“史上最大规模”勒索病毒席卷全球

国内高校成病毒攻击重灾区,有消息称病毒武器源自遭泄密的美国国安局

从5月12日开始，包括中国在内的全球近百个国家和地区部分电脑遭遇同一类勒索病毒的攻击。记者了解到，目前安全机构暂未能有效破除该勒索软的恶意加密行为，用户只能进行预防，用户中毒后可以通过重装操作系统的方式来解除勒索行为，但用户重要数据文件不能直接恢复。

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。

【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WannaCry（“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。”

【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。英国首相特雷莎·梅当天说，英国国家网络安全中心正与国民保健制度联手应对这次危机。

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%。另一名消息人士称，俄政府文件未在此次攻击中泄密。

【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爱德华·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。

【国内情况】

13日，中国国家互联网应急中心发文称，互联网上出现针对Windows操作系统的勒索软件的攻击案例，勒索软件利用此前披露的Windows SMB服务漏洞(对应微软漏洞公告：MS17-010)攻击手段，向终端用户进行渗透传播，并向用户勒索比特币或其他价值物。

腾讯反病毒实验室接受记者采访时也表示，这是最近几年极为流行的、依靠强加密算法进行勒索的攻击手段。与之前的攻击不同的是，此次勒索病毒结合了蠕虫的方式进行传播，传播方式采用了前不久美国国家安全局(NSA)被泄漏出来的MS17-010漏洞，因此无需受害者下载、查看或打开任何文件即可发动攻击。

中国国家互联网应急中心还表示，勒索软件的攻击涉及到国内用户(已收到多起高校案例报告)，已经构成较为严重的攻击威胁。

从5月12日晚间起，中国多个高校的师生陆续发现自己电脑中的文件和程序无法打开，而是弹出对话框要求支付比特币等赎金后才能恢复。

记者注意到，山东大学、南昌大学、广西师范大学、东北财经大学、电子科技大学中山学院在内十几家高校发布遭受病毒攻击的通知，提醒师生注意防范。

部分高校通知称，近期国内多所院校出现ONION勒索软件感染情况，磁盘文件会被病毒加密为.onion后缀，只有支付高额赎金才能解密恢复文件，对学习资料和个人数据造成严重损失。根据网络安全机构通报，这是不法分子利用NSA黑客武器库泄漏的“永恒之蓝”发起的病毒攻击事件。

腾讯反病毒实验室认为，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。

【快打补丁】

据360安全中心分析，此次勒索病毒是由NSA泄漏的“永恒之蓝”黑客武器传播的。监测数据显示，国内首先出现的是ONION病毒，平均每小时攻击约200次，夜间高峰期达到每小时1000多次；WNCRY勒索病毒则是5月12日下午新出现的全球性攻击，并在中国的校园网迅速扩散，夜间高峰期每小时攻击约4000次。

针对NSA黑客武器利用的Windows系统漏洞，微软在今年3月已发布补丁修复。此前360安全中心也已推出“NSA武器库免疫工具”，能够一键检测修复NSA黑客武器攻击的漏洞；对XP、2003等已经停止更新的系统，免疫工具可以关闭漏洞利用的端口，防止电脑被NSA黑客武器植入勒索病毒等恶意程序。

计算机安全专家建议：立即关闭Windows系统的445端口：打开控制面板——网络和共享中心——更改适配器设置——右键点击正在使用的网卡然后点击属性——取消勾选Microsoft网络文件和打印机共享——确定——重启系统。同时，尽快升级系统安装补丁，Windows 2003和XP没有官方补丁，用户可打开并启用Windows防火墙，进入“高级设置”，禁用“文件和打印机共享”设置；或启用个人防火墙关闭445以及135、137、138、139等高风险端口。已感染病毒机器请立即断网，避免进一步传播感染。此外，应尽快备份电脑里的重要资料。

综合新华社消息

认尸启事

2017年5月4日,在衡阳市珠晖区粤汉码头处湘江河内发现一男婴死者。死者全身赤裸。有知情者或者亲属见到启事后速与珠晖公安分局刑侦大队联系。

联系电话:18944991720

衡阳市公安局珠晖分局刑侦大队