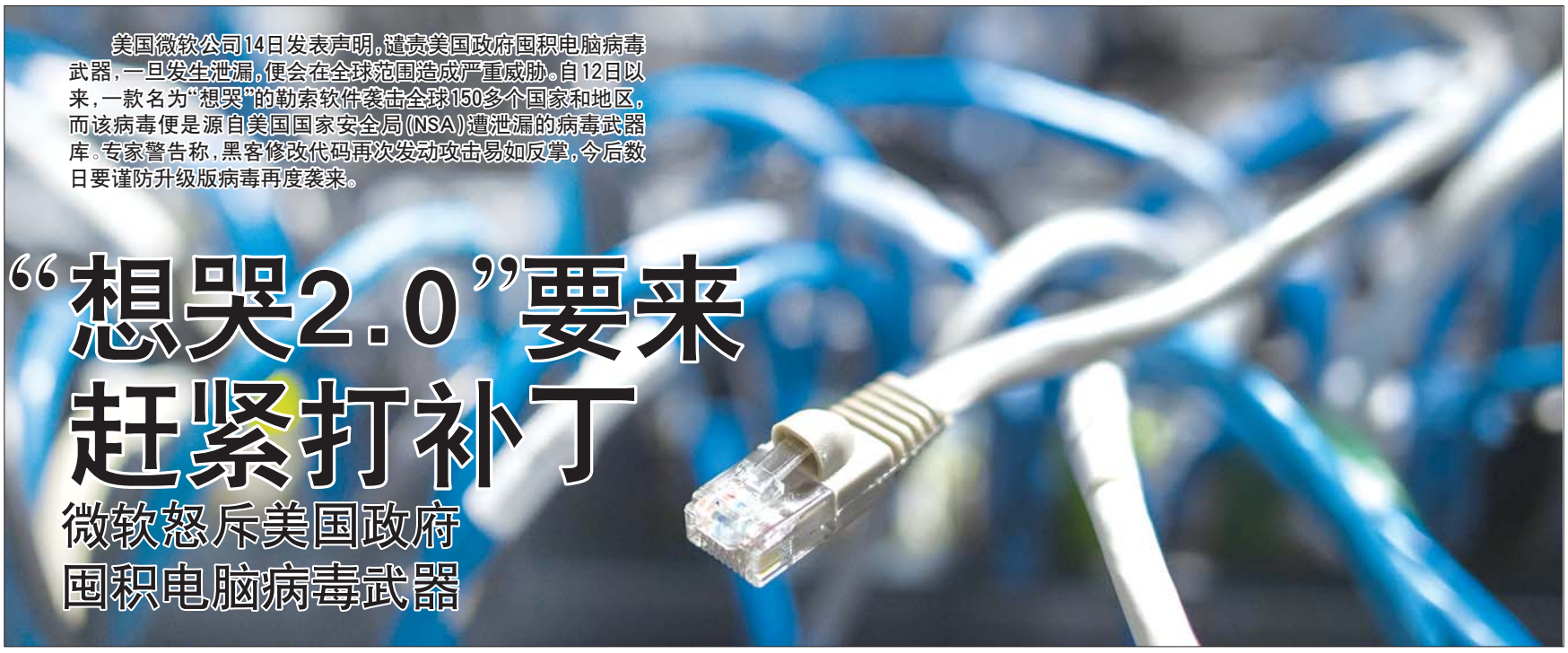

美国微软公司14日发表声明,谴责美国政府囤积电脑病毒武器,一旦发生泄漏,便会在全球范围造成严重威胁。自12日以来,一款名为"想哭"的勒索软件袭击全球150多个国家和地区,而该病毒便是源自美国国家安全局(NSA)遭泄漏的病毒武器库。专家警告称,黑客修改代码再次发动攻击易如反掌,今后数日要谨防升级版病毒再度袭来。

"想哭2.0"要来 赶紧打补丁

微软怒斥美国政府囤积电脑病毒武器

事件影响堪比"战斧"导弹失窃

微软总裁兼首席法务官布拉德·史密斯14日经由博客发布一份声明,谴责美国政府部门囤积黑客攻击工具的做法。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。

"我们以前见过美国中央情报局(CIA)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。

史密斯在谈到这次网络攻击的教训时说,这给世界各国政府敲响了警钟。最新攻击事件说明,当今世界面临的最严峻的两种网络安全威胁形式——国家行为和有组织犯罪行为发生关联。这种关联"出乎预期,令人担忧"。

他认为,各国政府应引以为戒,改变做法,在网络空间中也同样遵守物理空间中适用于武器监管的规则。政府应考虑储藏并利用安全漏洞可能对平民造成的损害。政府应向信息产品供应商报告所发现的安全漏洞,而不是储存、售卖和利用这些漏洞。

按史密斯的说法,"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,这次病毒袭击应给全球各国"敲响警钟"。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。

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。

相关工具被盗取和泄漏后,被犯罪分子用来对医院、企业、政府等方面的计算机发动攻击。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。

升级版病毒 这几天可能来袭

英国广播公司(BBC)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。欧盟刑警组织把这轮病毒攻击描述为"达到史无前例的级别"。

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2.2万英镑(约合2.8万美元)的赎金。美国Proofpoint电脑技术公司网络安全专家达里恩·赫斯说,这起袭击事件受关注度颇高,恐怕吸引更多黑客争相效法以非法获利。

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。

12日的病毒扩散已得到有效遏制,但不少电脑专家提醒仍不能掉以轻心。欧盟刑警组织认为,黑客组织已开发出升级版病毒,或于今后数日发动新一轮攻击。一名参与遏制病毒扩散的英国电脑专家曾预测,"想哭2.0"可能最早于15日来袭,而升级版病毒将更难杀灭。

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易如反掌,"即使周一(意指15日)没有遭遇新一轮攻击,预计很快也会发生"。

眼下,美国、英国、俄罗斯等国都在追查这次袭击的幕后黑手。一名美国高级官员透露,美国总统特朗普12日晚下令召集一次紧急会议,联邦调查局(FBI)、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。

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。

综合新华社消息