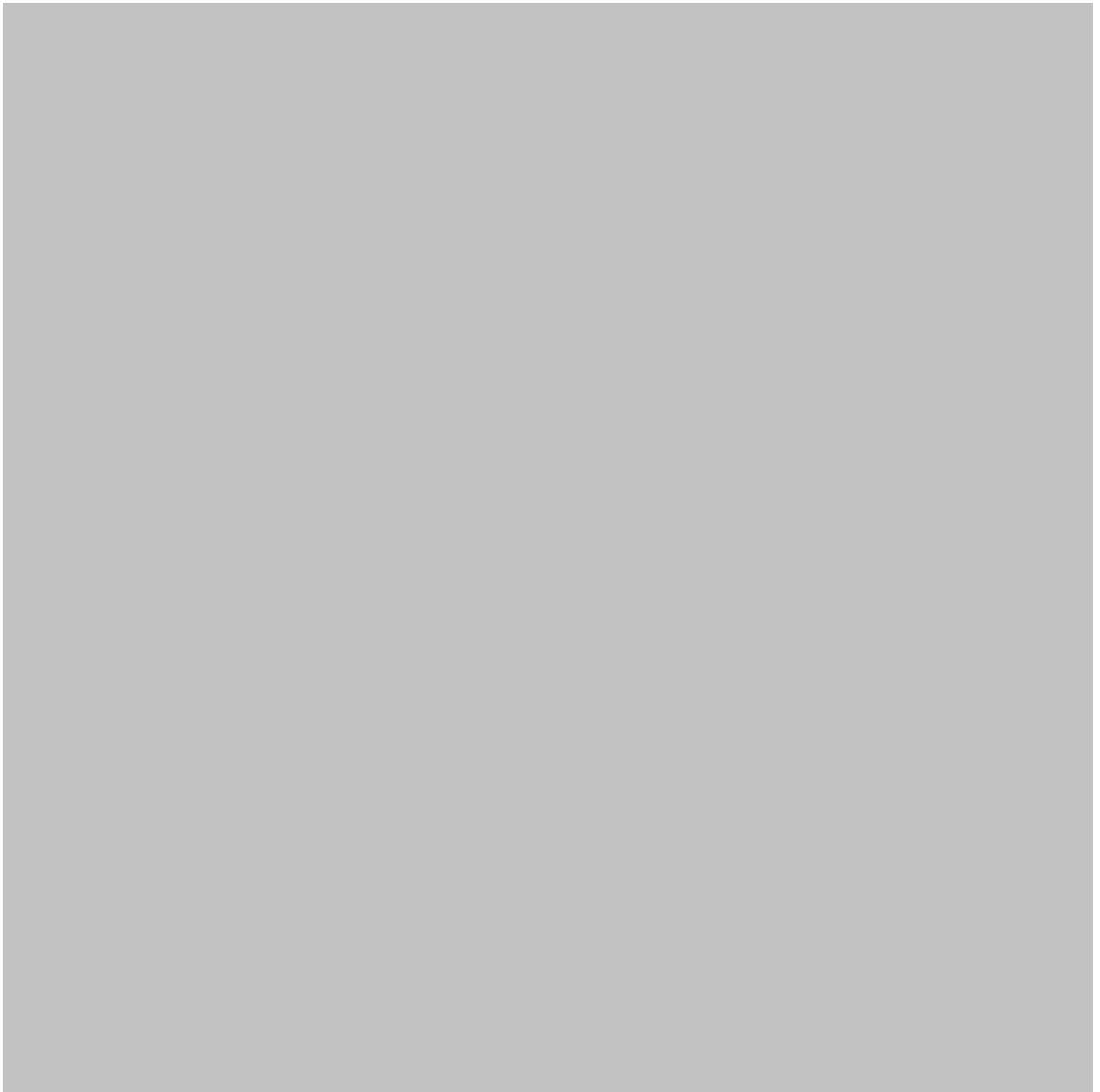


图27：控制码

5.2 镜像回调：

镜像回调函数是蜗牛锁页木马的浏览器劫持和淘宝客劫持功能核心点，其逻辑如下：

1. 如果msvcrt.dll被加载时且当前的进程是浏览器进程会通过命令行参数的方式进行导航劫持，如果浏览器命令行参中包含电商域名关键词就将命令行参数替换如下。

https://ai.taobao.com/?pid=mm_34440408_12080698_110948961

<http://www.woniulock.com/tuguan.php?name=jd>

<http://www.woniulock.com/tuguan.php?name=jd>



<http://www.woniulock.com/tuguan.php?name=sn>

2.当ntdll.dll被载时将safe32.dll(C:\\ProgramFiles\\Common
Files\\System\\ado\\hehe.dat) 注入到浏览器中

3.当explorer就加载时，进行safemonn32.dll的恢复

流程图如下：

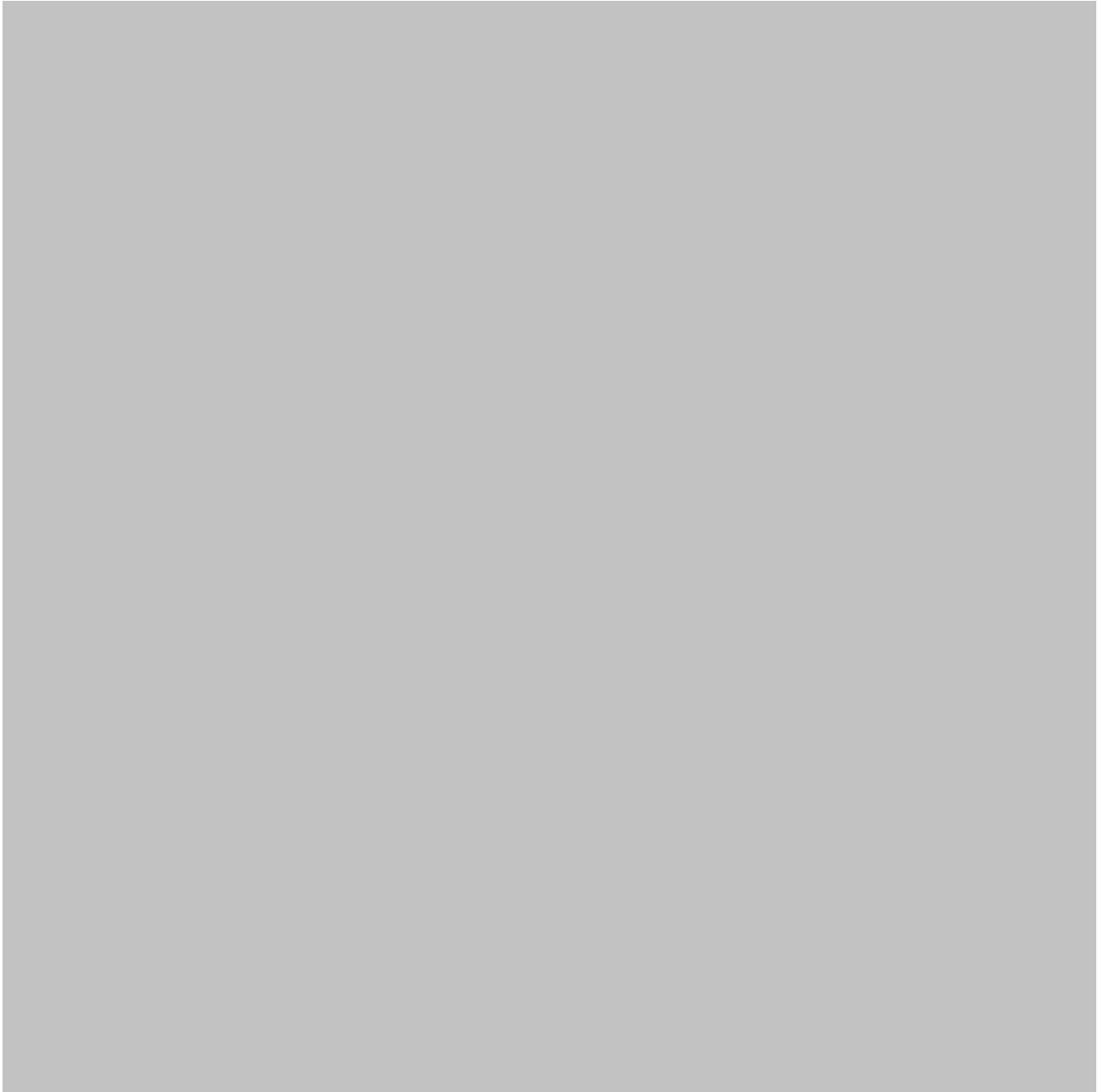


图28：流程图

5.3对抗安全厂商：

1.注册mini File filter对安全软件厂商的浏览器保护模块进行文件读取过滤，防止安全厂商浏览器保护模块被加载。



图29：安全厂商浏览器防护模块

2.重新加载内核获取原始SSDT表中函数地址，然后通过KeServiceDescriptorTable[0]获取到现有的SSDT表，然后循环判断ZwOpenKeyEx、ZwCreateKey、ZwSetKeyValue函数是否被HOOK，如果被HOOK，则进行恢复

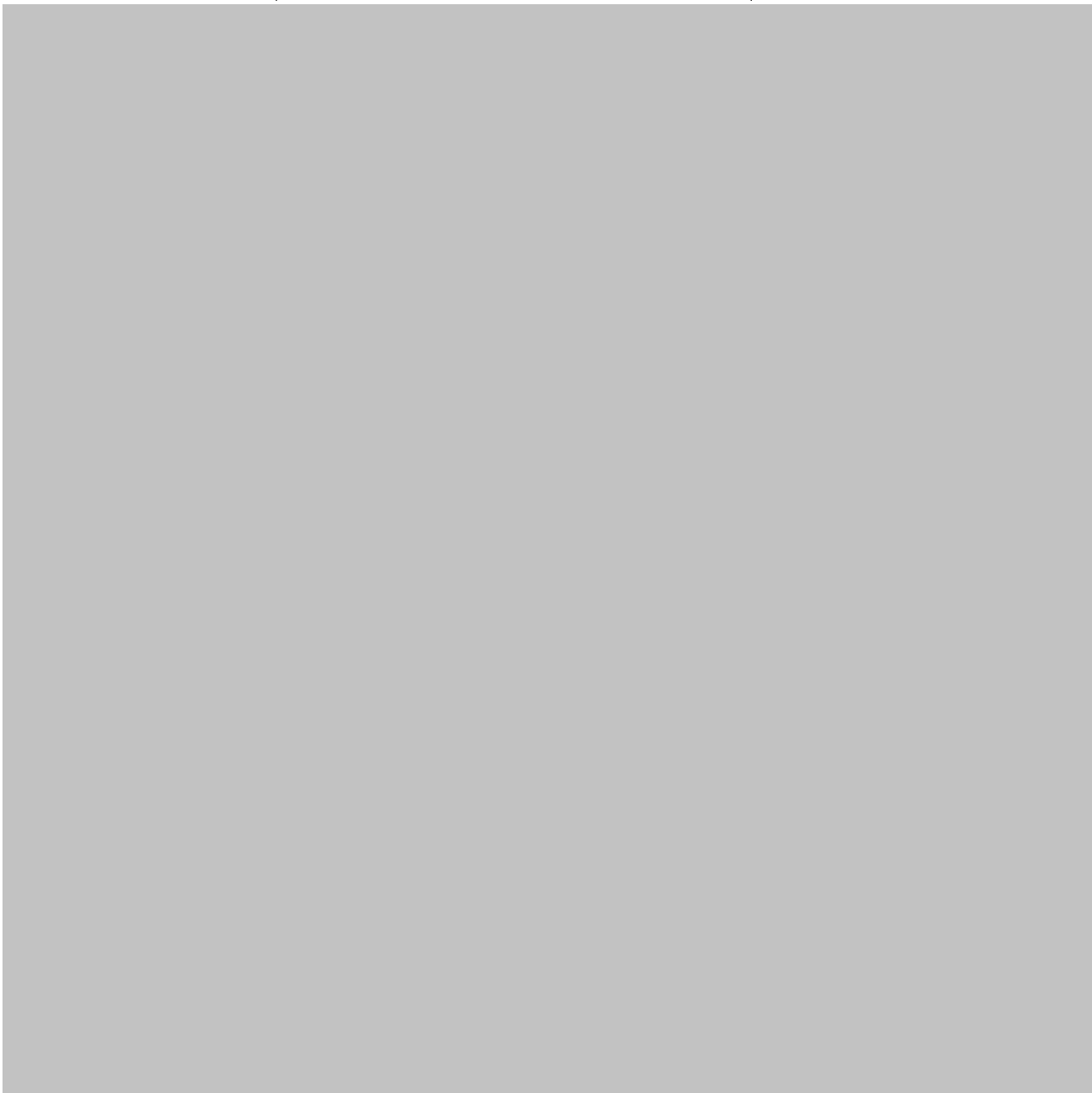


图30：摘除ZwOpenKeyEx、ZwCreateKey、ZwSetKeyValue钩子

3.通过暴力搜索特征0x2B、0xE1、0xC1、0xE9、0x2得到现有的kifastCallEntry，通过内核加载获取到原始的kifastCallEntry进行恢复。



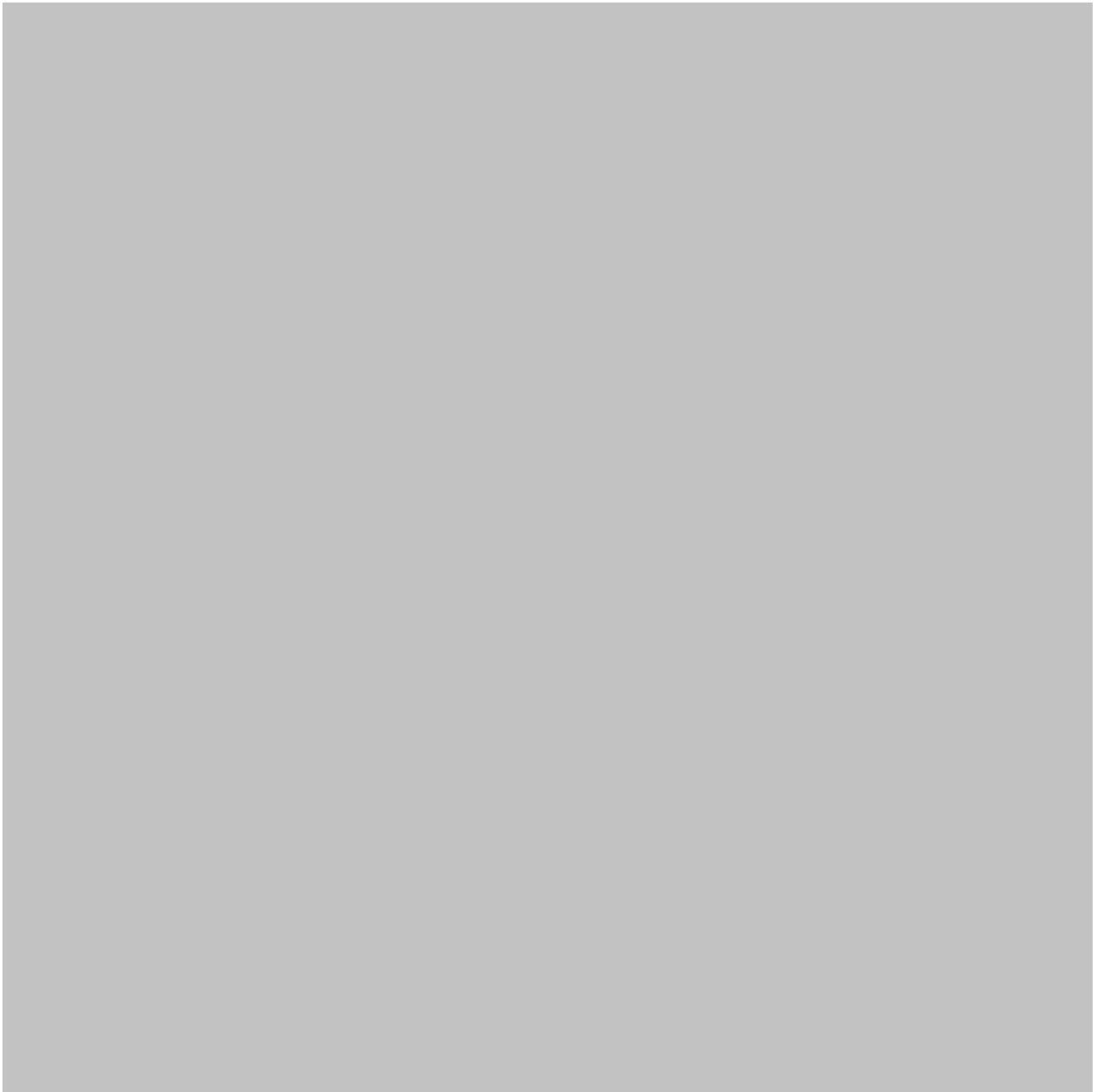


图31:恢复kifastCallEntry钩子

4. 枚举移除 LoadImageNotifyRoutine，让安全厂商镜像加载监控失效

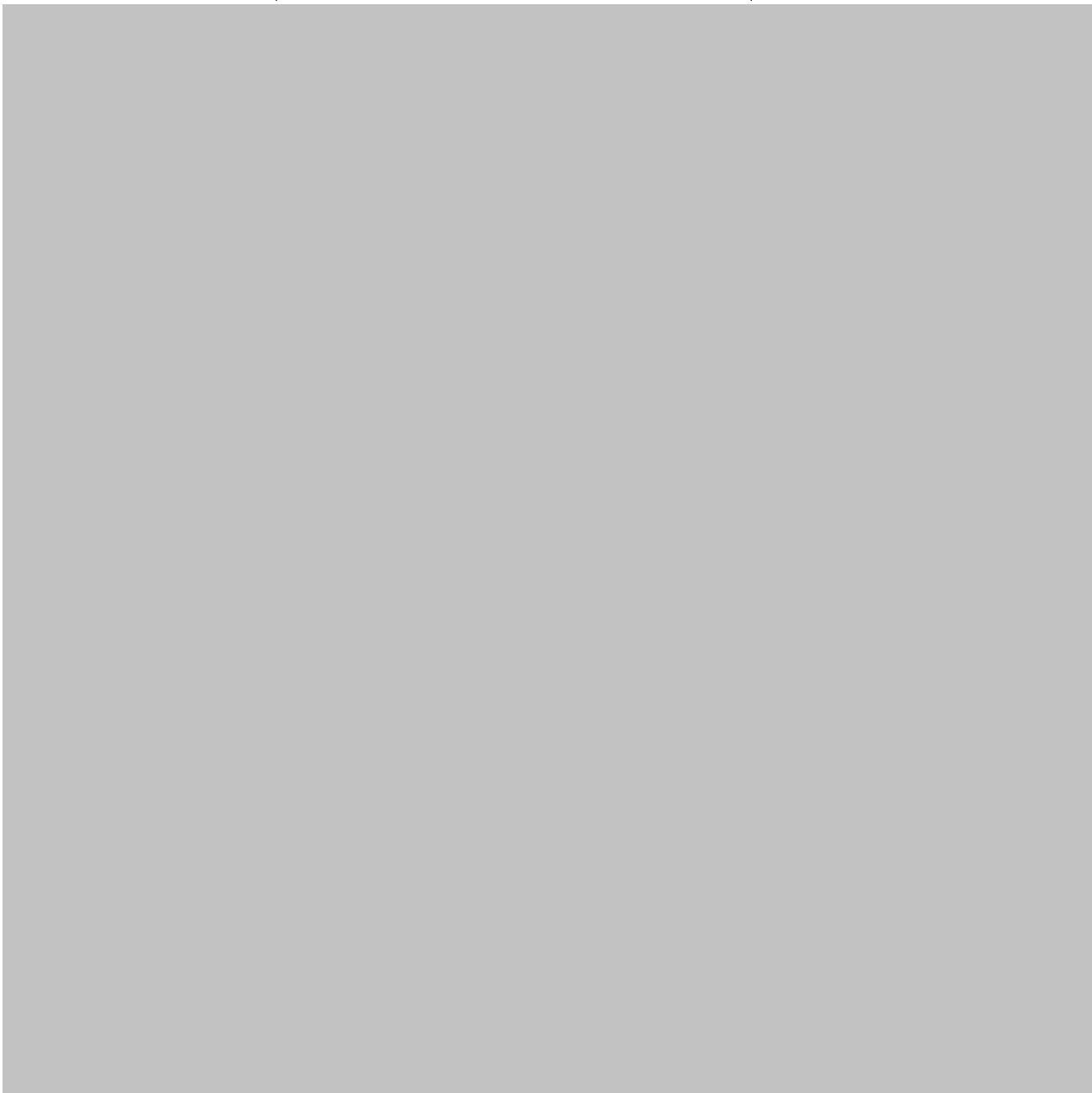


图32: 枚举移除LoadImageNotifyRoutine

5.4注册表回调：

创建注册表回，对注册表

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\00Ove:
Icon进保护防止打开访问



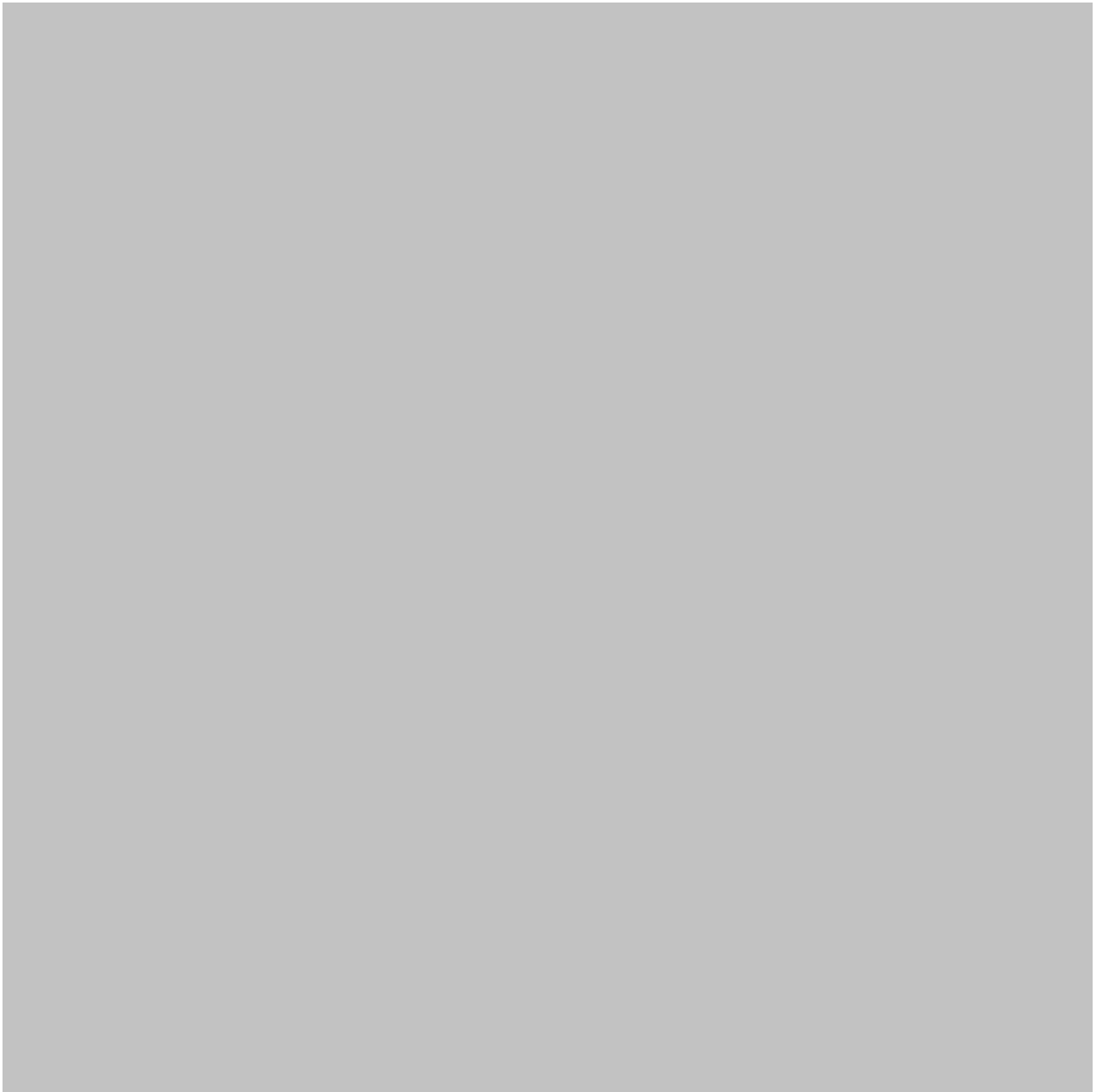


图33：注册表回调

5.5关机回调：

关机回调函数，进行safemonn32.dll模块的恢复。

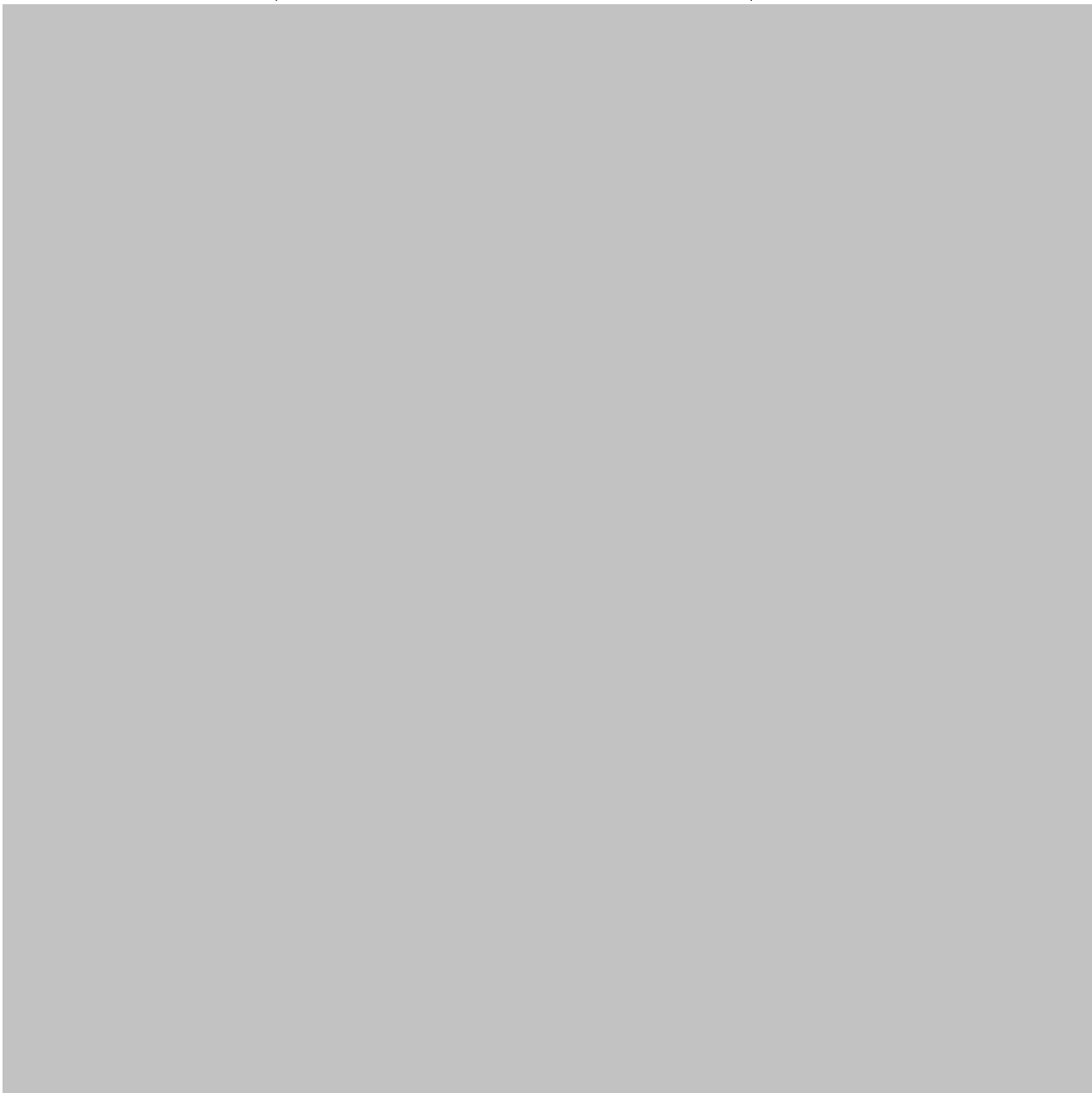


图34：关机回调

三、安全建议

金山毒霸安全专家建议推广技术人员特别警惕这种主页生成器，切勿帮助他人进行病毒的传播。

*本文作者：渔村安全，转载请注明来自FreeBuf.COM

上一篇：[简要指南 | 处理器Meltdown & Spectre漏洞修复](#)

下一篇：[2017全球僵尸网络DDOS攻击威胁态势报告](#)

老周2018-01-12

1楼回

写的不错,赞

亮了

小傅2018-01-12

2楼回

活捉老周

亮了

幕刃2018-01-12

3楼回

感觉不止一只蜗牛

亮了

神刀安全网2018-01-12

4楼回

很地道

亮了

金山毒霸👁2018-01-12

5楼回

转发微博

亮了

选择文件

未选择任何文件

昵称

请输入昵称

必须 您当前尚未登录。[登陆?](#) [注册](#)

邮箱

请输入邮箱地址

必须 (保密)

表情 插图

提交评论(Ctrl+Enter)

[取消](#)

☒ 有人回复时邮件通知我



渔村安全

珠海猎豹团队官方账号

24
文章数

3
评论数

最近文章

- [病毒分析 | 一只“蜗牛”偷梁换柱，靠锁主页进行牟利](#) 2018.01.12
- [病毒分析 | 一只“蜗牛”偷梁换柱，靠锁主页进行牟利](#) 2018.01.08
- [年终盘点 | 2017年网络安全大事回顾](#) 2017.12.25

浏览更多

相关阅读

- [安全科普：详解流量劫持的形成原因](#)
- [国外安全研究员：中国ISP将用户的合...](#)
- [黑客修改WordPress核心文件，劫持网...](#)
- [针对某电商网站流量劫持案例分析与...](#)
- [病毒分析 | 一只“蜗牛”偷梁换柱，靠锁...](#)


特别推荐



极客DIY：手机文件直传U盘，三步教你做一根OTG传输线 <small>关注我们 分享每日精选文章</small>	独家分析：安卓“Janus”漏洞的产生原理及利用过程
geekman 2014-12-27	顶象技术 2017-12-12
量子计算从概念走入现实，公钥加密是否岌岌可危	快讯：联想官网被黑，内部邮件被劫持
Elaine_z 2017-07-18	hujias 2015-02-26



Copyright © 2018 WWW.FREEBUF.COM All Rights Reserved [沪ICP备13033796号](#)

 阿里云 提供计算与安全服务