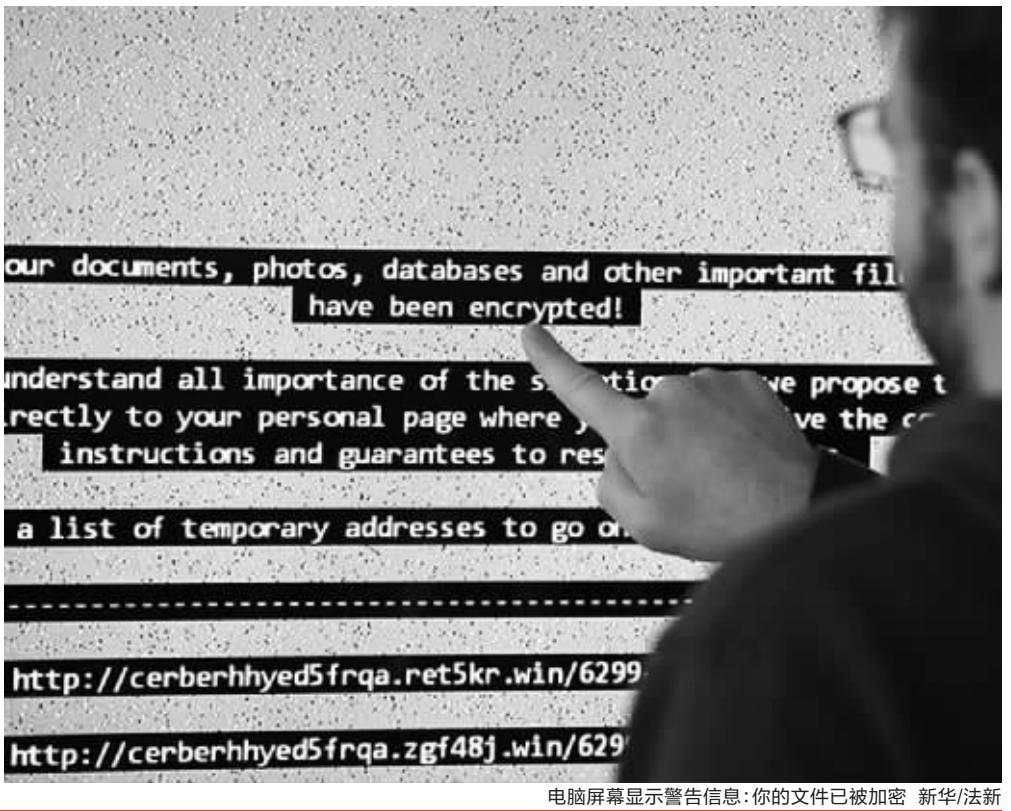
# WARNING

# 勒索软件肆虐全球

## 近百国遭黑客攻击 病毒武器源自美国

12日,全球99个国家和地区发生超过7.5万起电脑病毒攻击事件,罪魁祸首是一个名为“想哭”(WannaCry)的勒索软件。俄罗斯、英国、中国、乌克兰等国“中招”,其中英国医疗系统陷入瘫痪、大量病人无法就医。这款病毒源自上月遭泄密的美国国家安全局病毒武器库。不少网络专家和电脑安全公司批评,美国网络项目开支的90%用于研发黑客攻击武器,一旦该“武器库”遭泄密,势必殃及全球。



电脑屏幕显示警告信息:你的文件已被加密 新华/法新

**勒索**

### 在规定期限支付300美元赎金

据捷克网络安全企业爱维士公司统计,全球99个国家和地区12日共遭遇超过7.5万次电脑病毒攻击,其中俄罗斯、乌克兰等国遇袭尤其严重。

这款病毒名为“想哭”,属于一种勒索软件。电脑用户会收到一封电子邮件,往往是打着工作邀约、发货清单、安全警告等“幌子”,但一旦打开相关链接,就会导致电脑中招。

该勒索软件随即会对电脑储存的文件进行加密,使用户无法打开。电脑屏幕上弹出警告语:“你或许会试图夺回文件,还是别浪费时间了!”

接着,电脑提示用户在规定期限内支付300美元赎金,便可恢复电脑资料;每耽搁数小时,赎金额度就会上涨一些,最高涨至600美元。

据俄罗斯卡巴斯基实验室研究员库尔特·鲍姆加特纳观察:“在支付赎金的用户中,多数人在最初几小时内就乖乖掏出300美元。”

**遭殃**

### 涉及英国、西班牙、葡萄牙、阿根廷等

据Splunk网络安全公司主管里奇·巴杰描述,“这是全球迄今最大的勒索软件攻击事件之一”。卡巴斯基全球研究和分析团队表示,俄罗斯所受攻击远远超过其他受害者,而中国大陆和台湾地区也受到较多攻击。

英国公共卫生体系国民保健制度的服务系统12日被病毒入侵后,多家医院电脑瘫痪,不得不停止接待病人,一些救护车等医疗服务也受影响。

西班牙、葡萄牙、阿根廷等多国电信企业,以及美国联邦快递公司均受这款病毒侵袭。

俄罗斯内务部、梅加丰电信公司遭遇同种病毒攻击,据信已控制住病毒扩散规模。俄罗斯国际文传电讯社援引俄内务部发言人伊琳娜·沃尔克的话报道,俄内务部大约1000台电脑被感染,不到该部门电脑总数的1%。

**共识**

### 病毒被指来源于美国国安局

目前,尚未有黑客组织认领这次袭击。但业界人士的共识是,这款“想哭”病毒来源于美国国安局的病毒武器库。上个月,美国国安局遭遇泄密事件,其研发的病毒武器库被曝光于网上。

路透社援引美国联邦政府公布的数据以及情报部门官员的话报道,美国网络项目开支中,90%用于研发黑客攻击武器,例如侵入“敌人”的电脑网络、监听民众、设法让基础设施瘫痪或受阻等。

面对外界批评,美国国安局尚未作出回应。美国国土安全部计算机紧急应对小组表示,正密切关注这起波及全球的黑客攻击事件。

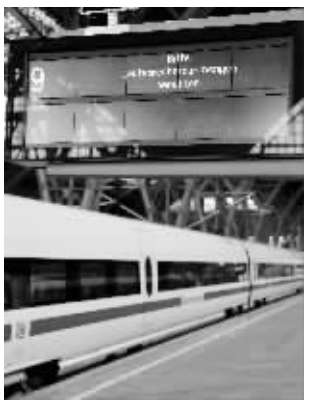
**进展**

### 已停止技术支持的 微软也提供补丁

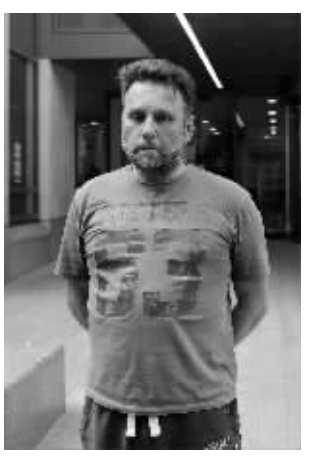
网络安全专家说,这种勒索软件利用了“视窗”操作系统的一个名为“永恒之蓝”的漏洞。

微软表示,它已在3月发布了安全补丁,修复上述漏洞。运行了这一补丁的用户可免受网络攻击。对于使用“视窗”所附杀毒软件Windows Defender的用户,微软在12日早些时候发布了一个安全补丁。微软说,有些用户还在使用微软已不再提供技术支持的“视窗”版本,鉴于用户可能受到的潜在影响,微软决定向这些“视窗”平台提供3月发布的补丁,包括“视窗XP”“视窗8”和“视窗”服务器2003在内的用户可下载这款补丁。

据新华社


**德国** 5月13日,在莱比锡火车站拍摄的无法正常工作的电子时刻表 新华社/法新


**德国** 5月12日,在开姆尼茨,一处电子时刻表遭到病毒攻击而无法工作 新华社/法新


**英国** 5月12日,在伦敦,一名由于医院电子系统遭到病毒攻击而无法进行心脏手术的男子在医院外接受媒体采访 新华社/美联

**我国情况**

## 多所高校中招 毕业论文“沦陷” 国家网信安全中心:尽快打补丁

中国多所高校也接连被“勒索”病毒命中。这种病毒致使许多高校毕业生的毕业论文(设计)被锁,支付赎金后才能解密。5月13日,现代快报从南京高校获悉,目前已经有高校封锁了被攻击的445端口,并告知全校师生及时下载微软发布的补丁、升级系统,而这一做法,对于社会用户同样适用。

现代快报/ZAKER南京记者 金凤

### 多所高校中招

5月12日夜晚、13日凌晨,国内高校成为此次病毒攻击的重灾区,学生电脑上的资料文档会被锁,需要付费才能解锁。临近毕业季,不少同学的毕业论文、毕业设计等重要资料已经宣告“沦陷”。部分高校已发布预警信息。

据悉,目前受影响的有贺州学院、桂林电子科技大学、桂林航天工业学院等学校。另外有网友反映,大连海事大学、山东大学等也受到了病毒攻击。

从12日晚开始,已经陆续有高校在其官方微博发布紧急通知,大连海事大学官微发布,“‘永恒之蓝’会扫描开放445文件共享端口的windows机器,无需用户任何操作,只要开机上网,不法分子就能在电脑和服务器中植入勒索软件、远程控制木马、虚拟货币挖掘机等恶意程序。”

360安全监测与响应中心透露,目前,国内平均每天有不低于5000台机器遭到“永恒之蓝”的远程攻击,并且攻击规模还有进一步扩大趋势。

### 南理工已封锁445端口

13日上午,现代快报记者从多所驻宁高校获悉,目前暂无高校受到攻击。但东南大学、南京理工大学、南京工程学院、南京信息职业技术学院等多所高校已经发布“关于防范ONION勒索软件病毒攻击的紧急通知”。

445端口是什么,为何会成为此次网络攻击的靶点?南京理工大学信息处副处长李华峰介绍,互联网端口有6万多个,445端口只是其中的一种,这就相当于学校有许多校门,网络信息通过这些“门”进出校园。而这种蠕虫,现在就在没有对445端口进行严格访问控制的中国教育研究网和企业内网大量传播。它们可以通过445端口,非法获取文件权限,并为之加密,如果用户不能按时支付解密赎金,将遭遇数据被销毁等隐患。

“目前南理工还没有接到遭遇攻击的反馈,但是我们已经把445端口封禁了,这意味着病毒无法出入校园网了。”李华峰说。

李华峰建议,当务之急是监测电脑是否存在漏洞、下载安装补丁。目前微软已针对Win7/Win8/Win10发布补丁MS17-010修复了“永恒之蓝”攻击的系统漏洞。除了广大师生,社会用户也应尽快根据各自操作系统安装补丁,地址:https://technet.microsoft.com/zh-cn/library/security/MS17-010。

此外,国家网络与信息安全信息通报中心也发布紧急通报,要求广大计算机用户尽快升级安装补丁,已感染病毒机器请立即断网,避免进一步传播感染。