

# WannaCry 勒索蠕虫可能是朝鲜干的？

(原创) 2017-05-16 周超臣 虎嗅网


```

Hiew: 766d7d59
3a1e5940fd6ac777f606ed64e731fd91b0b4c3
push ecx
push ebx
push ebp
mov ebp,[esp]
push esi
push edi
push 020 ;' '
mov eax,[ebp]
lea esi,[ebp]
and al,1
or al,1
inc esi
mov [ebp][0],b,[esi][-1]
mov b,[esi],1
inc esi
push esi
call .010001600
add esp,8
push 4
push 0
call time
add esp,4
cdq
push edx
push eax
call .010004CC0
mov [esi],eax
add esi,020 ;' '
add esp,00C
mov b,[esi],0
inc esi
call rand
cdq
mov ecx,5
xor edi,edi
idiv ecx
lea eax,[esi]
add edx,2

Hiew: 3e6de9e2baac930949647c3998
2a6de9e2baac-f070049647c399818e7a7c3a0a2626df6a468407954aa515e0d9
push ecx
push ebx
push ebp
mov ebp,[esp][010]
push esi
push edi
push 020 ;' '
mov eax,[ebp][0]
lea esi,[ebp][4]
and al,1
or al,1
inc esi
mov [ebp][0],eax
mov b,[esi][-1],3
mov b,[esi],1
inc esi
push esi
call .000400130 --41
push 0
call time
add esp,00C
push eax
call WS2_32.8
mov [esi],eax
add esi,020 ;' '
mov b,[esi],0
inc esi
call rand
cdq
mov ecx,5
xor edi,edi
idiv ecx
lea eax,[esi][2]
add edx,2
lea ebx,[edx][edx]*2
shl ebx,1
test ebx,ebx
jle .000402633 --42
mov [esp][018],eax
```

5月16日早上，腾讯玄武实验室负责人TK（在黑客圈有“TK教主”、“妇科圣手”的雅号）在朋友圈转发securelist的报道：“基于软件同源性分析等技术，多个研究人员得出了同一个结论：WannaCry 勒索蠕虫可能是朝鲜干的。”

据法新社和路透社等外媒报道称，赛门铁克、卡巴斯基和安全专家Matt Suiche等10位研究员均认为有证据显示，遍及全球的勒索病毒背后可能是朝鲜黑客团队“拉撒路组”。



卡斯基研究室安全人员表示，该研究室在研究了早期蠕虫病毒版本与2015年2月的病毒样本发现，其中部分相似的代码来自于卡斯基之前关注的朝鲜黑客团队“拉撒路组”，代码的相似度远超正常程度。卡斯基认为本次流行的WannaCry勒索病毒与之前的冲击波病毒出自同一黑客团队。

赛门铁克也发现了同样的证据。

至于这个结论的可能性有多大，TK在接受虎嗅采访时表示：“你问了一个要用一篇论文来回答的问题。”

TK告诉虎嗅：“基于软件源性分析发现的线索，好比监控摄像拍下昨天闯入陕西饭店抢走四大罐油泼辣子的蒙面劫匪左臂有个皮皮虾纹身，现在有人注意到去年在家乐福偷卫生巾的贼也有这个纹身。只能说有线索能把这两件事联系起来了，还说明不了什么问题。另外，网络攻击的溯源分析本身也是大学问，涉及很多技术。”

关于WannaCry勒索病毒的真凶到底是谁目前还处于猜测阶段，也没有任何一个黑客组织宣布对这一事件负责。

日前，腾讯安全反病毒实验室表示，此次勒索事件传播方式采用了前不久NSA被泄漏出来的MS17-010漏洞。在NSA泄漏的文件中，WannaCry传播方式的漏洞利用代码被称为“EternalBlue”，因此也有的报道称此次攻击为“永恒之蓝”。

微软公司总裁布拉德·史密斯发布声明怒斥美国政府囤积电脑病毒武器，“如果用传统武器来打比方，这就相当于美国军方的‘战斧’巡航导弹失窃。”

俄罗斯总统普京也对史密斯的这一说法表达了支持：“我认为，微软总裁已经说得很坦率了，病毒最初就是来源于美国的情报机构。”

MS17-010漏洞指的是，攻击者利用该漏洞，向用户机器的445端口发送精心设计的网络数据包文，实现远程代码执行。如果用户电脑开启防火墙，也会阻止电脑接收445端口的数据。

至于中国高校成为重灾区的原因，腾讯安全反病毒实验室负责人马劲松分析认为：“由各大高校通常接入的网络是为教育、科研和国际学术交流服务的教育科研网，此骨干网出于学术目的，大多没有对445端口做防范处理，这是导致这次高校成为重灾区的原因之一。此外，如果用户电脑开启防火墙，也会阻止电脑接收445端口的数据。但中国高校内，一些同学为了打局域网游戏，有时需要关闭防火墙，也是此次事件在中国高校内大肆传播的另一原因。”

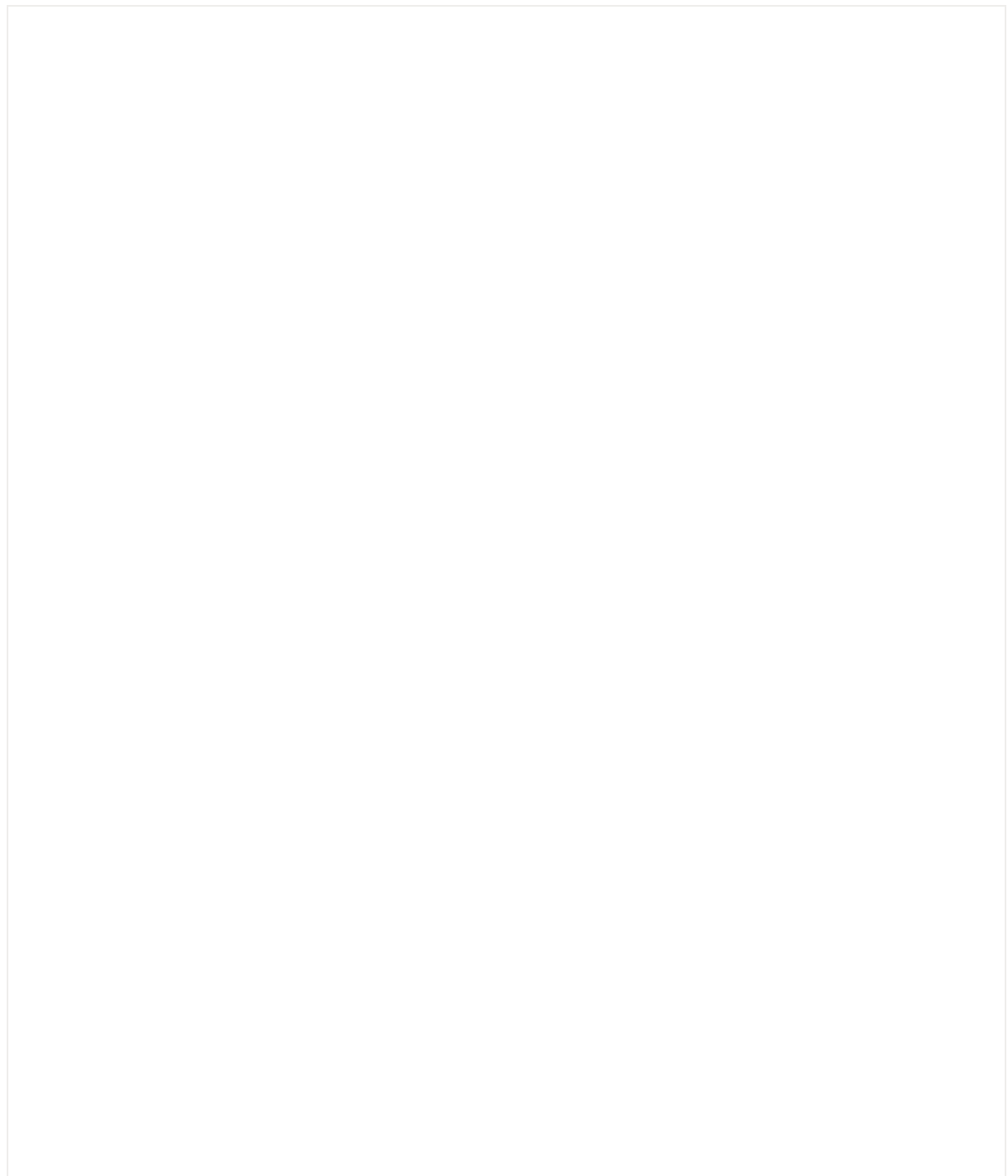
马劲松还表示：“敲诈者木马本身没什么不一样，但是Wana系列敲诈者木马的传播渠道是利用了445端口传播扩散的SMB漏洞MS17-101，微软在17年3月发布了该漏洞的补丁。2017年4月，黑客组织Shadow Brokers公布的Equation Group（方程式组织）使用的“网络军火库”中包含了该漏洞的利用程序，而该勒索软件的攻击者或者攻击组织就是在借鉴了“网络军火库”后进行了这次全球大规模的攻击，主要影响校园网，医院、事业单位等内网用户。”

他认为这场黑客攻击中，除了病毒作者，没有赢家，“实际上这场席卷全球的勒索病毒风波是一次网络灾难，对所有人都是一次巨大的打击。”

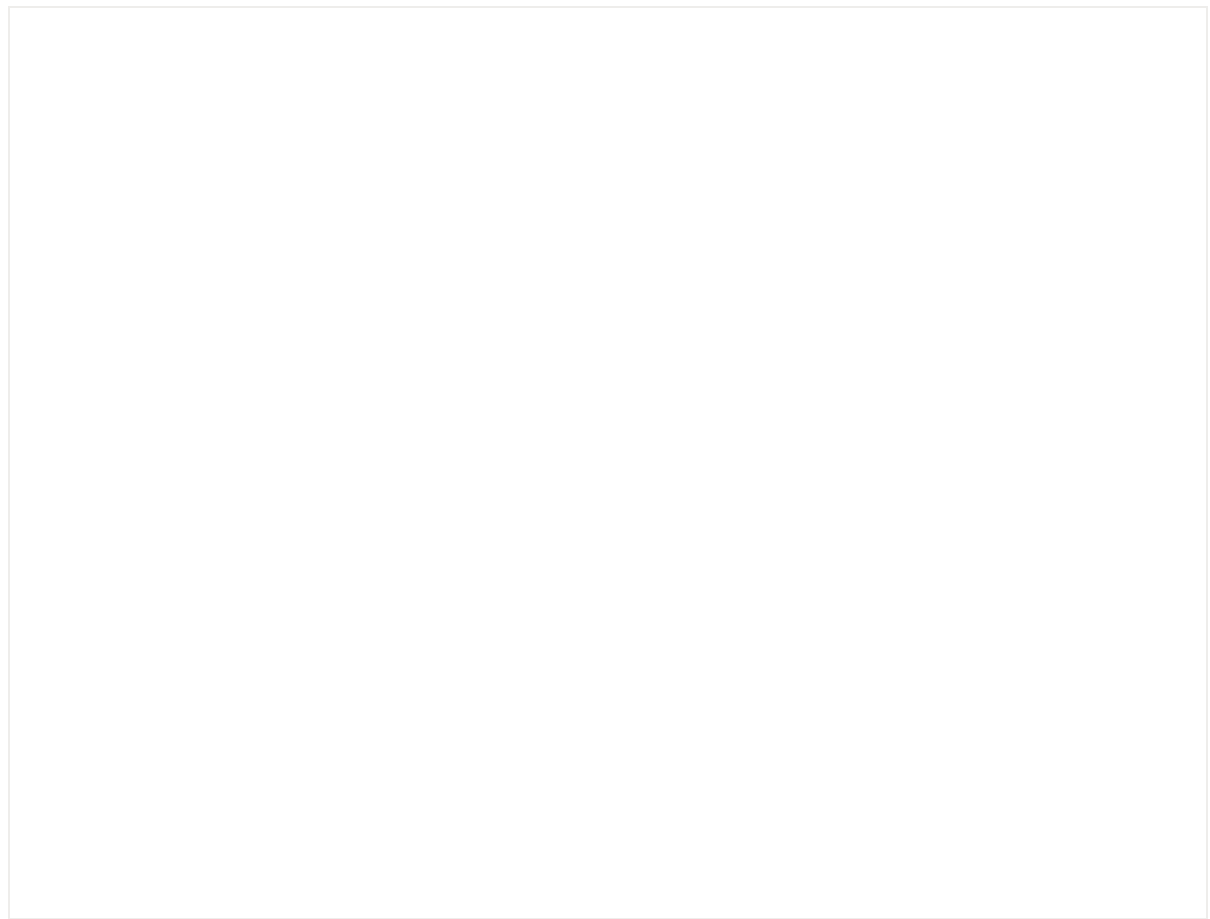
## 攻击流程

腾讯安全反病毒实验室还演示了整个的攻击流程，简要如下：

勒索病毒被漏洞进程执行后，会从资源文件夹下释放一个压缩包，此压缩包会在内存中通过 密码:WNCry@2017 解密并释放文件。这些文件包含了后续弹出勒索框的 exe，桌面背景 图片的 bmp，包含各国语言的勒索字体，还有辅助攻击的两个 exe 文件。这些文件会释放 到了本地目录，并设置为隐藏。



其中 `u.wnry*` 就是后续弹出的勒索窗口。



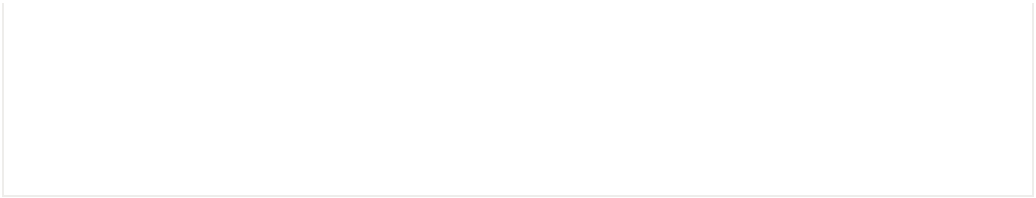
窗口右上角的语言选择框，可以针对不同国家的用户进行定制展示。这些字体的信息也存在于之前资源文件释放的压缩包中。

通过分析病毒，可以看到，以下后缀名的文件会被加密：

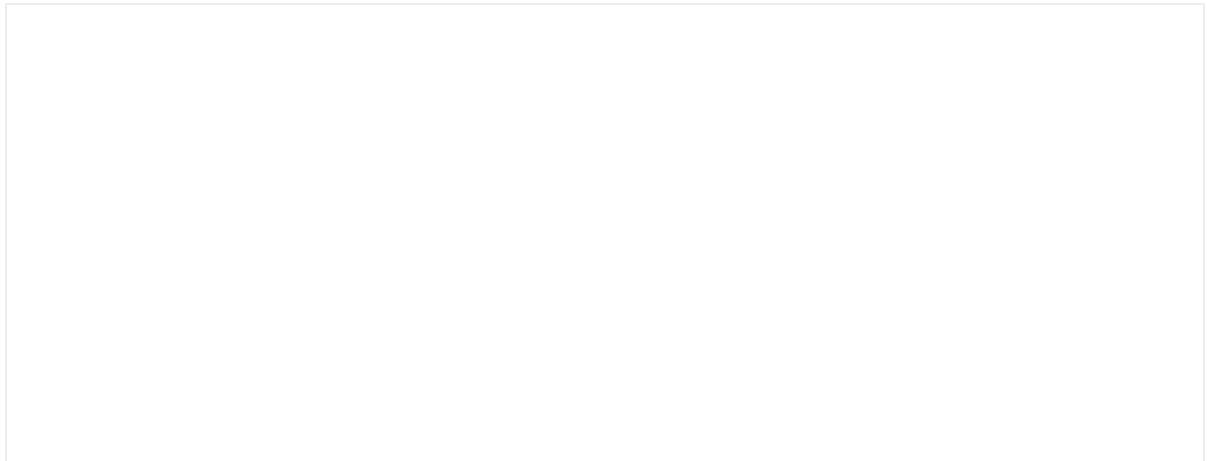
docx.docb.docm.dot.dotm.dotx.xls.xlsx.xlsm.xlsb.xlw.xlt.xlm.xlc.xltx.xltm.ppt.pptx.pptm.pot.pps.ppsm.ppsx.ppam.potx.potm.pst.ost.msg.eml.edb.vsd.vsdw.txt.csv.rtf.123.wks.wk1.pdf.dwg.onetoc2.snt.hwp.602.sxi.sti.sldx.sldm.sldm.vdi.vmdk.vmx.gpg.aes.ARC.PAQ.bz2.tbk.bak.tar.tgz.gz.7z.rar.zip.backup.iso.vcd.jpeg.jpg.bmp.png.gif.raw.cgm.tif.tiff.nef.psd.ai.svg.djvu.m4u.m3u.mid.wma.flv.3g2.mkv.3gp.mp4.mov.avi.asf.mpeg.vob.mpg.wmv.flac.swf.wav.mp3.sh.class.jar.java.rb.asp.php.jsp.brw.sch.dch.dip.pl.vb.vbs.ps1.bat.cmd.js.asm.h.pas.cpp.c.cs.suo.sln.ldf.mdf.ibd.myi.myd.frm.odt.dbf.db.mdb.accdb.sql.sqlitedb.sqlite3.asc.lay6.lay.mml.sxm.otg.odg.uop.std.sxd.otp.odp.dp.wb2.slk.dif.stc.sxc.ots.ods.3dm.max.3ds.uot.stw.sxw.ott.odt.pem.p12.csr.crt.key.pfx.der。



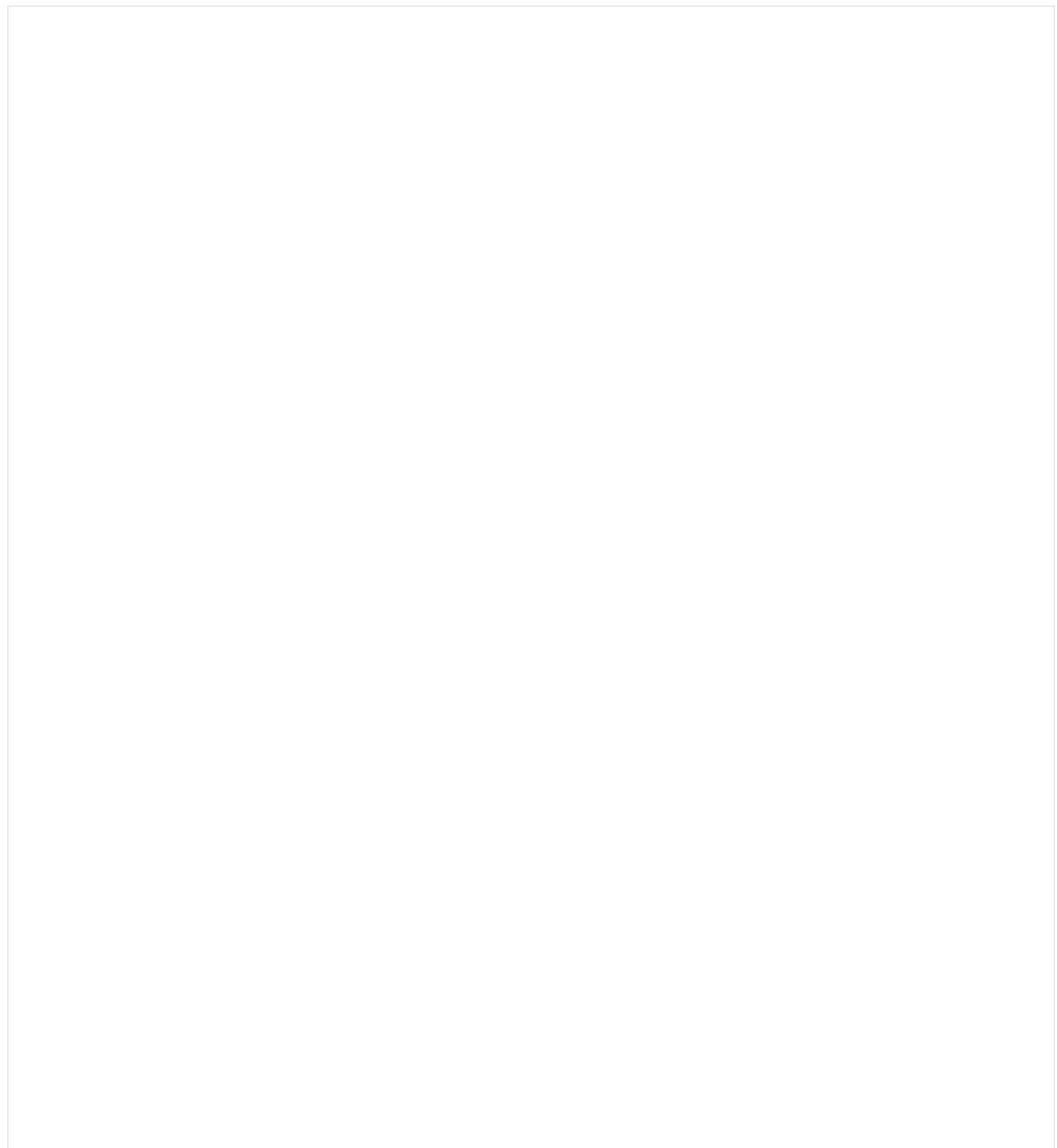





以图片为例，查看电脑中的图片，发现图片文件已经被勒索软件通过 Windows Crypto API 进行 AES+RSA 的组合加密。并且后缀名改为了\*.WNCRY



此时如果点击勒索界面的 decrypt，会弹出解密的框。



但必须付钱后，才可以解密



115p7UMMngo1pMvkcHjRdfJNXj6LrLn  
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw  
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

黑客目前是通过这三个账号随机选取一个作为钱包地址，收取非法钱财。

## 如何防范

这场始于英国，随后波及到全球上百个国家的黑客攻击让人人心惶惶，从5月12日晚上开始，中国的校园网、机场、银行、加油站、医院、警察、出入境等事业单位开始大规模爆发，众多学生、机构电脑被感染。尽管被感染的电脑只占一小部分，但网络安全无小事，注意和防范是必然的。

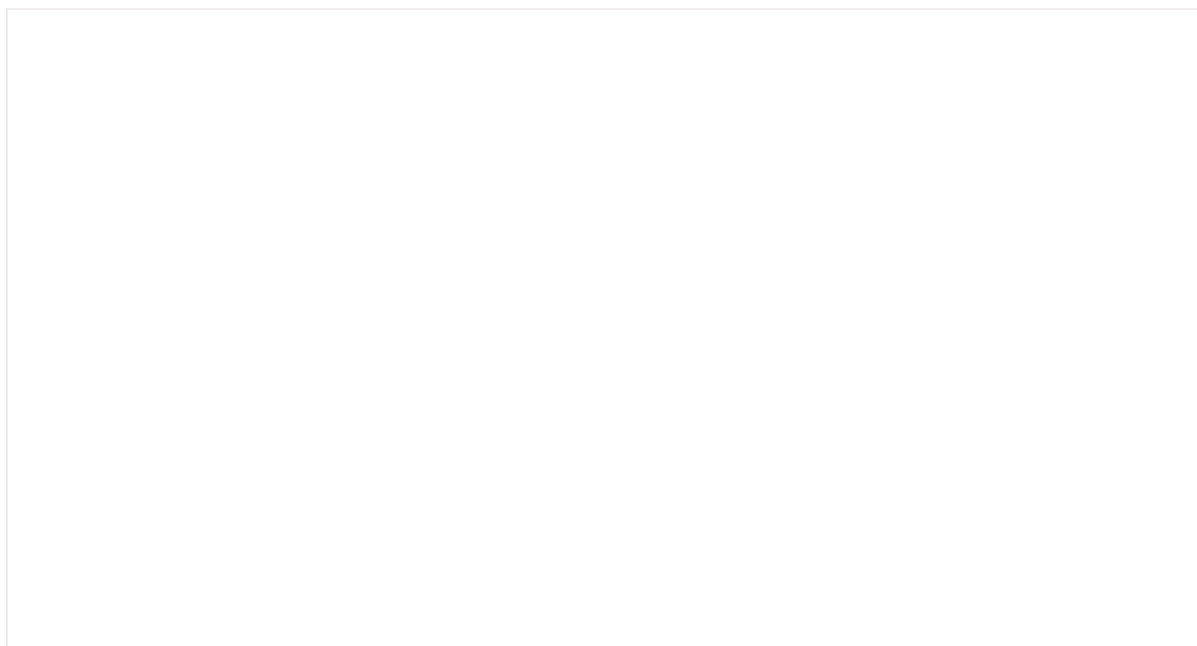
关于如何防范，除了微软紧急发布了补丁外，开启防火墙是简单直接的方法，步骤如下：

1. 打开控制面板点击防火墙
2. 点击“高级设置”

3. 先点击“进站规则”，再点击“新建规则”
4. 勾选“端口”，点击“协议不端口”
5. 勾选“特定本地端口”，填写 445，点击下一步
6. 点击“阻止链接”，一直下一步，并给规则命名

## 一个推荐

---





[阅读原文](#)

---