



德国，一处电子时刻表遭到病毒攻击而无法工作。 ■ 据新华网

# 勒索病毒席卷全球 近百国家遭黑客攻击 病毒武器源自美国国安局

## 恶意勒索

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时间内支付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。

## 多国遭殃

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。

## 英国小伙意外拯救世界 8.29镑阻止勒索病毒蔓延

据新华社电 全球近百个国家和地区12日遭受勒索软件攻击，英国公共卫生体系、法国第二大汽车制造商雷诺集团等均受波及。不过，这种软件并非没有弱点，英国一名年轻网络工程师13日“无意中”阻拦了勒索软件的疯狂传播。

英国媒体13日报道，这名22岁的英国网络工程师12日晚注意到，这一勒索软件正不断尝试进入一个极其特殊、尚不存在的网址，于是他顺手花8.5英镑（约合75元人民币）注册了这个域名，试图借此网址获取勒索软件的相关数据，了解传播范围。令人不可思议的是，此后勒索软件在全球的进一步蔓延竟然得到了阻拦。

他和同事分析，这个奇怪的网址很可

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。俄罗斯媒体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%。

## 美国挨批

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。

不少网络安全专家指责，美国斥巨资研发黑客攻击工具、而非自卫机制，结果造成全球网络环境“更不安全”。

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。

得知最新攻击事件后，“棱镜”监听项目曝光者、美国前防务承包商雇员斯诺登12日发推文说，“尽管多次被警告，（美国国安局）仍然研制了危险的攻击工具。今天，我们见到代价……医院里的病人生命受到威胁”。面对批评，美国国安局尚未作出回应。

能是勒索软件开发者为避免被网络安全人员捕获所设定的“检查站”，而注册网址的行为无意触发了程序自带的“自杀开关”。也就是说，勒索软件在每次发作前都要访问这个不存在的网址，如果网址继续不存在，说明勒索软件尚未引起安全人员注意，可以继续在网上畅行无阻；而一旦网址存在，意味着软件有被拦截并分析的可能。在这种情况下，为避免被网络安全人员获得更多数据甚至反过来加以控制，勒索软件会停止传播。

这位年轻的工程师在推特发帖说：“我坦白，在我注册这个域名之前，完全不知道它能停止这次恶意软件的传播。事情的开始完全是个意外！”

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”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。

# 想哭肆虐全球哭了

## 我国情况

### 清华北大等高校学生 毕业论文被大面积摧毁

记者获悉，由于全球多个国家爆发勒索病毒攻击，中国校园网也成为重灾区，包括清华、北大、上海交大、山东大学等全国各地众多院校出现病毒感染情况，大量学生毕业论文等重要资料被病毒加密，只有支付赎金才能恢复。

据当天360安全卫士紧急公告，不法分子使用NSA（美国国家安全局）泄露的黑客武器攻击Windows漏洞，使ONION、WNCRY等勒索病毒在校园网快速传播感染，部分企业甚至包括一些基础设施的隔离内网也遭遇攻击，建议电脑用户尽快使用360“NSA武器库免疫工具”预防病毒。

360首席安全工程师郑文彬介绍说，此次勒索病毒是由NSA泄露的“永恒之蓝”黑客武器传播的。“永恒之蓝”可远程攻击Windows的445端口（文件共享），如果系统没有安装今年3月的微软补丁，无需用户任何操作，只要开机上网，“永恒之蓝”就能在电脑里执行任意代码，植入勒索病毒等恶意程序。

郑文彬表示，由于国内曾多次出现利用445端口传播的蠕虫病毒，部分运营商对个人用户封掉了445端口。但是教育网并无此限制，存在大量暴露着445端口的机器，因此成为不法分子使用NSA黑客武器攻击的重灾区。正值高校毕业季，勒索病毒已造成一些应届毕业生的论文被加密篡改，直接影响到毕业答辩。 ■ 据《北京晚报》

## 应对措施

### 如何能预防电脑 被勒索病毒“绑架”？

在防范上，国内多家安全机构均提示，一是，及时更新Windows已发布的安全补丁。在3月MS17-010漏洞刚被爆出的时候，微软已经针对Win7、Win10等系统在内提供了安全更新；此次事件爆发后，微软也迅速对此前尚未提供官方支持的Windows XP等系统发布了特别补丁。

二是，在电脑上安装腾讯电脑管家、360安全卫士等安全类软件，并保持实时监控功能开启，可以拦截木马病毒的入侵。

Windows 7系统用户可打开控制面板点击防火墙-高级设置-入站规则-新建规则-勾选“端口”-点击“协议与端口”，勾选“特定本地端口”，填写445后点击下一步，继续点击“阻止链接”，一直下一步，并给规则命名，可完成关闭445端口。

中国国家互联网应急中心还建议，关闭445等端口（其他关联端口如：135、137、139）的外部网络访问权限，在服务器上关闭不必要的上述服务端；加强对445等端口（其他关联端口如：135、137、139）的内部网络区域访问审计，及时发现非授权行为或潜在的攻击行为；由于微软对部分操作系统停止安全更新，建议对Window XP和Windows server 2003主机进行排查（MS17-010更新已不支持），使用替代操作系统；做好信息系统业务和个人数据的备份。 ■ 据中新社

## 彩票开奖台

全国联网电脑体育彩票“7星彩”  
第17055期开奖公告  
本期开奖结果：2451944

全国联网电脑体育彩票“排列3”开奖公告  
第17127期

中奖号码：739

全国联网电脑体育彩票“排列5”开奖公告  
第17127期

中奖号码：73949

“安徽风采”电脑福利彩票25选5玩法  
开奖公告第2017127期

中奖号码：12、15、22、23、24

中国福利彩票15选5玩法开奖公告  
第2017127期

中奖号码：04、06、08、11、13

中国福利彩票3D玩法

第2017127期中奖号码：623

中国福利彩票“双色球”开奖公告

第2017055期中奖号码：

红色球号码07、12、13、20、24、31

蓝色球号码：05