“勒索”继续！今天是一个考验关口

网络安全专家称，用户最好断网开机

一个名为“想哭”(WannaCry)的勒索软件从12日起袭击了全球近百个国家和地区使用微软视窗操作系统的电脑。欧盟刑警组织说，这次网络病毒袭击“达到史无前例的级别”。全球受此次网络攻击影响的国家和地区单单用于修复漏洞的花费就将高达数千万美元，而全球的损失则不可估量。

我国教育、银行、交通等多个行业也遭受不同程度影响。网络安全专家指出，许多网络用户特别是中国用户仍面临风险关口。建议用户要断网开机，即先拔掉网线再开机，这样基本可以避免被勒索软件感染。

综合 新华社、央视

最新消息

今天是考验关口 用户最好断网开机

记者14日从国家互联网应急中心获悉，“WannaCry”病毒属于蠕虫式勒索软件，通过Windows漏洞（被称为“永恒之蓝”）主动传播感染受害者。

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。

国家互联网应急中心建议广大用户及时更新Windows已发布的安全补丁，关闭445、135、137、139等端口（可以认为是计算机与外界通讯的出口）的外部网络访问权限，加强这些端口的内部网络区域访问审计；安装并及时更新杀毒软件；不要轻易打开来源不明的电子邮件；定期在不同存储介质上备份信息数据。

“15日是重要考验关口”，360公司首席安全工程师郑文彬强调。由于时区关系，中国将是较早面临这个风险的国家。

安天公司安全研究与应急处理中心主任李柏松同样判断：“勒索软件网络攻击大规模爆发于北京时间12日晚8点左右，当时国内有大量机构和企业的网络节点已关机，因此15日开机将面临安全考验。”他还说，许多重要的计算机系统处于内网环境，无法访问前述域名，并且也可能无法及时更新安全补丁，因此仍可能面临较大风险。

网络安全专家建议，用户要断网开机，即先拔掉网线再开机，这样基本可以避免被勒索软件感染。开机后应尽快想办法打上安全补丁，或安装各家网络安全公司针对此事推出的防御工具，才可以连网。

“勒索”未来仍可能持续

网络安全专家都在严阵以待15日这个关口。那么，假如过了这个关口，今后又会怎么样？郑文彬认为：“这个勒索软件的攻击未来应该还会持续一段时间。”

“一些不法黑客还可能受到此次勒索软件攻击的启发，将更多技术手段与勒索软件相结合，”李柏松说，“勒索模式带动蠕虫病毒的回潮不可避免，黑客可能利用僵尸网络分发病毒，还可能针对物联网设备的漏洞制造和传播病毒软件，这些问题都会出现。”

比特币的兴起也为勒索软件提供了帮助。比特币是一种虚拟货币，在网上交易难以追踪，成为许多黑客爱用的交易媒介。在此次事件中，就有用户因一台电脑被感染而被勒索5个比特币，目前约合人民币5万元。

此次勒索软件威胁的不仅是个人用户，还有众多机构和企业。专家因此提醒，所有网络用户今后都应加强安全意识，注意更新安全补丁和使用各种杀毒工具。

光漏洞修复就将花数千万美元

美国著名软件公司赛门铁克公司研究人员13日预计，全球受此次网络攻击影响的国家和地区单单用于修复漏洞的花费就将高达数千万美元，而全球的损失则不可估量。

赛门铁克公司研究人员表示，修复漏洞中最昂贵的部分是清空每台受攻击的电脑或服务器的恶意软件，并将数据重新加密。单单此项内容就将花费高达数千万美元。

据路透社报道，软件公司关于修复漏洞的高额损失并没有包含受影响的企业所遭受的损失。

13日，受此次网络攻击影响的汽车生产商“雷诺”公司就表示，他们将暂停全球多个地区的汽车生产任务，以阻止该恶意软件通过公司内部系统传播。除了雷诺公司以外，受影响的企业还有汽车生产商“日产”公司、国际快递公司“联邦快递公司”以及欧洲数家大型电信公司等等。预计损失无法估量。

元凶难查

欧盟刑警组织称该袭击“史无前例”

欧盟刑警组织说，这次网络病毒袭击“达到史无前例的级别”，要找到元凶需要进行复杂的国际调查。

“想哭”进入电脑后，会锁住用户的文件，要求用户支付赎金以换回文件。多家网络安全企业认定，“想哭”源自几周前遭泄密的美国国家安全局病毒武器库。

微软3月就已发布针对此类勒索软件的补丁，但许多用户尚未安装。13日，微软宣布这一补丁完全免费使用，所有用户都可下载安装。

目前，俄罗斯受该病毒的攻击次数最多。俄罗斯卡巴斯基实验室和捷克网络安全企业爱维士公司均认为，此次受攻击最严重的是俄罗斯。俄内务部、卫生部、俄罗斯储蓄银行、铁路系统均报告受到攻击。内务部1000台电脑被攻击，但发言人说没有造成泄密；卫生部说攻击“被有效压制”；俄央行说，银行机构的数据没有泄露；俄铁路系统表示，铁路运行未受到影响。

英国公共卫生体系国民保健制度（NHS）则受到严重影响。该国的技术专家13日仍在忙碌，以尽快恢复NHS的运转。

英国媒体报道，大部分公共医疗组织的电脑操作系统陈旧，没有安全更新程序。

受此次病毒攻击影响的还包括中国的一些校园网络、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、日产汽车公司位于英国的工厂、法国雷诺汽车公司工厂、挪威和瑞典的几家足球俱乐部等。

意外之喜

英国小伙一个小举动 阻拦勒索软件疯狂传播

全球近百个国家和地区从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，可以继续在网络上畅行无阻；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，完全不知道它能阻止这次恶意软件的传播。事情的开始完全是个意外！”

不过，这名英国网络工程师和一些网络安全专家都表示，这种方法目前只是暂时阻止了勒索软件的进一步发作和传播，但帮不了那些勒索软件已经发作的用户，也并非彻底破解这种勒索软件，新版本的勒索软件很可能不带这种“自杀开关”而卷土重来，用户应当尽快更新电脑系统的安全补丁。

白鳍豚疑似重现长江

已“功能性灭绝”十年

5月14日上午，中国生物多样性保护与绿色发展基金会（以下简称“中国绿发会”）官方微博发消息称，14日早晨6:30，绿发会科考队在长江芜湖段“中华白鳍豚保护地”目击、拍摄、记录到两头疑似白鳍豚。

14日中午12:20，中国绿发会官微再发消息称，科考队顾问华元渝对这两头白鳍豚的出现作出认定，甚至直接使用了“我看了，绝对是”的表述，随后又表示“图像很清晰！无须开会、可以发布。若有异议视频为证。”资料显示，华元渝曾是武汉中科院水生所的教授，长期关注白鳍豚的生存状态。

截至记者发稿，尚未有其他淡水豚专家对绿发会的该发现作出其他认定。

白鳍豚于2007年被宣布功能性灭绝，与江豚一样，是长江中的淡水鲸类。专家指出，功能性灭绝与完全灭绝不同，不排除长江里还有少量个体生存。

事实上，白鳍豚功能性灭绝后，曾有多次媒体报道出现疑似白鳍豚，却始终没有确凿证据。

14日中午，中国绿发会白鳍豚科考队工作组工作人员苏菲向记者还原了整个发现过程：5月14日上午五点五十八分，科考队开启了考察取证工作。起初，科考队员发现了江豚跃出江面的情景，随即摄像拍照跟随江豚“而上”，随着江豚两三个，四五个一群的情景多次出现，科考队员当机立断地登上小型快艇，贴近拍摄。

六点十几分，科考队三次发现、看到“白鳍豚”拱型跃出水面并露出鳍背的情景，由于所在位置接近长江主航道，且豚的群体也向主航道驶近，科考队员担心惊扰豚群，以及主航道大轮船给豚群带来伤害，科考队小艇立即返回出发点。

据中科院水生所博士郝玉江介绍，白鳍豚体色青白，有背鳍，有一个长长的吻，体型要明显大于江豚，体态优雅。

苏菲也表示，长嘴和背鳍是白鳍豚的特征。脸颊至胸腹部是白色，但是受阳光反射或逆光影响，背部颜色看上去不一定是白的或者灰色的，也可能是黑的、棕色的，“白鳍豚出水是长吻先出水，接下来是背部、背鳍，每次出水，背鳍必定会露一下。出水动作优雅潇洒，非常温柔。白鳍豚个头明显大于江豚。” 综合