

中国网友笑对“勒索”病毒 黑客看到后大概会气吐血

15日是病毒爆发后中国的第一个工作日,勒索病毒带来的最大规模的考验也拉开帷幕。虽然勒索病毒尚未终止,但来自中央网信办的最新消息说,它的传播速度已经明显放缓。

网友调侃“勒索”病毒

新的周一,新的工作日,大家上班第一件事是做什么?这一天的工作流程是先拔网线后开电脑。

然而,我们的上班党和学生党在微博中呈现的内容却是这样:有人一点都不害怕,他们希望自己的电脑中毒,不然不好意思让老板换新的电脑。还有人拿出了自己的独门绝招应对病毒,让生物老师看了想打人!我们高中生物老师说过,任何病毒在高温下都无法生存,所以把病毒感染的电脑放在水里煮上一会就没事了。还有人希望通过断电关机把病毒饿死,对于不想上班的你,这个理由大概能让老板无言以对了。甚至还有人开始吐槽自己公司电脑配置低:这简直就是对病毒的侮辱,因为电脑配置太低病毒带不起来,刚蹦出付费页面就显示该程序无响应。

如果这些理由被黑客看到,大概会气吐血吧。

北京三部门: 勒索蠕虫已出现新变种

吐槽归吐槽,不可否认的是互联网病毒是全人类的公敌,造成的影响还是很严重的。

据央视新闻消息,截至5月13日晚8点,我国共39730家机构被新型“蠕虫”式勒索病毒感染!感染该病毒后,不到十秒,电脑里所有文件全被加密无法打开,只有按弹窗提示交赎金才能解密。

值得我们注意的是,这场上周末掀起的“勒索病毒”风波仍在“肆虐”。不过,来自中央网信办的消息称,目前,该勒索软件虽然还在传播,但传播速度已经明显放缓。

据中新网,欧洲刑警组织指出,至欧洲时间14日早上,多达150个国家的20万台电脑遭“想哭”勒索病毒侵害。预计到15日,人们返回公司上班,这一数字还会进一步增加。

有报道称,一些网络安全专家指出,到14日早上,“想哭”(WannaCry)病毒的侵害速度已经放慢,但是,这一停歇时段是短暂的。

5月13日,发现了诡异域名注册即可中止病毒程序的安全工程师也坦白承认,这是个美丽的巧合,同时提醒需要为电脑打上补丁,以免病毒变种,绕过这一域名,发动下一波攻击。

北京市委网信办、北京市公安局、北京市经信委联合发出《关于WannaCry勒索蠕虫出现变种及处置工作建议的通知》。《通知》同样指出,WannaCry勒索蠕虫已经出现新变种,并给出了具体处理建议。



制造出这个病毒的祸根,竟然是他们!

据媒体报道,这个病毒的发行者是利用了去年被盗的美国国家安全局(NSA)自主设计的 Windows 系统黑客工具永恒之蓝(Eternal Blue),把今年2月的一款勒索病毒进行升级后的产物,被称作 WannaCry。

该病毒使用了从美国国家安全局(NSA)发现并泄露“永恒之蓝”(EternalBlue)漏洞,能利用445端口主动攻击并传染网络上的电脑,只要网络中有一台中毒,其他电脑只要联在同一网络上就可能中毒!

然而,美国政府从来没有承认过此事。但美国的前情报人员表示,这些病毒程序确实是美国国家安全局研发出来入侵和锁定别国电脑系统的。

目前,单位局域网、专网、内网大多数没有关闭445端口,只要内网中有一台电脑中招,其他电脑开机在网上就可能会中毒!

又是谁从美国国家安全局手里 偷走了病毒程序

据每日经济新闻援引外媒报道,网络专家称,美国国家安全局曾记载勒索软件通过利用微软软件漏洞进行攻击。这份文件被叫做影子经纪人(Shadow Brokers)的犯罪团伙偷走并于4月公布于众。在这份文件泄露之前,微软公司于3月发布重要补丁修复该漏洞,但显然该补丁的效果并不显著,使得仍有大量电脑处于保护之外。

假如这次事件明确指向美国国家安全局的渗透武器泄露事件,那么此次大规模病毒肆虐恐怕很难被定义为孤立事件。

而更有可能是,此次事件与之前著名的黑客组织“影子经纪人(Shadow Brokers)”攻破NSA黑客武器库,导致大量基于Windows系统漏洞的黑客工具流失事件有关。这次流散出的工具绝不仅仅是“永恒之蓝”一种或一个类型。其中隐含的未知风险,也许比目前大众判断的更加惊人。

链接

中招了怎么办?

这个比特币勒索病毒,处理方法其实网上都说得差不多了,无非就是赶快打补丁和堵端口,微软史无前例地给已经退休多时的xp出了应急补丁,至于这次事件有多严重,不再赘述。

16日,中央网信办网络安全协调局负责人就“蠕虫”式勒索软件攻击接受媒体采访时表示,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。

■来源:中国青年报、综合央视新闻、国家网络与信息安全通报中心等



关注三湘都市报微信
看E报。

