莫放松！勒索病毒变种袭来

中央网信办：病毒还在传播，但速度已放缓

自5月12日起，在全球大范围内爆发的勒索病毒“WannaCry（想哭）”对我国互联网络也构成了严重安全威胁。中央网信办网络安全协调局负责人15日表示，该勒索病毒仍在传播，但速度已明显放缓，对广大用户而言最有效的应对措施是要安装安全防护软件，及时升级操作系统和各种应用的安全补丁。

勒索病毒大规模爆发

12日晚，由于受到勒索病毒波及，中石油部分加油站出现了加油卡、银行卡、第三方支付等网络支付无法使用的状况。

记者从国家互联网应急中心获悉，这种名为“WannaCry”的病毒属于蠕虫式勒索软件，通过利用编号为MS17-010的Windows漏洞（被称为“永恒之蓝”）主动传播感染受害者。

“北京时间5月12日20时左右，该勒索病毒在全球范围内大规模爆发，受到影响的国家达上百个。”国家互联网应急中心博士、工程师韩志辉说。

截至14日10时30分，国家互联网应急中心已监测到约242.3万个IP地址遭受“永恒之蓝”漏洞攻击；被该勒索软件感染的IP地址数量近3.5万个，其中中国境内IP约1.8万个。另监测发现5471个IP连接“WannaCry”蠕虫病毒的内置域名及IP，表明可能已感染该病毒，IP主要分布在中国内地的广东、浙江、北京和上海等地。

大量行业企业内网感染

韩志辉告诉记者，被该勒索软件入侵后，用户主机系统内的文件会被恶意加密，并会在桌面弹出勒索对话框，要求受害者支付价值数百美元的比特币到攻击者的比特币钱包，且赎金金额还会随着时间的推移而增加。

“一旦中招，用户主机系统内的照片、图片、文档、压缩包、音频、视频、可执行程序等几乎所有类型的文件都将被加密，加密文件的后缀名被统一修改为‘.WNCRY’。”猎豹移动安全专家李铁军说，由于该病毒使用RSA非对称算法，没有私钥就无法解密文件。

韩志辉表示，目前网络安全业界暂未能有效破除该勒索软件的恶意加密行为，用户主机一旦被勒索软件渗透，只能通过重装操作系统或使用专杀工具的方式来清除勒索软件，但若用户重要数据文件没有备份，则很难完全直接恢复。

监测发现，国内大量行业企业内网遭到感染，包括教育、企业、医疗、电力、能源、银行、交通等多个行业受到不同程度的影响。

随着5月15日本周第一个工作日的到来，国内继续有多地的公共服务部门被曝出电子设备遭上述勒索病毒侵袭的消息。其中，中西部多个省份的交管部门都受到上述病毒影响，部分业务暂停办理。包括成都在内，四川多地交管、户籍等民生服务系统受到病毒影响，正在紧急维护或处置。山西全省11市大部分交管业务停办。

国家互联网应急中心博士、高级工程师高胜表示，该勒索软件对于企业局域网或内网的主机系统破坏性尤其严重。“由于大量内网主机没有及时更新补丁或使用XP系统，因此一旦有一台主机被感染，将造成网内大规模扩散。”高胜说，我们已接到或看到了多个社会重要信息系统受攻击瘫痪的情况。

病毒出现多个变种

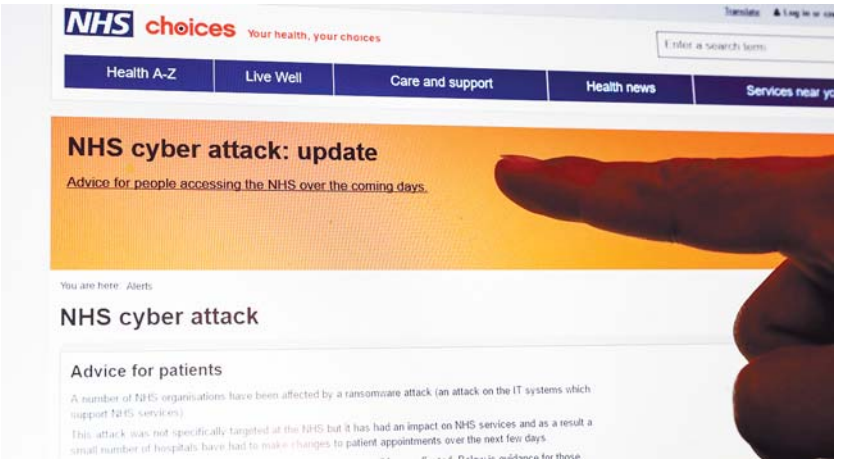
15日一早到单位后，赖女士就按照网上发布的病毒防范指南“拔网线、倒数据、安补丁”，防止自己的电脑中招。记者了解到，除了个人加强防范外，多家单位也给员工发出了安全防范操作提示。

“目前，该勒索软件还在传播，但传播速度已经明显放缓。”中央网信办网络安全协调局负责人表示，事件发生后，我国公安、工信、教育、银行、网信等有关部门都对防范工作提出要求。奇虎360、腾讯、安天、金山安全等相关企业迅速开展研究，主动提供安全服务和防范工具。各相关媒体做了大量报道，对提高全社会的防范意识、遏制勒索软件发挥了重要作用。

“此次勒索软件较大范围传播是近年来少有的，再一次给人们敲响了警钟，互联网等信息技术的快速发展，在给人们带来巨大福祉的同时，也带来了前所未有的网络安全挑战。”该负责人建议，各方面都要高度重视网络安全问题，及时安装安全防护软件，及时升级操作系统和各种应用的安全补丁，设置高安全强度口令并定期更换，不要下载安装来路不明的应用软件，对特别重要的数据采取备份措施等。

国家网络与信息安全信息通报中心15日监测发现，WannaCry勒索病毒出现多个变种，如开关域名变化、收钱地址变化等，但主要的传播机制和破坏方式没有改变，威胁依然存在。建议用户要加强安全意识，做好安全措施。

国家互联网应急中心表示，后续将密切监测和关注该勒索软件的攻击情况，同时联合安全业界对有可能出现的新的攻击传播手段、恶意样本进行跟踪防范。 **据新华社、澎湃等综合整理**



□新华社发

这是5月15日英国公共卫生体系（NHS）网站上关于网络袭击事件的说明。

微软怒斥美政府囤积病毒武器

全球追查难锁定黑客身份，相关调查仍在初始阶段

美国微软公司5月14日发表声明，谴责美国政府囤积电脑病毒武器，一旦发生泄露，便在全球范围造成严重威胁。

自12日以来，名为“想哭”的勒索软件袭击全球150多个国家和地区，而该病毒便是源自美国国家安全局遭泄露的病毒武器库。专家警告称，今后数日要谨防升级版病毒再度袭来。

如“战斧”导弹失窃

微软总裁兼首席法务官布拉德·史密斯14日经博客发布一份声明，谴责美国政府部门囤积黑客攻击工具的做法。“我们以前见过美国中央情报局储存的有关（电脑网络）弱点的各种情报遭维基揭秘网站曝光。如今，美国国家安全局储存的这类情报失窃，以致影响全球各地的电脑用户。”史密斯说。

英国广播公司报道，“想哭”病毒12日袭来，迄今已有150多个国家和地区的超过20万台电脑“中招”，影响领域包括政府部门、医疗服务、公共交通、邮政、通信、汽车制造业等。包括微软在内，业界人士的共识是：该病毒来源于美国国安局的病毒武器库，上个月遭泄密而公之于众。

按照史密斯的说法，“若用传统武器打比方，这次事件相当于美国军方的‘战斧’巡航导弹失窃”。因此，这次病毒袭击应该给全球各国“敲响警钟”。

有媒体报道说，这次勒索软件攻击是美国国安局开发的网络武器被“民用化”的全球首例。一些信息安全专家指出，如果国安局在发现“视窗”的安全漏洞时就向微软披露，而不是据此开发黑客工具，那么这次大规模网络攻击可能就不会发生。

对于微软方面的指责，美国国安局和白宫方面目前均未作出回应。

谨防新一轮攻击

史密斯14日特别提醒，全球电脑用户应立即安装系统更新包，及时给电脑打补丁。微软3月已发布针对此类勒索软件的补丁，但许多用户迟迟没有安装。“网络犯罪分子越来越老谋深算，电脑用户简直防不胜防，除非他们及时更新电脑系统，”史密斯说。

作为一款勒索软件，“想哭”侵入电脑后，会锁住用户的文件，然后要求用户支付300美元至600美元的赎金以换回文件。据英国广播公司的跟踪分析，在12日病毒袭击中，黑客已收到至少约2.8万美元的赎金。

12日的病毒扩散已经得到有效遏制，但不少电脑专家提醒仍不能掉以轻心。欧盟刑警组织认为，黑客组织已经开发出升级版病毒，或于今后数日发动新一轮攻击。

英国网络安全公司“数字阴影”的电脑专家贝姬·平卡德告诉法新社记者，对黑客而言，修改代码以再次发动病毒攻击简直易如反掌，“即使星期一（意指15日）没有遭遇新一轮攻击，预计很快也会发生”。

全球追查幕后黑手

目前，全球多国都在追查“想哭”病毒背后的黑客组织，以便将其绳之以法。

在12日病毒袭击中，俄罗斯内务部、卫生部、俄罗斯储蓄银行、铁路系统均报告受到攻击。英国公共卫生体系国民保健制度受到严重影响，不少病人无法就医，甚至连手术、化疗等都被取消。此外，印度尼西亚的数家医院、美国联邦快递公司、西班牙电话公司、法国雷诺汽车公司工厂、挪威和瑞典的几家足球俱乐部等也遭遇病毒袭击。

据美国网络安全专家赫斯分析，虽然这次袭击影响范围极广，但具体犯罪手法“单一、不复杂”，更像是“业余选手”所为。眼下，美国、英国、俄罗斯等国都在追查这次袭击的幕后黑手。一名不愿公开姓名的美国高级官员透露，美国总统唐纳德·特朗普12日当晚下令召集一次紧急会议，联邦调查局、国安局随后联手展开调查。

据路透社报道，相关调查都在初始阶段，而锁定黑客身份的难度相当大。

据新华社综合整理

揭秘

黑客为啥将比特币作为赎金

本次勒索病毒幕后黑客索要的赎金是比特币。据悉，到北京时间5月14日上午，1个比特币的价值已升至1805美元（约合12450元人民币），年涨幅高达267%。

为什么黑客选择比特币为支付赎金？有专家指出，首先，比特币有一定的匿名性，便于黑客隐藏身份；其次它不受地域限制，可以全球范围收款；同时比特币还有“去中心化”的特点，可以让黑客通过程序自动处理受害者赎金。此外，相比于其他数字货币，比特币目前占有最大的市场份额，具有最好的流动性，所以成为黑客的选择。比特币还被利用来洗钱和进行资产非法转移，用本国货币买入比特币，在国外交易平台上卖出，再以美元取出，几分钟就可以完成资产转移。 **央视**