蓝宝菇（APT-C-12）针对性攻击技术细节揭秘

奇安信威胁情报中心 2018-07-17 共261347人围观，发现 5 个不明物体 终端安全

背景

360公司在2018年7月5日首次对外公开了一个从2011年开始持续近8年针对我国政府、军工、科研、金融等重点单位和部门进行网络间谍活动的高级攻击组织-蓝宝菇（APT-C-12），该组织的活动在近几个月内呈现非常活跃的状态。本文作为前期组织揭露报告的补充，详述蓝宝菇组织在近期攻击活动的技术细节，希望安全企业界了解其攻击手法共同完善拼图，输出防御方案联合起来对抗这个国家级的威胁。

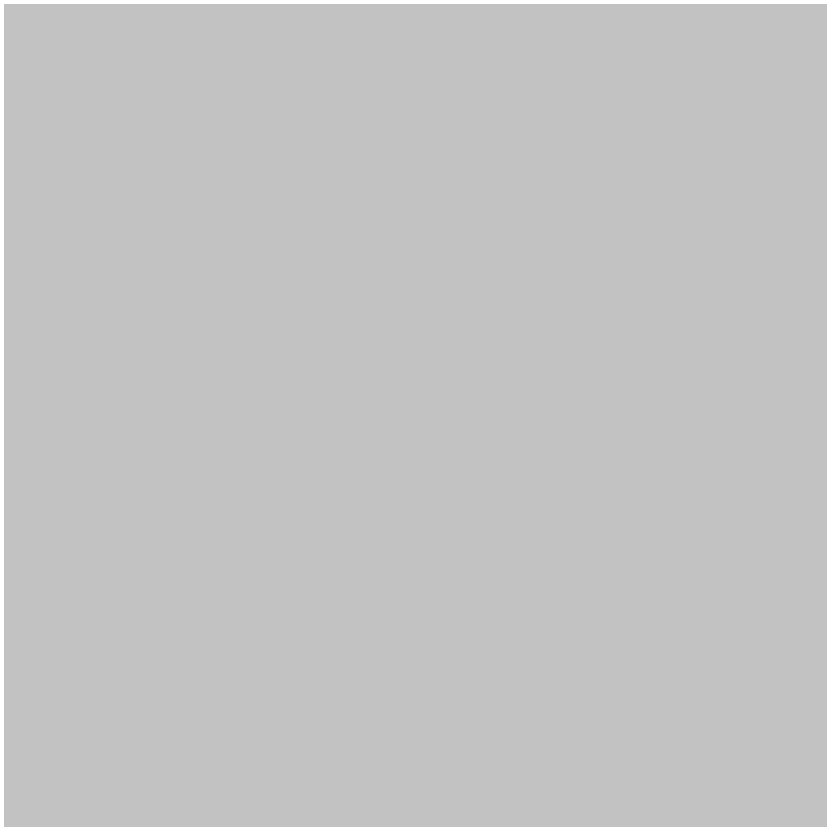
鱼叉邮件

2018年4月以来，360安全监测与响应中心和360威胁情报中心在企业机构的协同下发现了一批针对性的鱼叉攻击，攻击者通过诱导攻击对象打开鱼叉邮件云附件中的LNK文件来执行恶意PowerShell脚本收集上传用户电脑中的敏感文件，并安装持久化后门程序长期监控用户计算机。该攻击过程涉及一些新颖的LNK利用方式，使用了AWS S3协议和云服务器通信来偷取用户的敏感资料，在此我们分析并公开整个攻击过程。

360威胁情报中心确认多个政企机构的外部通信邮箱被投递了一份发自boaostaff[@]163.com的鱼叉邮件，钓鱼邮件仿冒博鳌亚洲论坛向攻击对象发送了一封邀请函：

邮件附件被放到163的云附件里，此附件即为攻击者的恶意Payload，这是一个通过RAR打包的快捷方式样本。接下来我们对同一波攻击中的另一个完全相同功能的样本进行详细分析，以梳理整个攻击过程。

附件内容如下：



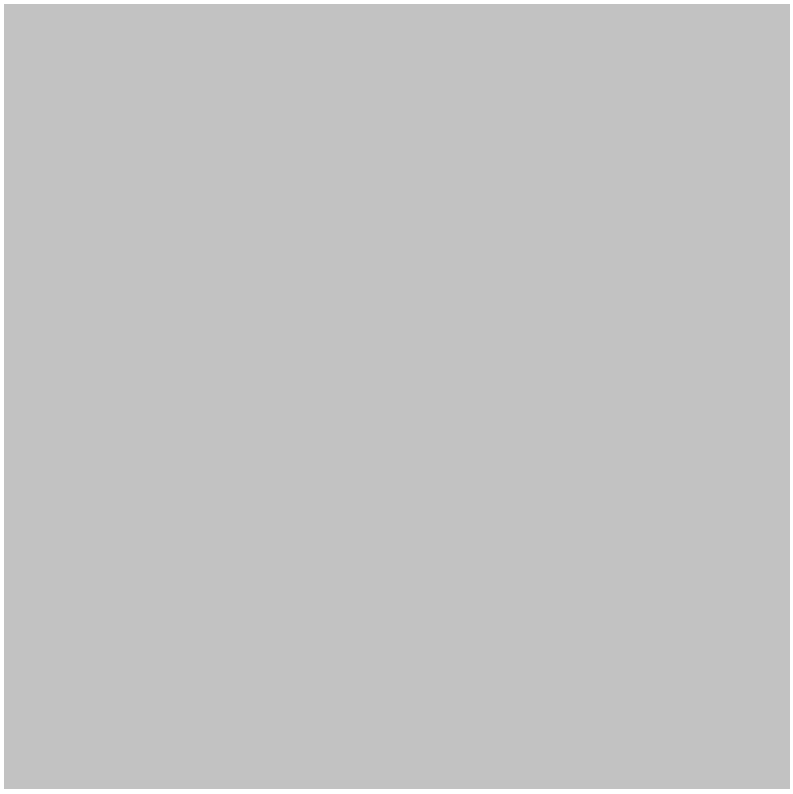
一旦攻击对象被诱导打开该LNK快捷方式文件，LNK文件便会通过执行文件中附带的PowerShell恶意脚本来收集上传用户电脑中的敏
文件，并安装持久化后门程序长期监控用户计算机。

样本分析

Dropper

附件压缩包内包含一个LNK文件，名字为：《政法网络舆情》会员申请.lnk，查看LNK文件对应的目标如下：

可以看到目标中并没有任何可见字符，使用二进制分析工具查看LNK文件可以看到PowerShell相关的字符串，以及很多Unicode不可
字符：

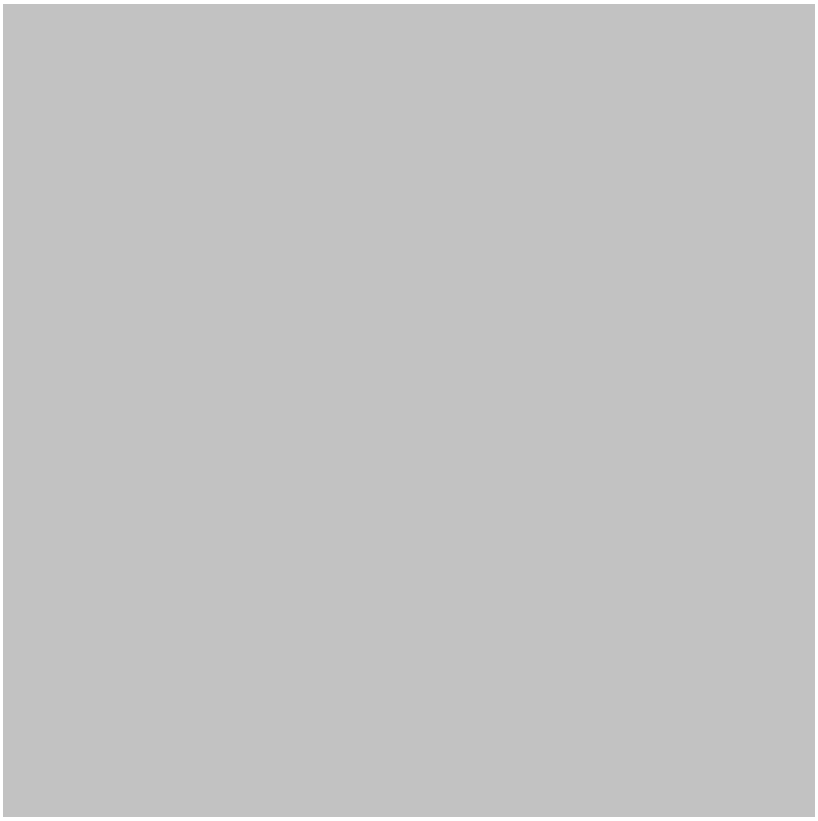


通过分析LNK文件格式中几个比较重要的结构，完整还原出样本真实执行的恶意目标，其中涉及3个LNK文件格式的重要结构：LinkTargetIDList、COMMAND_LINE_ARGUMENTS和EnvironmentVarableDataBlock。

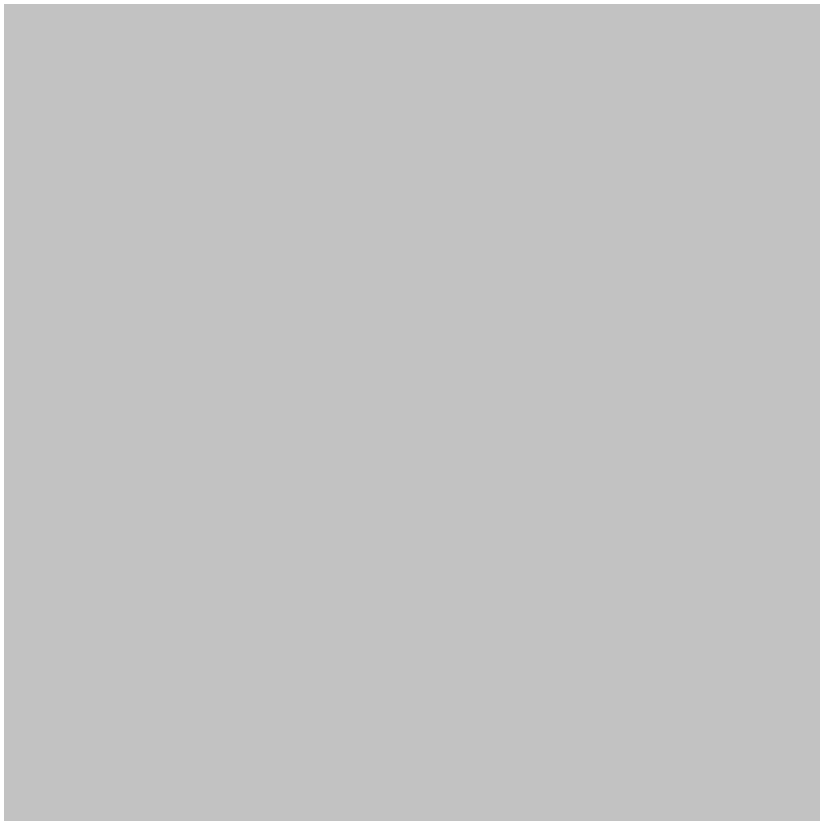
l LinkTargetIDList，该结构是一个数组，用于标记具体的快捷方式的链接目标，而样本中多个LIST里的元素拼接起来才是快捷方式的体链接目标：

CLSID_MyComputer\C:\Windows\system32\windOW~1\V1.0\POwersHELl.exe

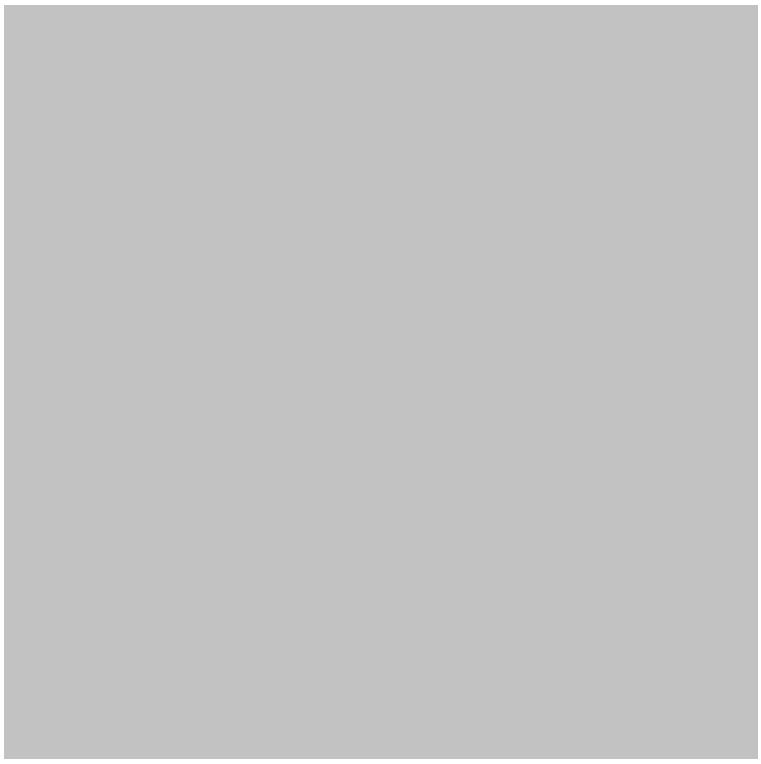
通过调试可以看到目标路径和LinkTargetIDList拼接出来的结果一致：



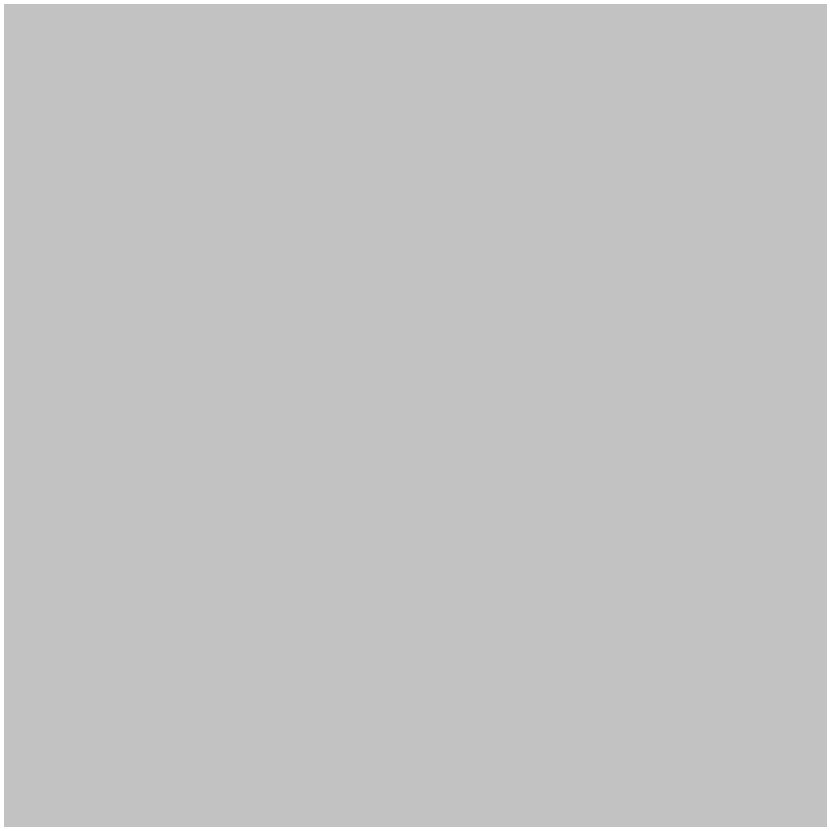
l COMMAND_LINE_ARGUMENTS，该选项为目标程序的参数



样本中的目标程序参数则为具体需要执行的PowerShell恶意代码，另外由于在参数中包含了大量的不可显示Unicode字符，从而导致
键打开快捷方式时目标中并不会包含对应的PowerShell代码：



l EnvironmentVarableDataBlock，当链接目标程序涉及到环境变量时会使用



该值设置后会导致具体的快捷方式中的目标被设置为对应的EnvironmentVarableDataBlock值，但是需要注意的是，样本中EnvironmentVarableDataBlock对实际的程序调用并不起作用（删除并不影响最终的样本启动），最终Shell32.dll靠解析LInkTargetIDList数组来启动PowerShell。

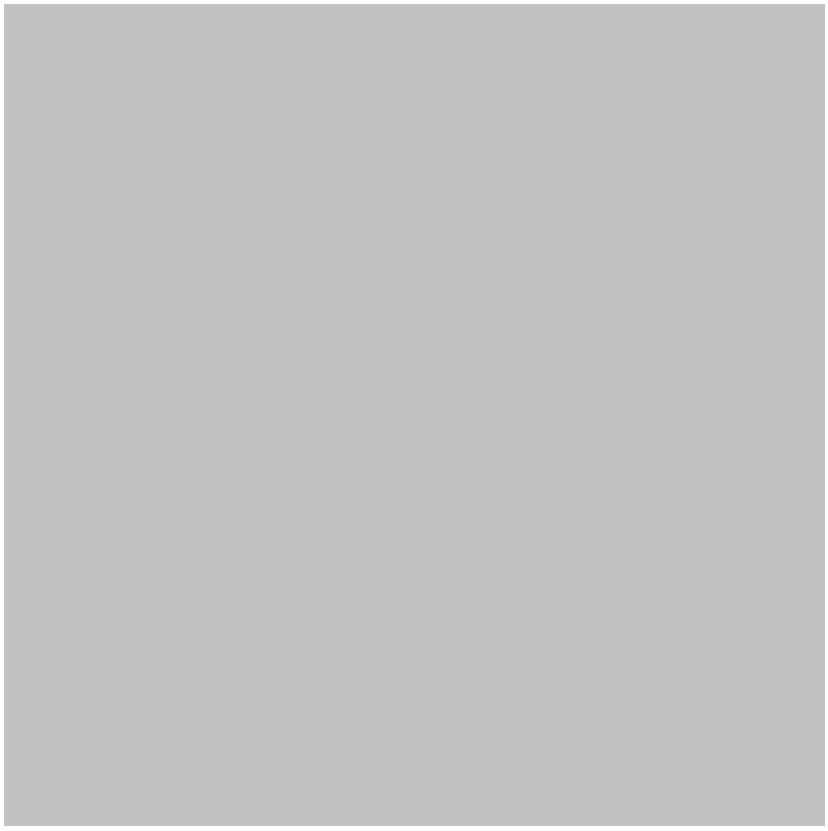
Payload（PowerShell脚本）

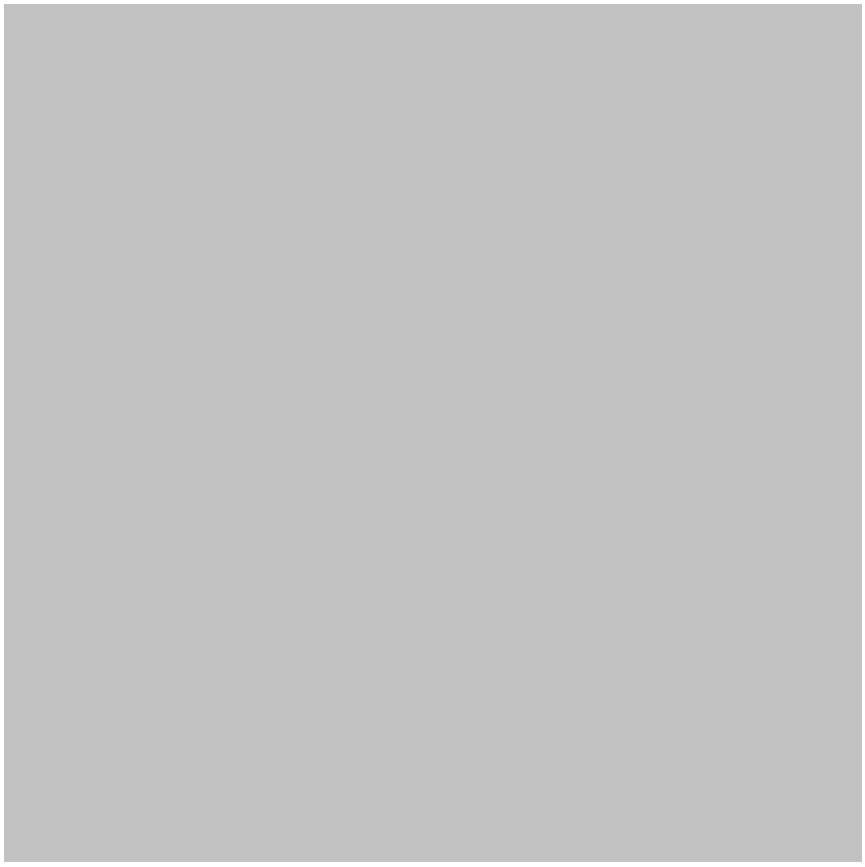
解密PowerShell脚本

将LNK文件指向执行的PowerShell脚本解密，该PowerShell命名为ps_origin，代码如下：

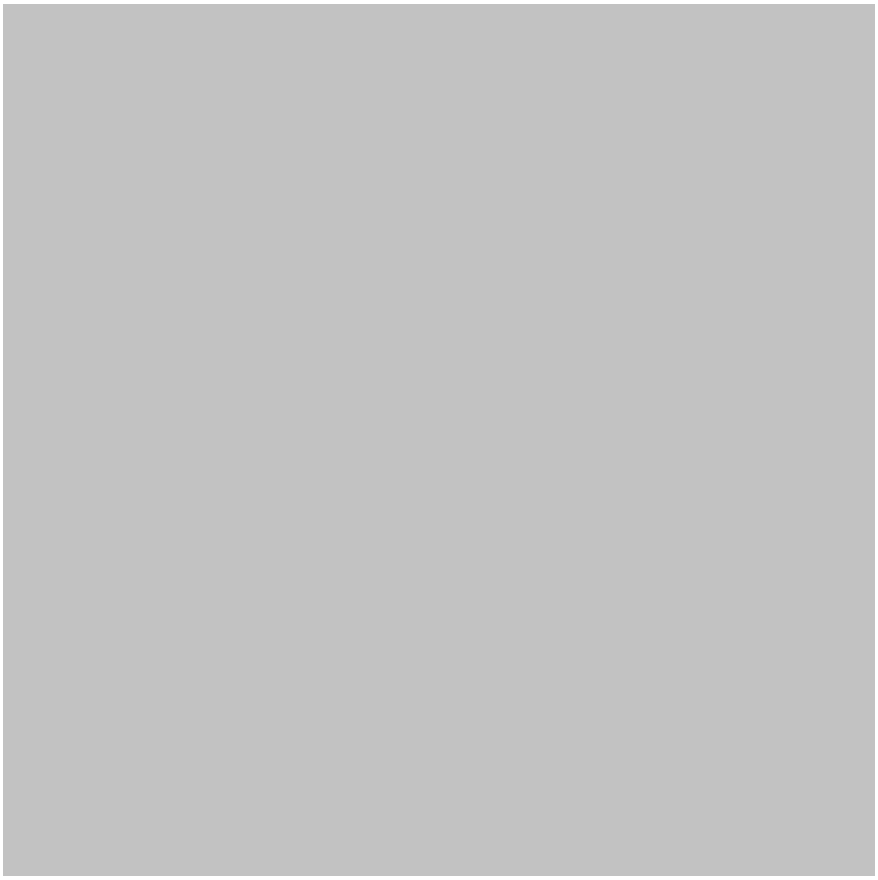
PowerShell脚本会定位执行LNK文件的最后一行，文件的最后一行如下：

文件最后一行经过Base64编码，解码后的数据为[压缩包+PowerShell脚本]的形式：



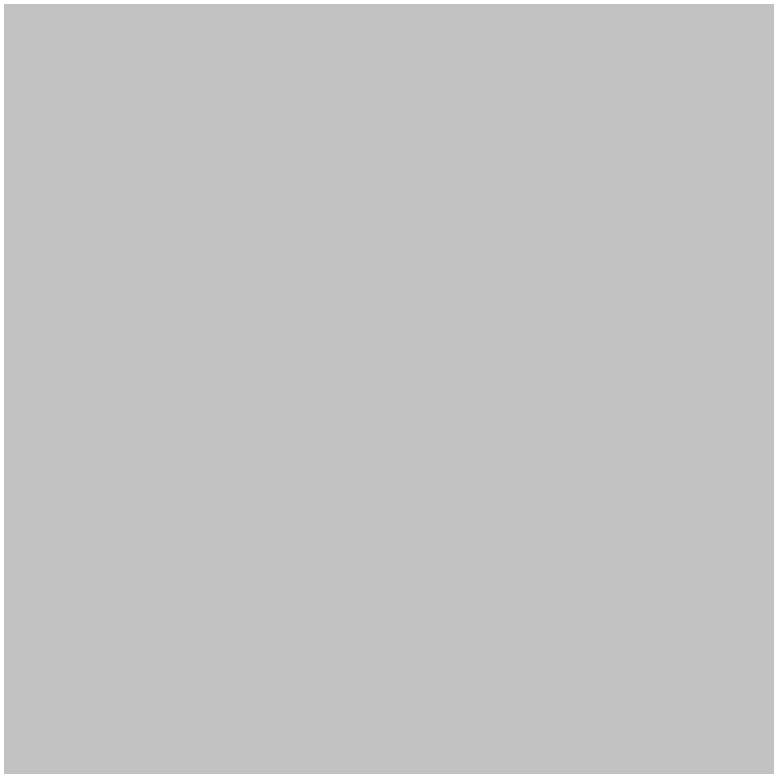


将最后的PowerShell脚本解密后如下（名称为ps_start）：

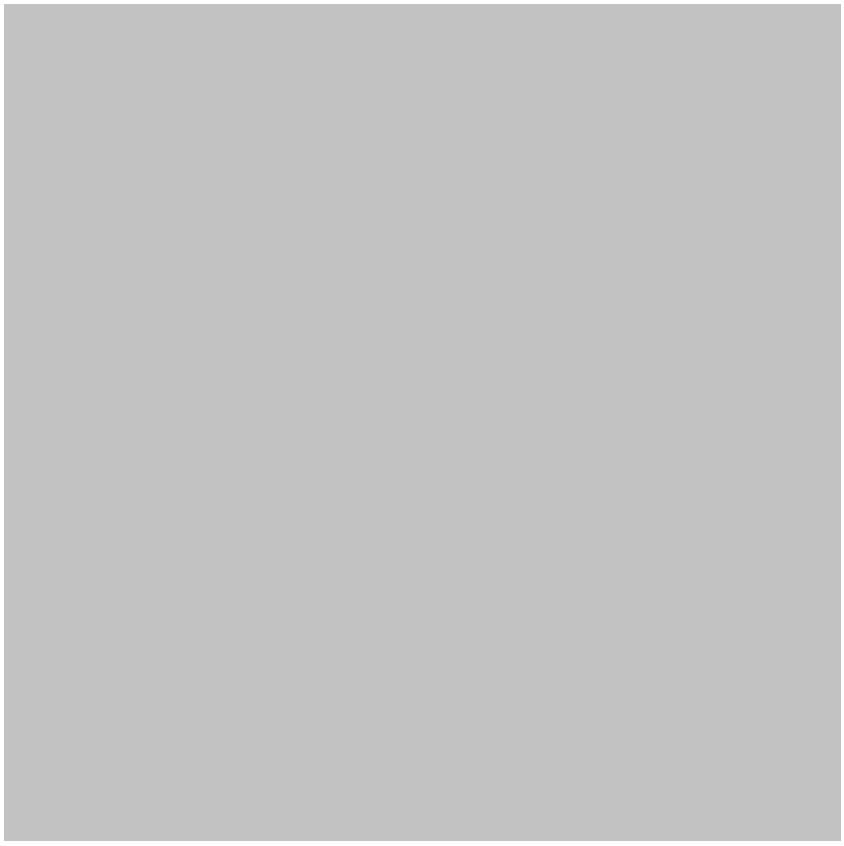


ps_start

被解密后的LNK文件最后一行中的PowerShell脚本中的ps_start会被首先执行，该PowerShell脚本主要用于解压出后续的压缩包，并续运行其中的脚本，同时压缩包包含了相应的文件窃取模块，如下图所示脚本通过[convert]::frombase64string((gc $a|select -l 2|select -f 1)));以Base64解密出对应的压缩包文件，之后使用Rundll32加载其中beoql.g后门文件（加载函数为DllRegister），同时一段PowerShell脚本作为参数传入，该PowerShell命名为ps_loader：



压缩包解压后包含名为beoql.g的DLL后门、合法的Rar.exe压缩工具、以及真实呈现给用户的诱惑性DOC文档：

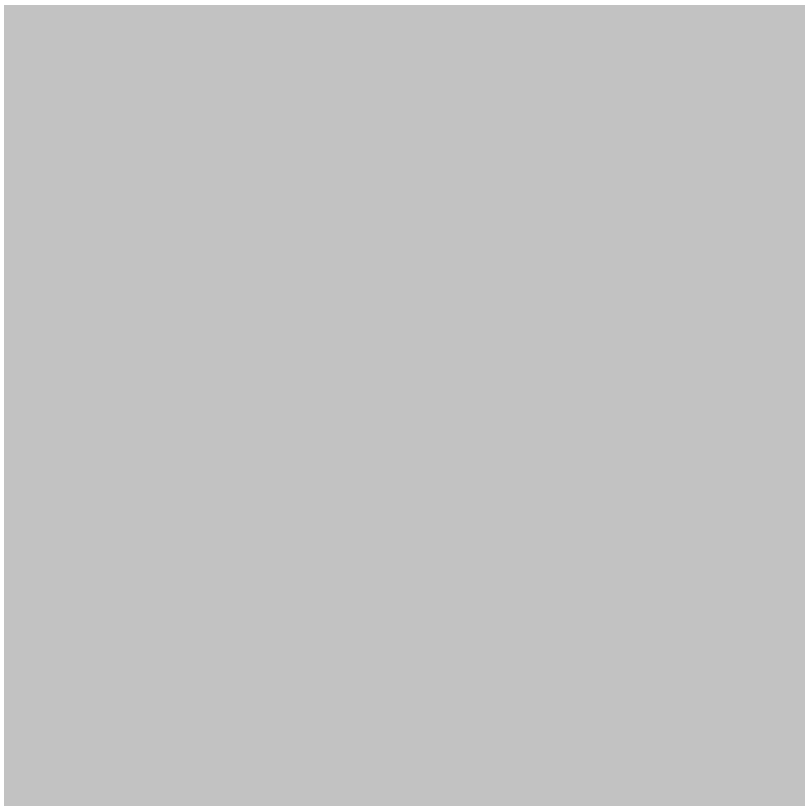


脚本会尝试访问以下3个IP地址，以确保C&C存活：

159.65.127.93

139.59.238.1

138.197.142.236



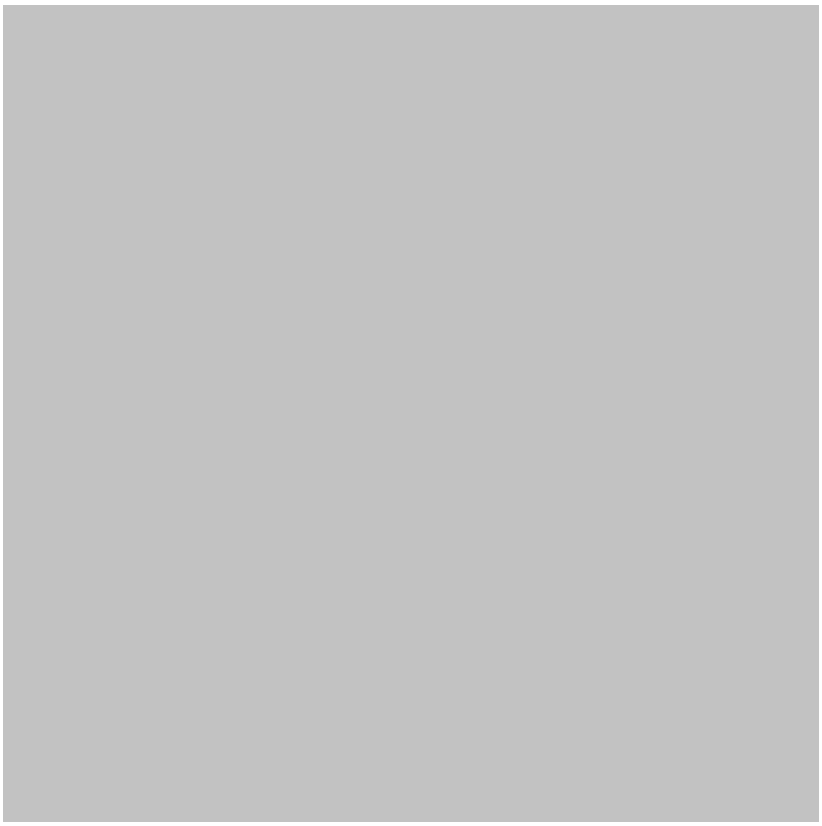
若确认C&C存活，则通过命令行收集系统的基本信息：

命令

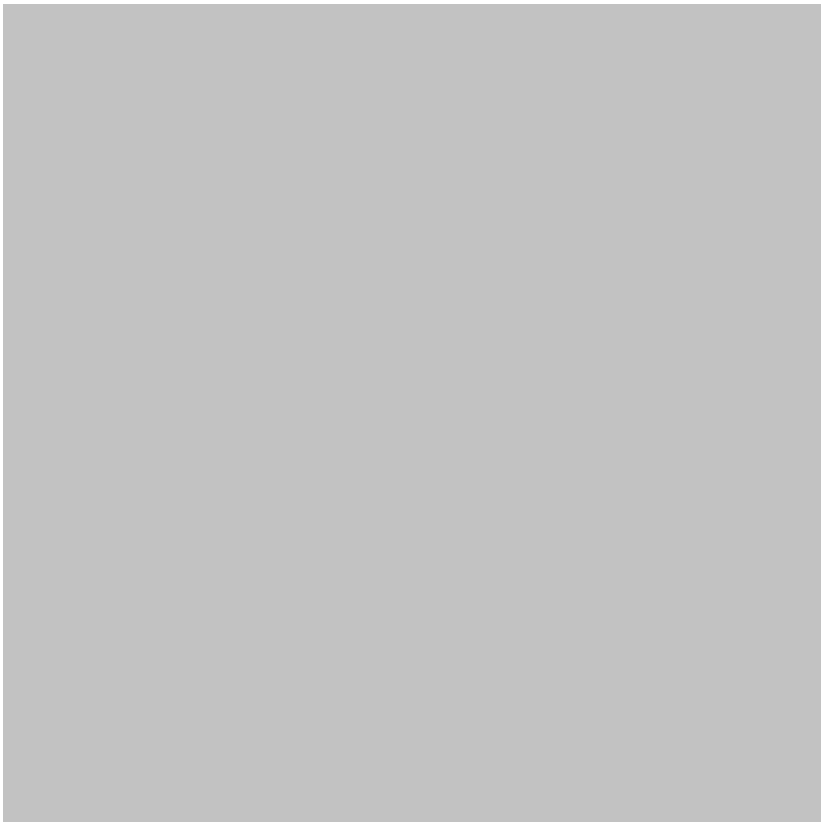
命令	描述
Ipconfig /all	IP地址信息
Netstat -a	相关网络连接信息
Arp -a	ARP table信息
Desktop files	桌面文件
programfiles	Programfiles文件
Programfiles x86	Programfiles文件

脚本获取基本信息后，再通过Rar.exe压缩为start.rar文件，之后使用RSA算法加密一个随机字符串e，秘钥如下：

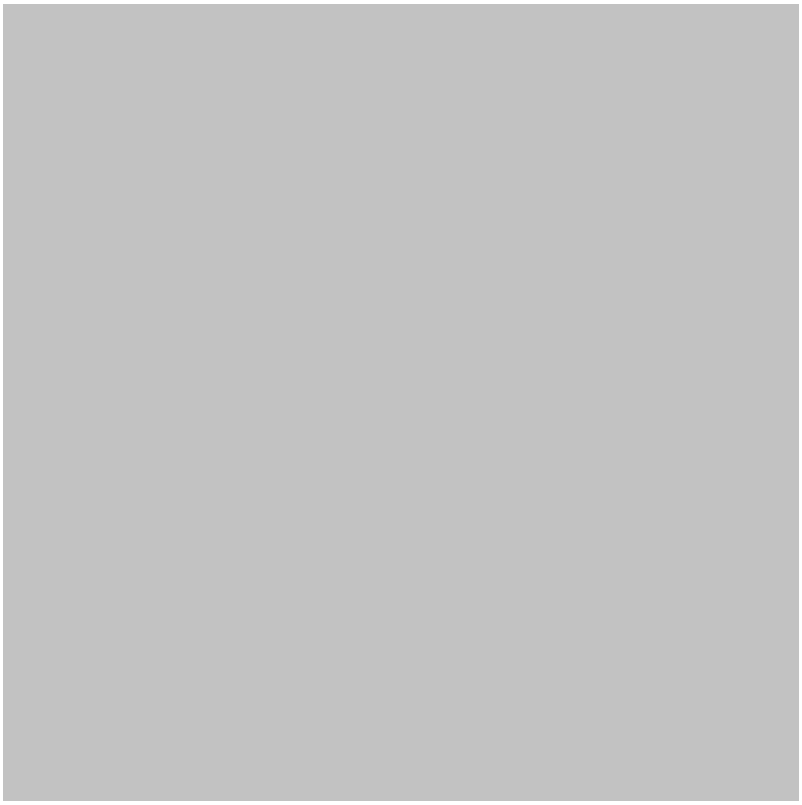
该随机字符串为之后上传文件的RAR加密密码，脚本会将该加密后的字符保存成id.rar文件，并通过函数pv9上传start.rar及id.rar文件
攻击者的云服务器中：



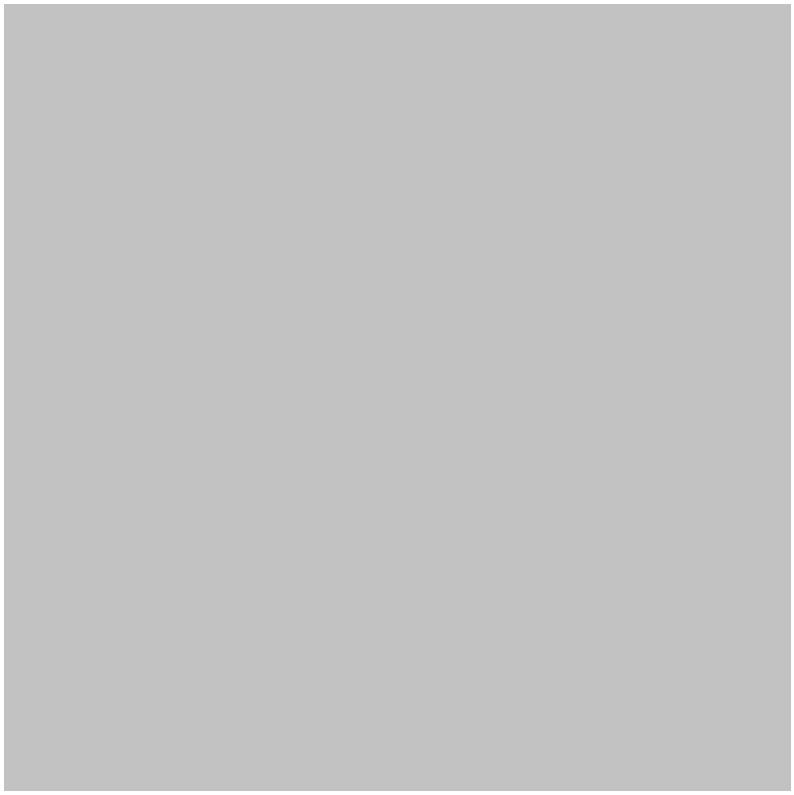
最后脚本会遍历系统中指定的后缀文件（jpg,txt,eml,doc,xls,ppt,pdf,wps,wpp,et，只获取180天以内的文件），继续使用Rar.exe压
获取的指定文件，密码为之前生成的变量e：



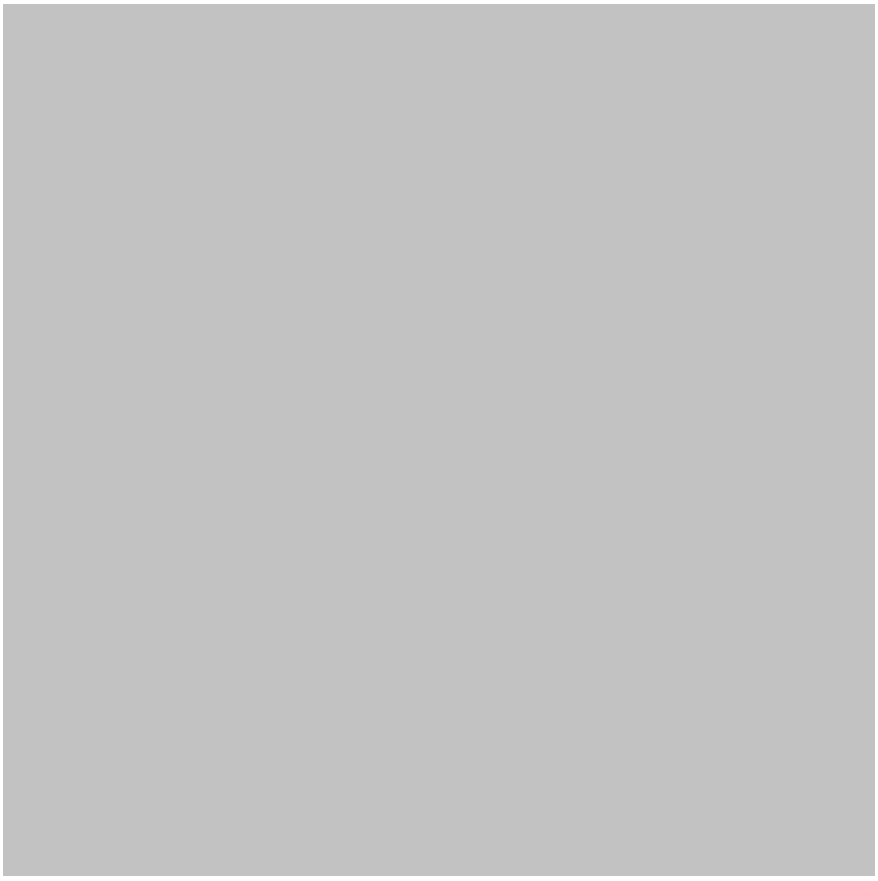
而函数pv9会将对应的RAR文件通过AWS S3 存储协议上传到一个网上的云服务商的地址：0123.nyc3.digitaloceanspaces.com，代
中包含的ACCESS_KEY和SECRET_KEY疑似亚马逊S3云服务存储协议所使用的相关KEY信息：



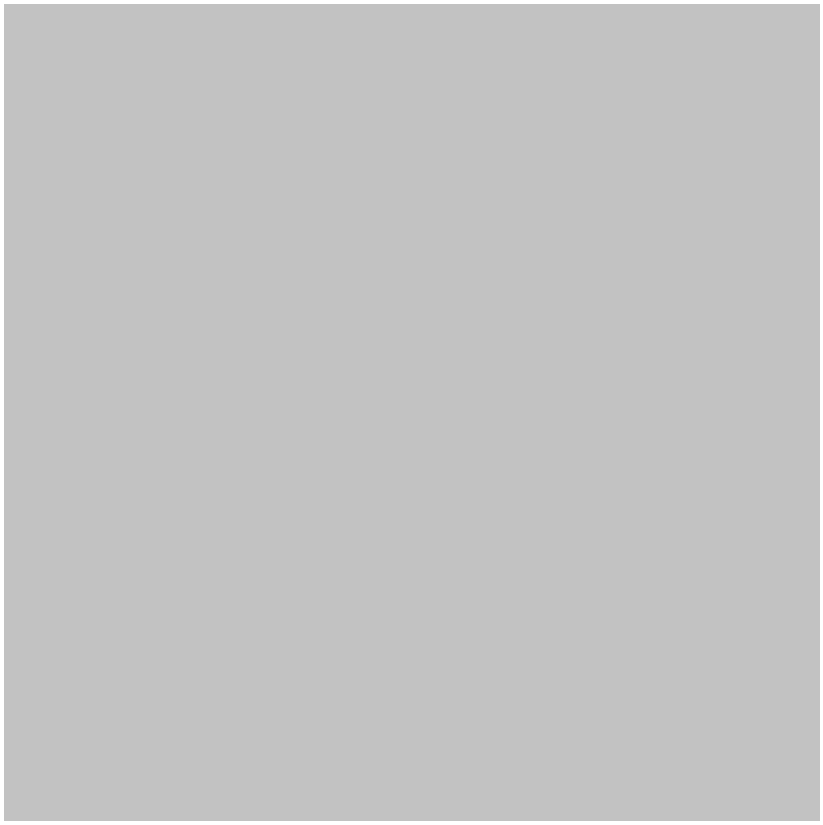
Amazon S3相关介绍：



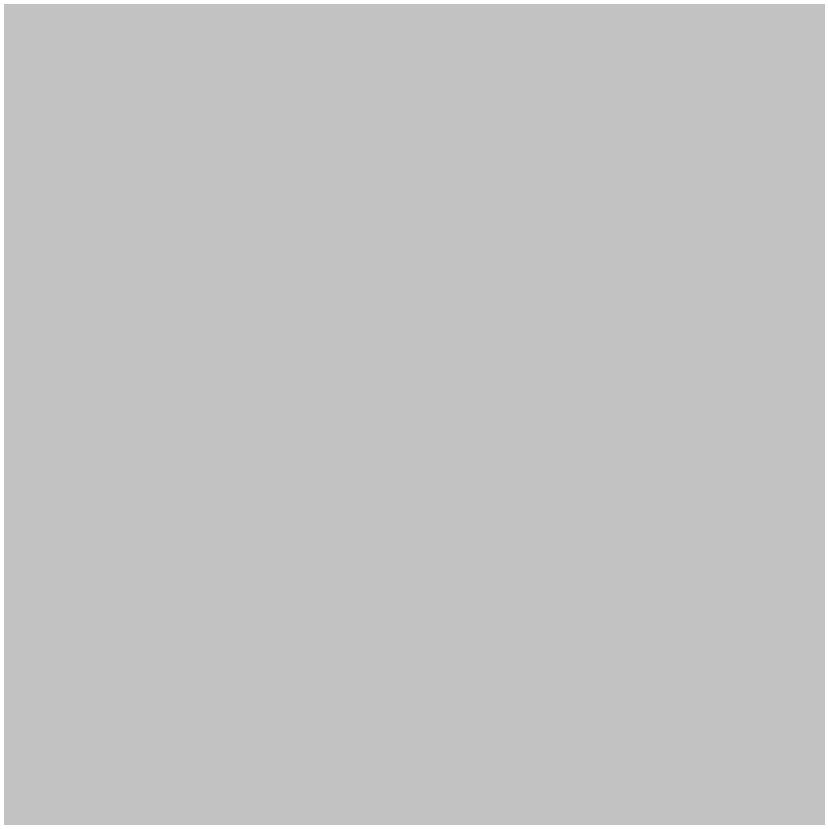
样本中使用该协议不过是添加一些跟服务端协商的请求头，请求头的value是用AWS s3 V4签名算法算出来的，一个标准的请求头如下示：



一次通信流程由上图代码红框中的函数ul3和ig3完成，其中ul3用于配置生成对应的请求头，ig3完成文件的上传。而ul3中用于封装请求，aws3对应的请求头如下图为其中的，其中一个重要的参数为，由函数，共同生成，之后9会封装到中，g作为最终的请求头返回：

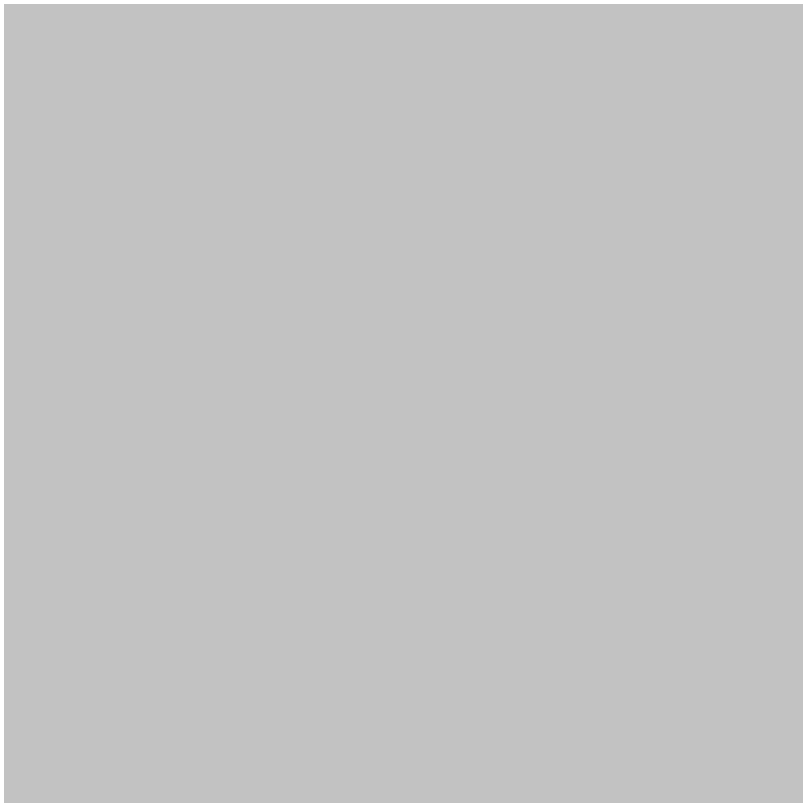


最终完成上传文件：

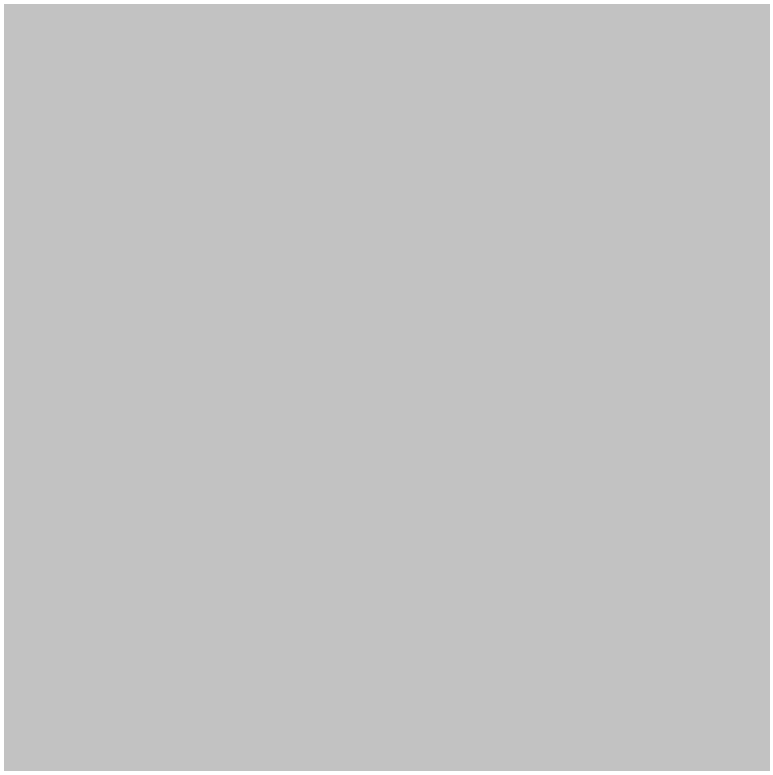


ps_loader

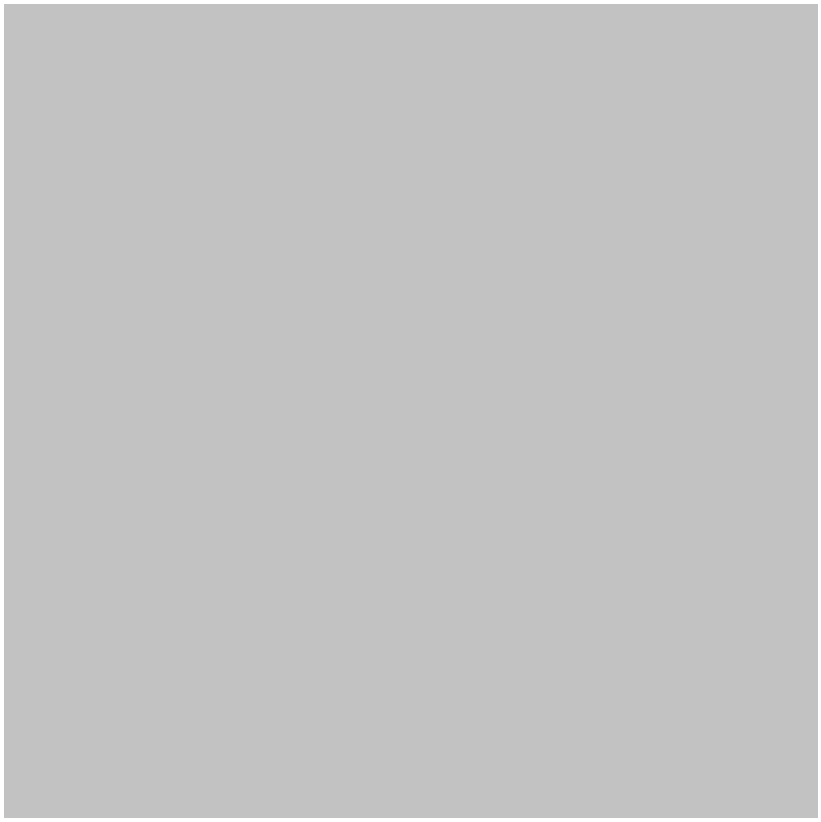
ps_start中加载执行DLL后门后会从内置的三个IP地址中选择一个作为C&C，再次下载一段PowerShell，此处称之为ps_loader：



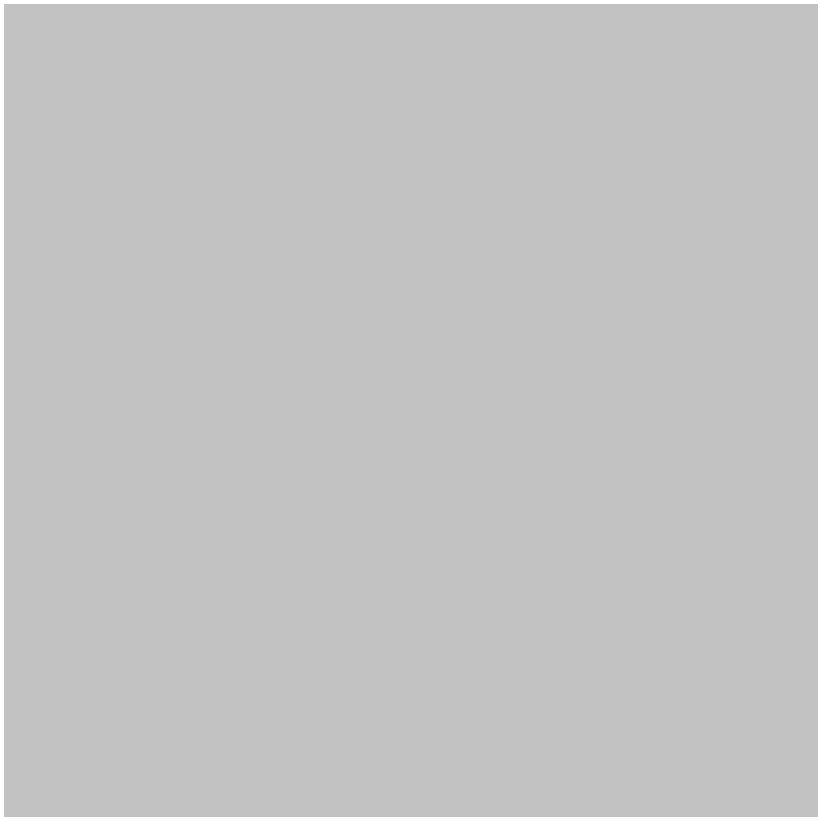
ps_loader会首先生成用于请求的对应的us及Cookie字段，具体请求如下所示，可以看到返回的数据是一系列的十进制字符：



接着对返回数据进行简单的初始化后，通过函数sj8对数据进行解密，可以看到攻击者使用了whatthefuckareyoudoing这个极富外国彩的调侃俚语作为秘钥：



解码后的内容也是一段PowerShell，此处命名为ps_backdoor，ps_backdoor会调用其对应的函数ROAGC：



ps_backdoor

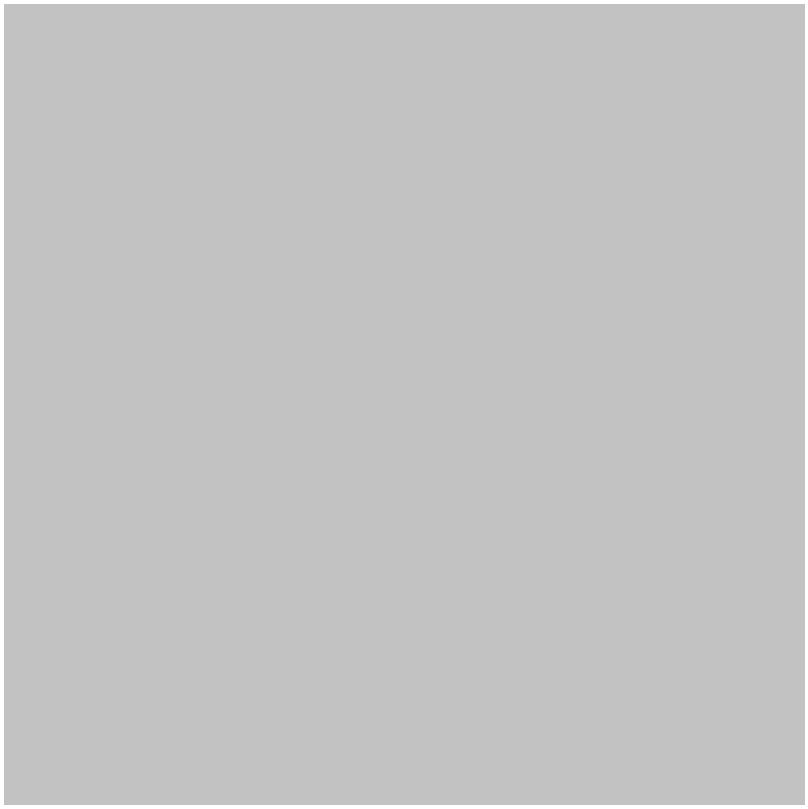
参数1：周期，此处为10

参数2：id，此处为zhengyi5

参数3：IP/Port二元组

参数4：对应加

参数5：对应的MAC地址



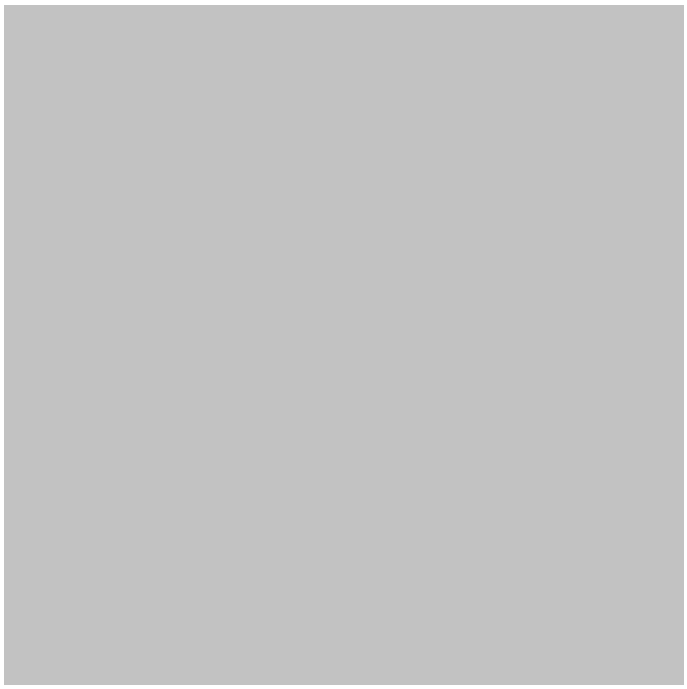
分析显示后门支持以下命令：

命令	描述
rs	执行CMD命令
up	上传文件
dw	下载文件

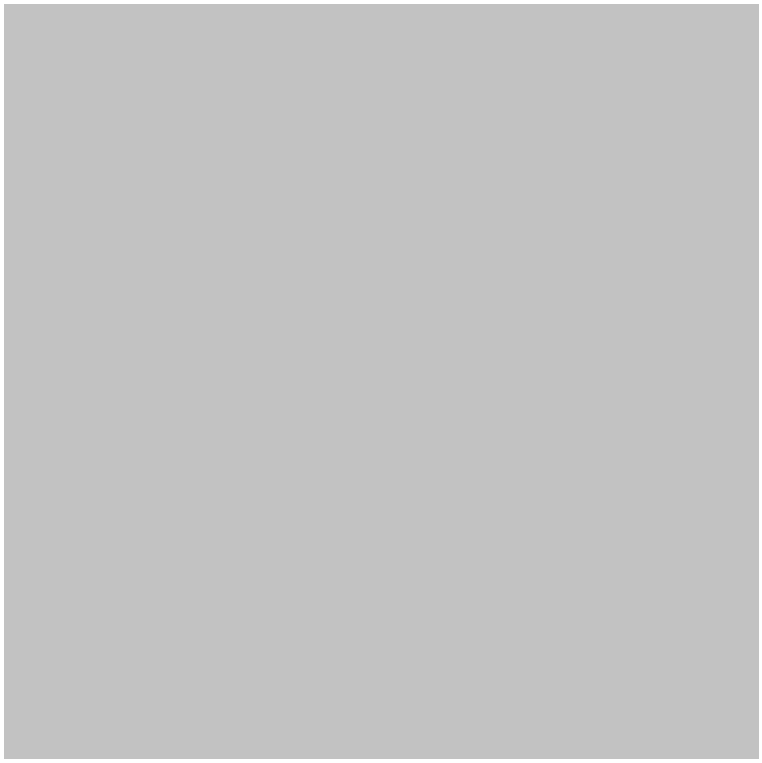
该脚本还支持CMD命令功能，除了Windows外，还支持Linux下的命令执行：

命令	描述
ls/dir	目录操作
mv/move/co	
cd	

命令	描述
Ipconfig/ifconfig	网络相关
ps/tasklist	进程信息获取
whoami/getuid	用户信息获取
rteboot/restart	开关机

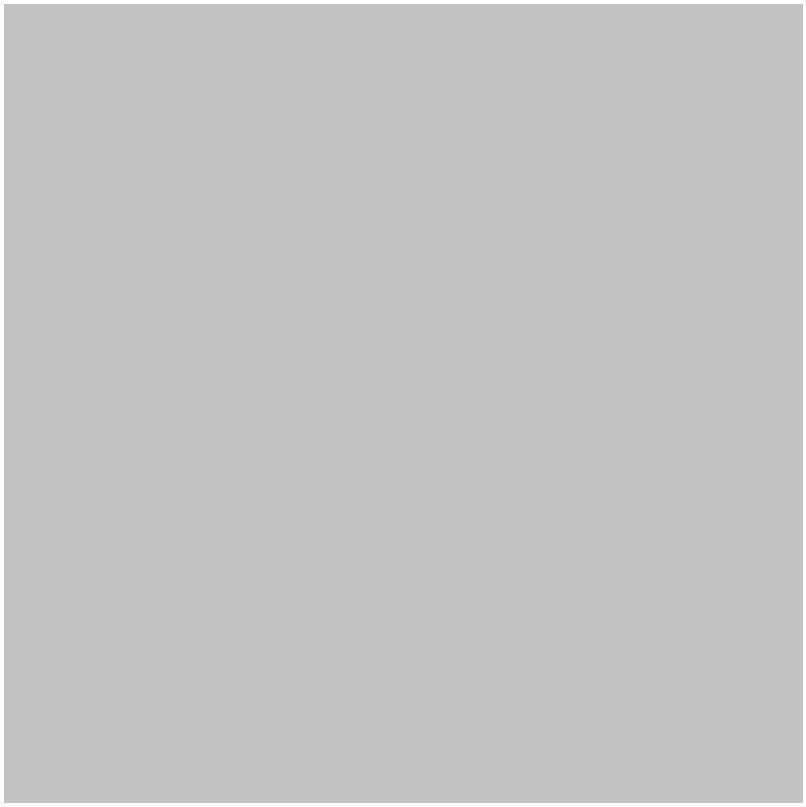


上传下载的通信流量通过AES进行了处理，KEY为ps_loader中传入的Dqd6lfRDcXK2KxIFDqU1S/MMyxGJ7qPIwM/xZe0R6Ps=：



持久化

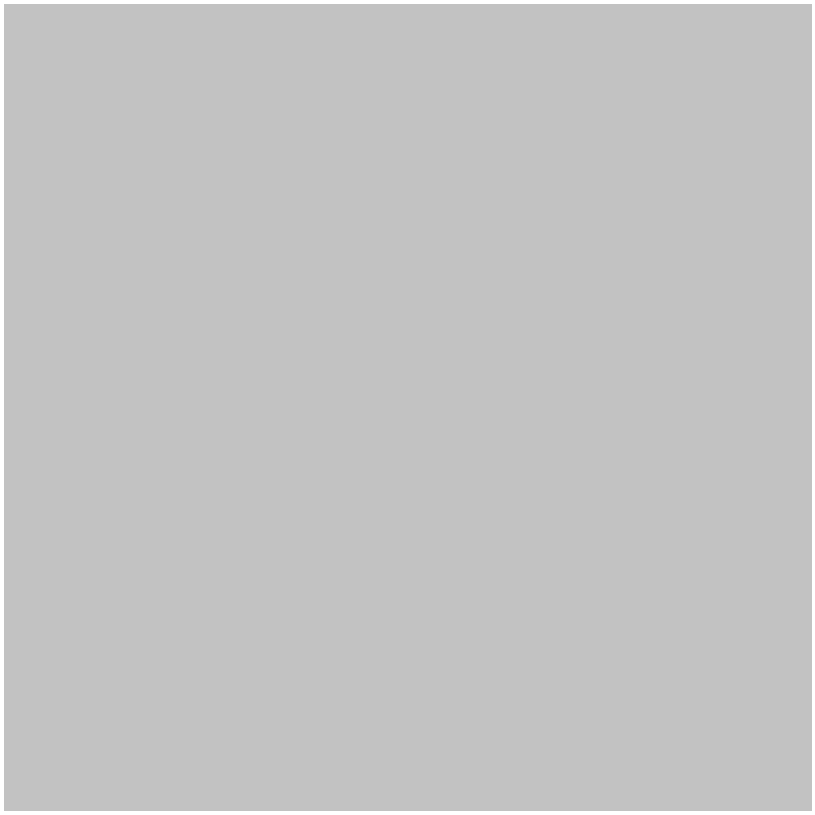
ps_start脚本会使用Rundll32.exe加载执行样本中解压出来的beoql.g后门文件，该DLL为一个实现恶意代码持久化加载的模块，用于载ps_loader，并通过修改LNK文件来实现持久化，其导出的函数如下所示：



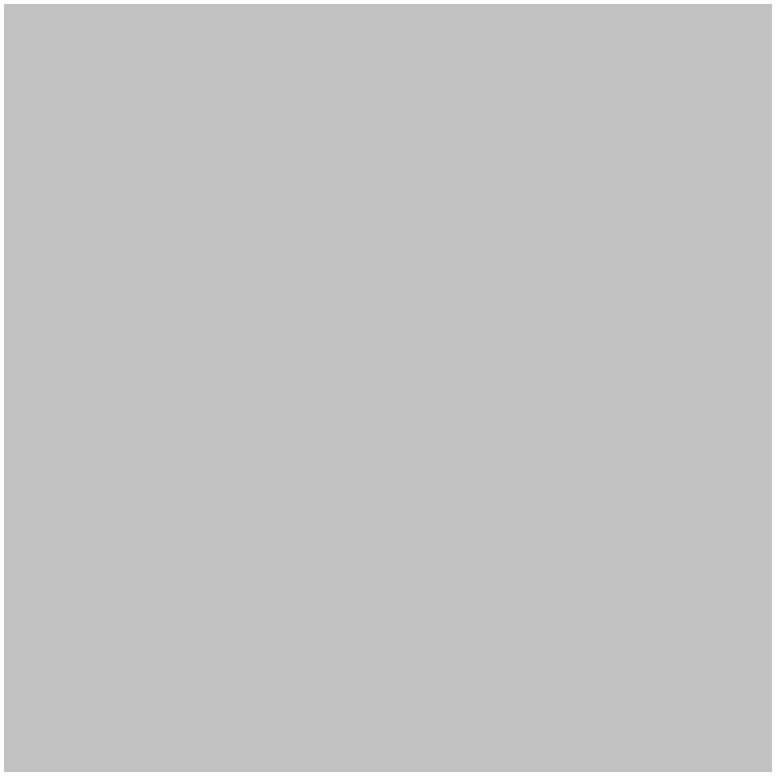
通过分析，DLL具体函数功能如下：

函数	功能
DllEntry	用于启动PowerShell
DllRegister	初始函数，用于保存传入的PowerShell，调用DllEntry启动PowerShell，调用DllInstall生成并启动用于修改系统LNK文件的BAT脚本
DllInstall	生成并启动用于修改系统LNK文件的BAT脚本
DllCanUnload	
DllSetClassObject	被BAT脚本调用用于修改LNK文件
DllUnsetClassObject	还原LNK文件
DllCopyClassObject	被BAT脚本调用用于拷贝LNK文件到临时目录下
DllEntryPoint	Dll入口

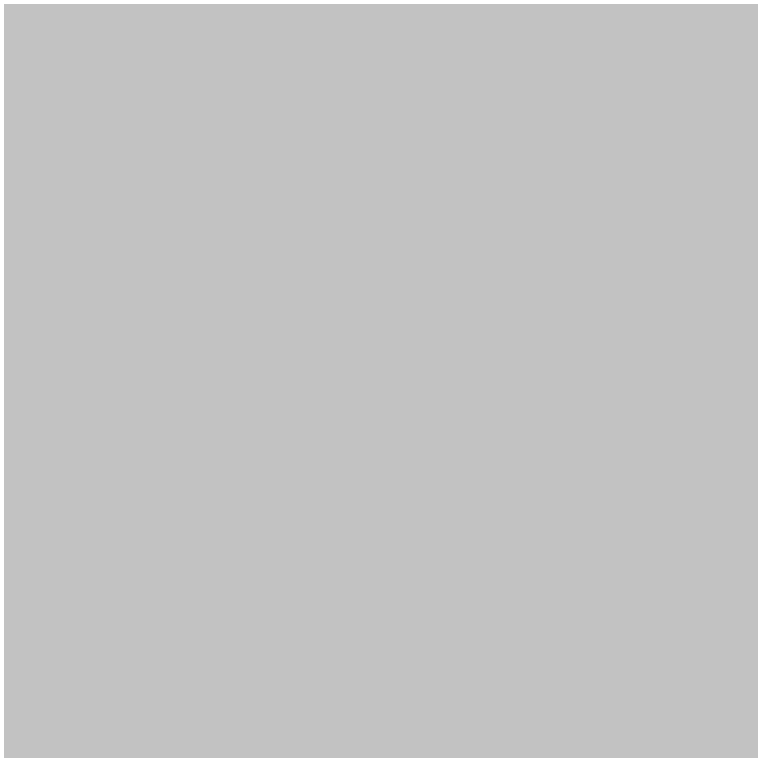
另外，ps_start中会直接调用该DLL的导出函数DllRegister，参数为对应的ps_loader脚本，函数首先会将ps_loader加密保存为beoql.g.ini，之后调用DllEntry和fun_Callinstall：



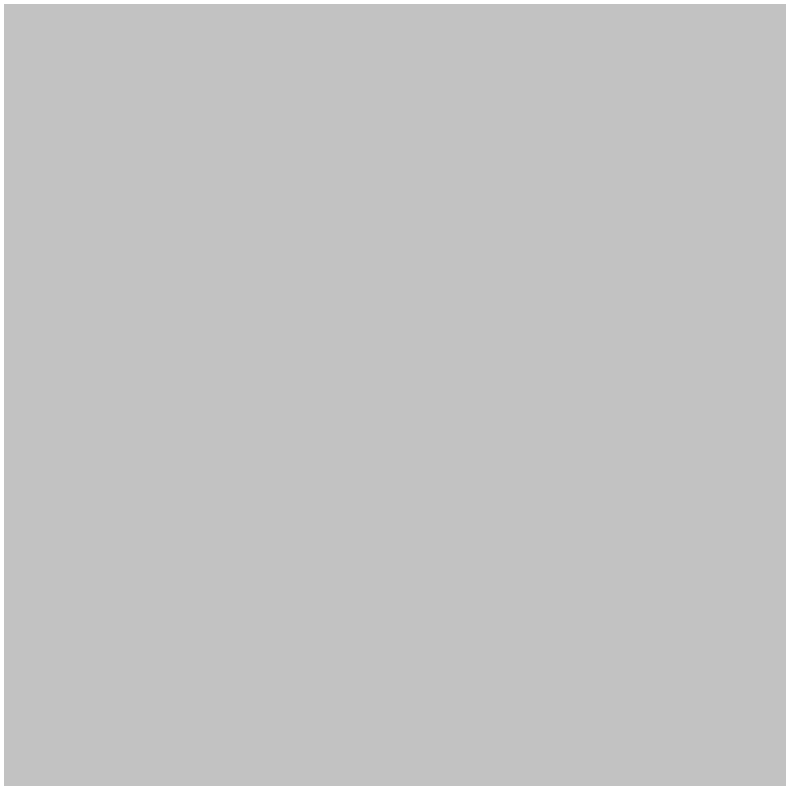
beoql.g.ini加密保存的PowerShell如下所示：



DllEntry被调用首先会通过CMD命令删除相关的金山的安全组件：

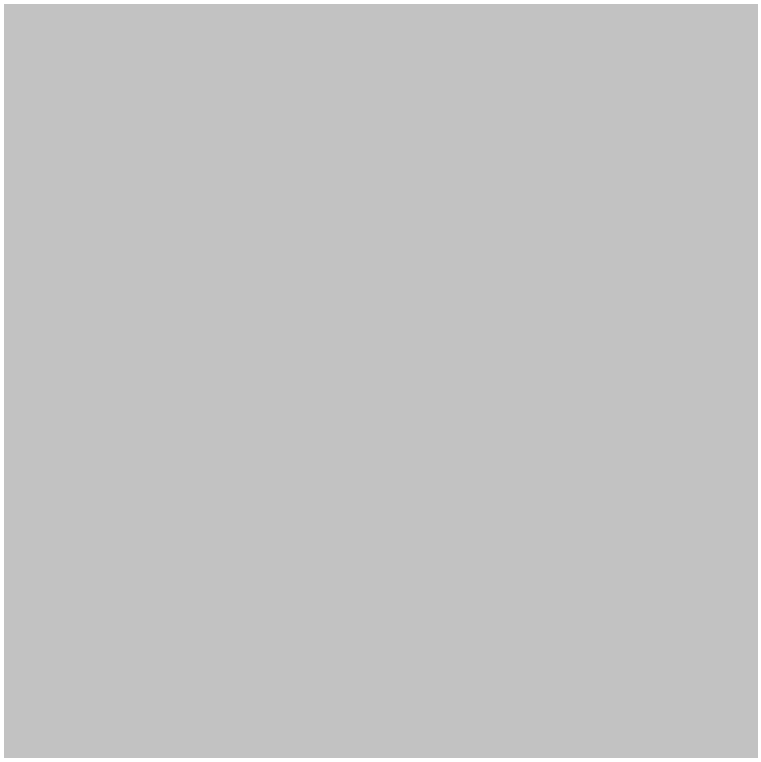


之后通过CreateProcess函数启动ps_loader脚本：

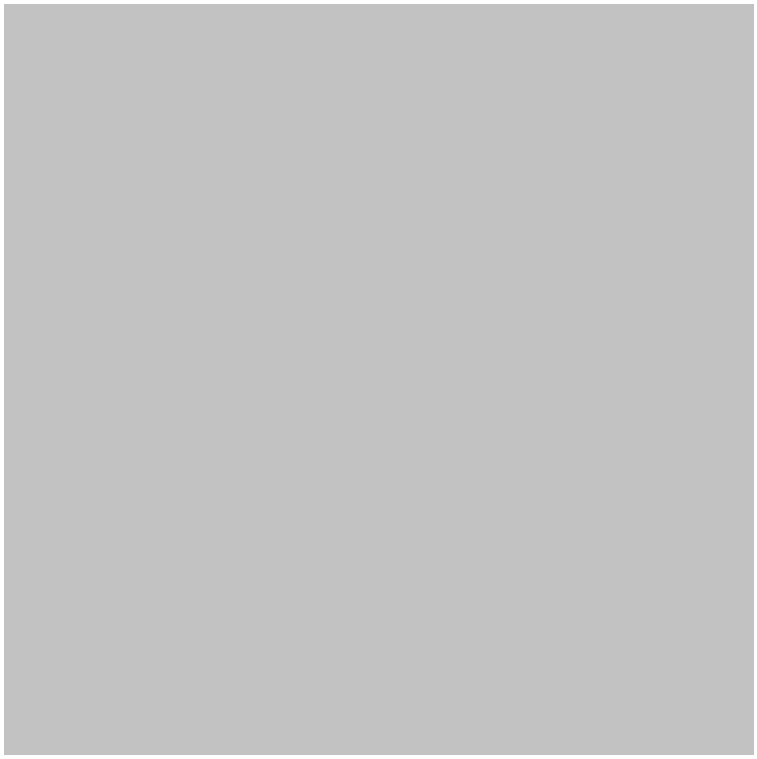


fun_Callinstall中解密出对应的加密字符，字符串为通过Rundll32.exe 调用导出函数DllInstall：

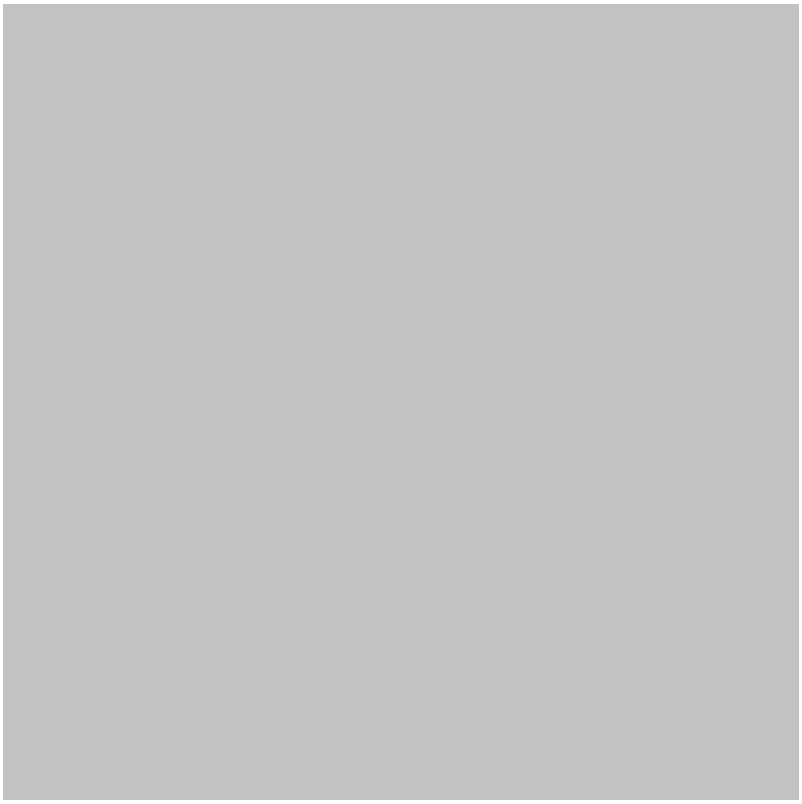
具体如下所示：



DllInstall函数首先遍历多个目录下的LNK文件：

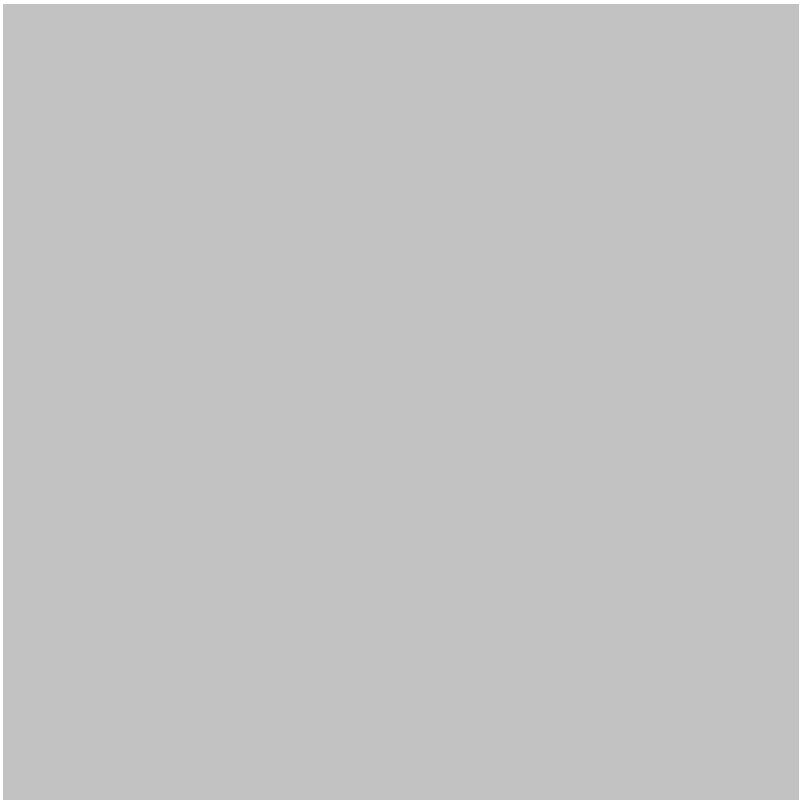


之后生成nview32_update.bat脚本，并运行：

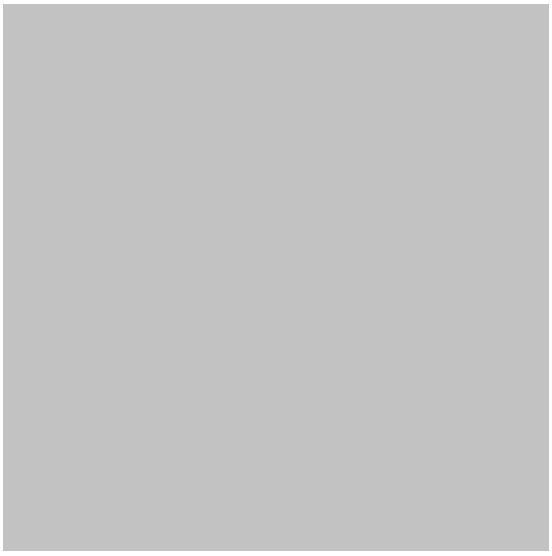


nview32_update.bat脚本执行后会检测并删除WPS的相关组件，之后对前面遍历获取的LNK文件进行修改操作：

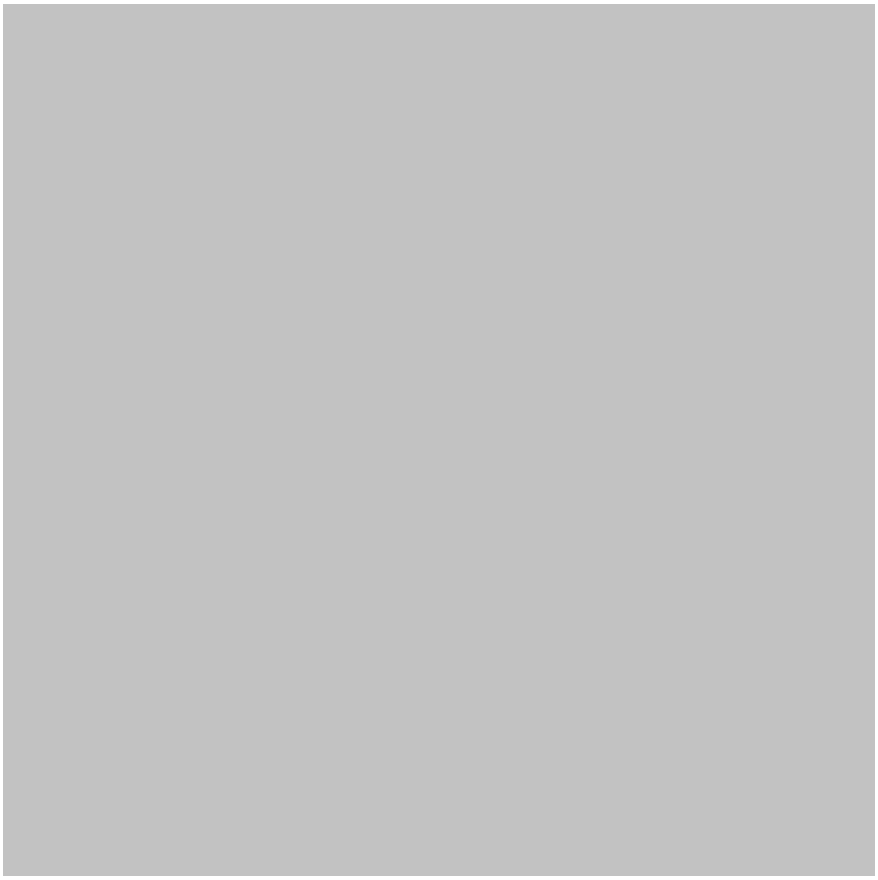
首先通过调用导出函数DllCopyClassObject将该LNK文件拷贝到临时目录，再通过函数DllSetClassObject修改%temp%目录下的LN
文件，最后将修改过的LNK文件拷贝覆盖回去：



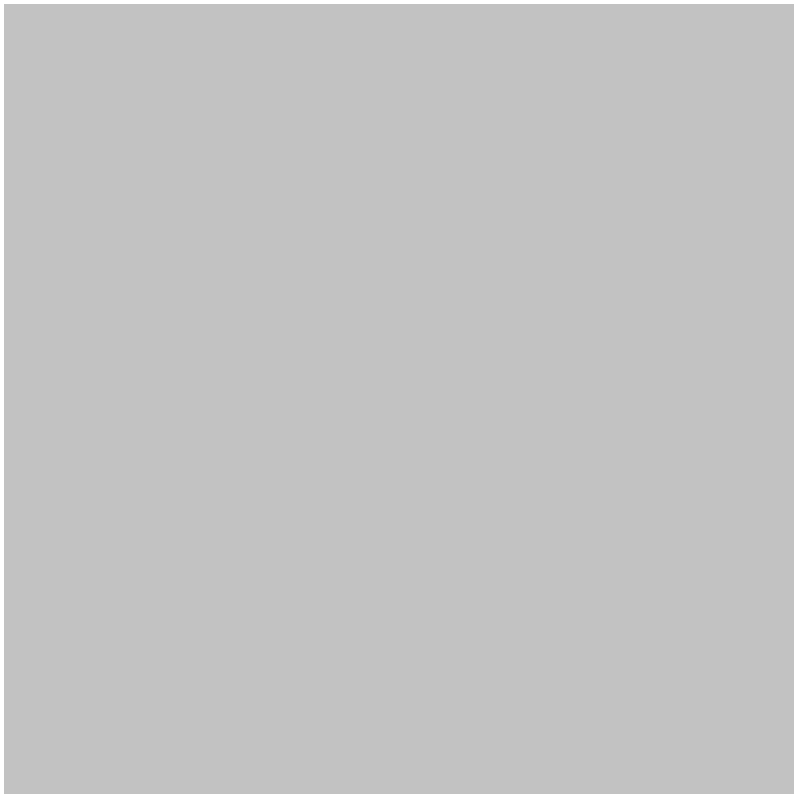
DllSetClassObject中通过函数fun_ChangeInk修改默认的LNK文件：



修改过的LNK文件以多个感叹号分割：

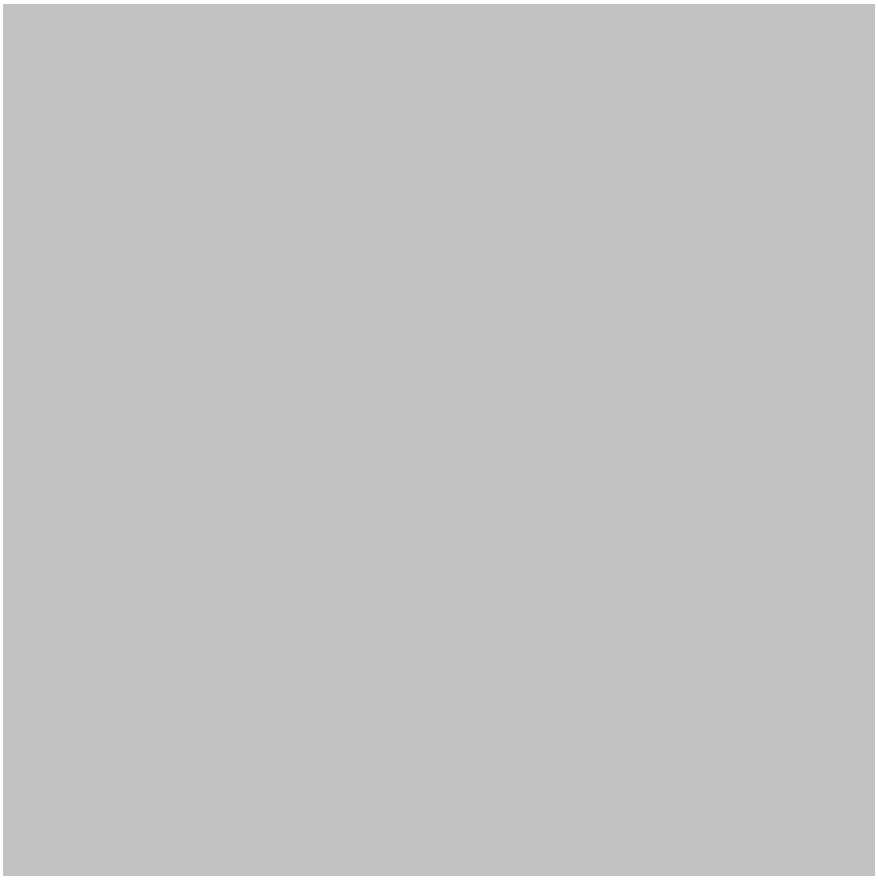


具体效果如下所示，LNK快捷方式文件被修改为通过Rundll32.exe调用该DLL的DllEntry函数，该函数的主要功能如前文所示用于运行
应的ps_loader脚本，通过劫持LNK快捷方式文件来起到持久化的作用：



攻击流程

整体攻击流程如下所示：



影响面评估

攻击时间

根据360网络安全研究院的全网数据抽样统计，对攻击者使用的两个云服务域名地址（子域名分别为0123和05011）的访问分别集中月和5月，这和我们捕获到的样本时间段完全一致，也就是说蓝宝菇APT组织在这两个月内使用本文描述的攻击方式进行了大量针对性攻击：

攻击对象

由于恶意样本会将窃取的用户数据通过Amazon S3云存储协议上传到攻击者的云服务器中，360威胁情报中心通过对AWS S3服务通
机制的深入解析，结合样本分析得到的数据模拟通信成功获取部分攻击者攻击过程中产生的中间数据，其中包括攻击对象的计算机名
被攻击时间等信息。数据显示仅一天时间内就有数个受害人员的信息被上传到服务器，整波攻击活动期间评估受控人员数量在百级。

总结

威胁情报在攻防对抗中发挥着越来越重要的作用，威胁情报不是简单的从blog、twitter等公开渠道获得开源情报。从本次事件中可以
出，只有具备扎实的安全能力、建立强大的数据基础并对威胁情报涉及的采集、处理、分析、发布、反馈等一系列的环节进行较长时
的投入建设，才能获得基于威胁情报的检测、分析、响应、预警等关键的安全能力。

目前，基于360威胁情报中心的威胁情报数据的全线产品，包括360威胁情报平台（TIP）、天眼高级威胁检测系统、360 NGSOC等，
已经支持对此APT攻击团伙攻击活动的实时检测和相关未知攻击的预警。

IOC

C&C IP
159.65.127.93
139.59.238.1
138.197.142.236
攻击者云服务地址
0123.nyc3.digitaloceanspaces.com
05011.nyc3.digitaloceanspaces.com

参考

[1].https://github.com/minio/minio-py

[2].https://docs.minio.io/docs/python-client-quickstart-guide

[3].https://docs.aws.amazon.com/zh_cn/AmazonS3/latest/dev/Introduction.html

[4].https://docs.aws.amazon.com/zh_cn/AmazonS3/latest/API/sig-v4-authenticating-requests.html

[5].https://developers.digitalocean.com/documentation/spaces/#authentication

[6].http://developer.huawei.com/ict/cn/doc/Object_Storage_Service_API_zh_p/zh-cn_topic_0016616545.html

***本文作者：360天眼实验室，转载请注明来自FreeBuf.COM**

更多精彩 # 蓝宝菇

相关推荐

蓝宝菇（APT-C-12
技术细节揭秘

已有 5 条评论

周鸿衣 2018-07-17 1楼 回

图片根本看不清。。。。。。。。。

亮了 (

360天眼实验室 (8级) 中国网络安全领导厂商奇安信旗下的威胁情报社交媒体 2018-07-17 [

@ 周鸿衣 https://ti.360.net/blog/articles/details-of-apt-c-12-of-operation-nuclearcrisis/

可以看这里，会清晰一点

亮了

萝卜不会飞 (1级) 2018-07-17 2楼 回

这是用座机截的图吧

亮了 (

360天眼实验室 (8级) 中国网络安全领导厂商奇安信旗下的威胁情报社交媒体 2018-07-17 [

@ 萝卜不会飞 https://ti.360.net/blog/articles/details-of-apt-c-12-of-operation-nuclearcrisis/

可以看这里会清晰一点

亮了

互联网的帽子戏法 （2级） 2018-07-17 3楼 回

没看到前期探针是怎么刺探信息的.或许他们用别的方法刺探信息;不需要探针.

这里没有看到出不来的话怎么上网,怎么获取wpad 和 LAN setting ; 测试 tcp: 21 22 23 80 443 8443 53 udp:53 161 123 137 dns:53 icmp. 包括获取 pptp l2tp ipse 等配置信息,wifi配置信息 等等. 应该还可以获取到本地软件,服务代理上网信息.

提权/过UAC也没看到.....

持久化修改lnk来达到劫持效果,也是一个idea.

没有获取ie firefox chrome历史记录和保存密码信息 不知道是他们漏了还是360漏写了...

没有键盘记录我估计是不好过360 + 考虑到其它方式实现的话中文字体获取会有问题...

肛需:

1.不被网关/防火墙给拦截了.

2.尽量别进了垃圾邮箱.

3.最好前期有探针,得知道对方一些基本信息.

(pc 移动端 客户端 操作系统 浏览器 内网ip 外网ip java版本 flash 部分客户端软件信息,或许包括有杀软的 jsonp刺探等等).当然省略探针也行.....

更高层次考虑的:

如何对抗各大厂商的沙盒检测.

躲避杀软查杀,静态和行为.

如何针对性的持久化控制.(注册表 任务计划 启动项 dll/exe之类的替换劫持 环境变量 针对一些软件和数据库来定制 等等...)

这里的修改lnk,达到劫持效果也差不多.

如何采用多种方式来长期潜伏,怎么采用多种方式来"发送按钮激活".

激活后的隐藏运作,各种方法测试+延迟两小时测试一下是否能出得来,出不来就自销毁,工作行为只做一次性.

工作做完后继续潜伏;各种潜伏方式轮换.

如何采取加密隐蔽的传输通道:例如根据目标环境找"云端加密传输数据"+"云端控制加密传输". （例如:OneDrive dropbox baiduyun 360网盘 tumblr facebook twrite google Microsoft skype qq等等.)

这里云端用到了AWS的s3,差不多的思路.

例如云端加密传输数据;平均每次10个分卷,分卷压缩前加密了;然后提取第一个压缩文件随机一行字节发送去远端存储,然后删除这一行. 等你本地下载回来自己组合还原,这样人家溯源到难度很大 1) 可能不知道你加密密码 2) 不知道你提取第一个压缩文件随机一行字节发送去远端存储,然后删除这一行是啥内容.

亮了 (

选择文件 未选择任何文件

昵称 必须 您当前尚未登录。登陆? 注册

请输入昵称

邮箱 必须（保密）

请输入邮箱地址

表情 插图

提交评论(Ctrl+Enter) 取消 有人回复时邮件通知我

奇安信威胁情报中心

中国网络安全领导厂商奇安信旗下的威胁情报社交媒体

139
文章数

4
评论数

最近文章

英国核发电厂遭受网络攻击，疑似法国电力公司受影响
2019.12.07

阻击“幻影”行动：奇安信斩断东北亚APT组织“虎木槿”伸向国内重要机构的魔爪
2019.12.05

追踪奥地利钓鱼木马，回顾仿冒美团钓鱼事件
2019.12.05

浏览更多

相关阅读

关于F-BOMB设备以及物理渗透设备介...

走进科学：我是如何破解学校饭卡实现...

新型银行木马病毒MysteryBot Androi...

取代苹果公司，是谁在帮助FBI解锁iPh...

揭秘：iOS恶意软件KeyRaider如何盗...

推荐关注

FreeBuf+微信小程序

FreeBuf官方微信小程序，把安全装进口袋

扫码添加小程序

FreeBuf微信订阅号

国内领先的互联网安全新媒体，同时也是爱好者们交

社区

11月 上海

CIS 2019首席信息安全官闭门高峰论坛

已结束

11月

CIS 2019议题抢先看

已结束

10月

公开课双十一活动

已结束

扫码关注公众号

FreeBuf企业安全服务号

FREEBUF

FreeBuf+小程序

本站由 阿里云 提供计算与安全服务

扫码把安全装进口袋

PreviousNext