

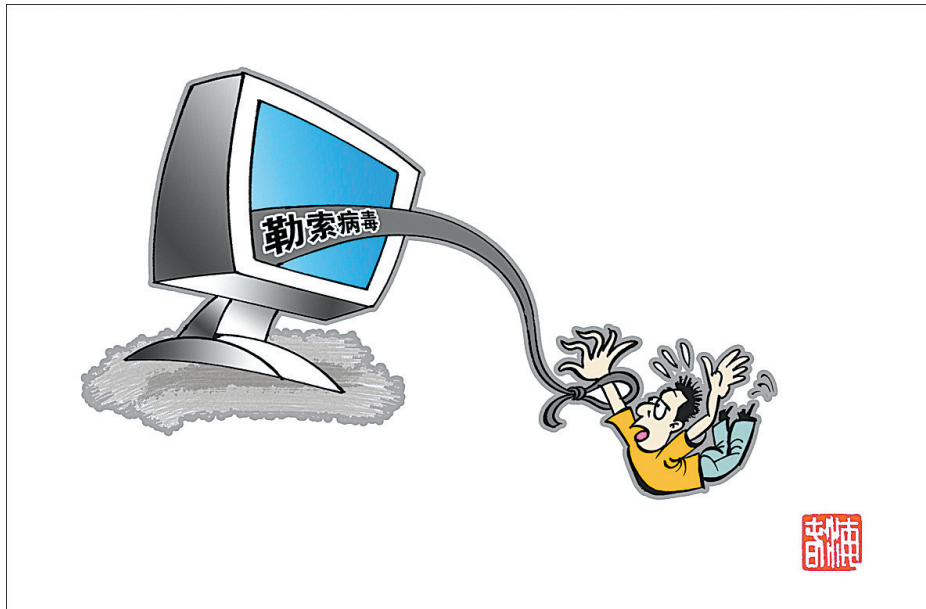
勒索病毒软件感染速度放缓

意外遏制勒索病毒的英国小伙3天睡5小时阻击新攻击

阅读提示

近日,全球多个国家遭受勒索病毒软件的攻击。这种病毒软件“想哭”主要针对微软“视窗”操作系统的一个漏洞发起攻击,电脑被感染后文件会被加密锁定,弹出勒索页面并索要赎金。

22岁的英国IT专家马库斯·哈钦斯因周末意外地破解来势凶猛的勒索软件的“命门”,帮助全球至少10万台电脑躲过这波病毒攻击。哈钦斯因而突然在网上多了许多粉丝,并收到许多科技公司的任职邀请。



“勒索”

新华社发 商海春 作

日说,5月12日开始的勒索软件网络袭击共获利近7万美元,据美方所知,支付赎金并未导致任何数据恢复。博塞特当天在白宫记者会上说,这款勒索软件“在周末期间,感染速度已经放缓”。

英国小伙还在阻止新攻击 卡巴斯基:感染病毒只能重装系统

正在与英国政府合作、加班加点与黑客斗智的哈钦斯警告说,勒索病毒软件“想哭”的新变种将修正被他识破之处,随着5月15日许多人回到工作岗位,可能将有更多电脑面临被勒索的威胁。

哈钦斯热爱冲浪,与父母和弟弟生活在英格兰一个海滨小镇。高中毕业后他学分不佳,没有继续深造。他的科技博客内容被一家总部在美国洛杉矶的网络安全公司相中后,他便开始在家中为其工作。他并非在工作时成功阻拦勒索软件的传播,当时,他其实正在休假。

英国媒体报道,5月12日晚,哈钦斯注意到,一款勒索软件正不断尝试进入一个并不存在的网址,于是他花8.5英镑(约合75元人民币)注册了这个域名。他告诉英国《每日邮报》,他知道借此网址可以获取勒索软件的相关数据,了解传播范围。但不可思议的是,此后“想哭”在全球的蔓延得到大幅控制。

英国《每日邮报》网站5月14日报道,哈钦斯过去72个小时只睡了5小时,其余时间差不多都在与这波网络攻击作战。在此期间,他的推特账号粉丝数涨了两万,他的推特信箱内收到数千封信。他的公司嘉奖他到洛杉矶游玩。同时,他收到许多公司提供的工作机会。

不过,他目前可考虑不了那么多,他还在与英国国家网络安全中心合作,试图阻止“想哭”变种在工作日的大爆发。他在推特上向网友给出具体建议,并坦言“我很可能无法制止下一个……我们可能无法阻止它,所以我得随时待命”。

哈钦斯此前一直没有暴露自己的身份。他担心,真实身份被曝光后,他将遭到勒索软件幕后黑客的报复。他对《每日邮报》说:“如果未来一些人想报复,他们在几秒钟内就能找到有关我的信息。如果他们知道我的住址,他们可以为我所欲为。”

俄罗斯卡巴斯基实验室北京时间昨天表示,及时下载正规补丁程序,确保全面启用最新升级的防护软件,可防止名为“想哭”的勒索病毒侵入电脑。但如果电脑已被这种病毒感染,目前只能重装系统来继续使用电脑,被“绑架”的文件将会丢失。(宗禾)

国内进展: 教育网辟谣“高校重灾区” 券商系统未发现感染

针对网传“中国此次遭受攻击的主要是教育网用户”消息,中国教育和科研计算机网CERNET网络中心5月15日发布声明称,“教育网并未出现大规模感染勒索病毒‘想哭’的现象,也不是重灾区。”

据不完全统计,截至5月14日中午,在近1600个高校用户中,确认感染病毒的高校仅66所,占比4%,仅涉及数百个IP地址。由于连接教育网的各高校校园网大多采用多出口模式,在被病毒感染的66所高校中,通过教育网感染病毒的高校仅有5所,通过其他运营商网络感染病毒的高校39所,无法确定感染病毒途径的高校22所。

昨天上午,《法制晚报》记者从北京国泰君安、大同证券、中信建投证券等多家券商交易部门获悉,上周,内部已经收到了监管层下发的紧急通知,要求并敦促券商尽快自查、保护,并下发处理建议。

据中信建投证券相关负责

人介绍,技术人员已经在周末加班,对系统进行加固。除此之外,多家券商也表示,均安排了数据中心及分支机构IT人员,加班对重点设备、高危设备进行查杀、打补丁。目前,并没有曝出哪家券商有系统被攻击的情况。

外国应对: 欧洲刑警组织提醒 不要支付赎金

据美国有线电视新闻网(CNN)昨晨报道,欧洲官方已经对遭遇勒索病毒袭击的用户发出警告:不要支付赎金。

报道称,欧洲刑警组织警告称,支付赎金无法保证能够将所有被封锁的信息追回,只会让黑客更加猖狂,进而继续寻求新的途径,让更多的电脑被感染,勒索更多的钱。

欧洲刑警组织5月15日表示,目前只有很少人支付赎金。专家表示,目前黑客只收到了5.1万美元的赎金。

欧洲刑警组织表示,遭受病毒攻击的电脑数量并没有想象中增长得那么快,他们所采取的措施似乎已经奏效。

英国国家犯罪部门执行长官欧文斯表示,并没有迹象显示,将会出现第二轮这一病毒感染高发期。

权威机构: 勒索病毒软件 感染速度放缓

根据360威胁情报中心发布的报告,虽然5月15日(周一)工作日电脑开机高峰到来,但监控数据显示,周一受感染机构的增长速度比前两天明显放缓,感染和影响得到控制,总体态势平稳。

360企业安全集团总裁吴云坤介绍,这次病毒爆发恰逢中国国内周末,是大型机构、政府机关使用电脑低峰期,在客观上避免了蠕虫病毒的快速扩散。

腾讯电脑管家反病毒高级工程师龙海指出,勒索病毒的“中招”用户必须同时满足“系统漏洞未及时修复”和“没有安装杀毒软件”两个条件,因此,互联网个人用户相对安全。但同时单位内网用户更易“中招”,“虽然此次勒索病毒的传播方式是蠕虫,但其功能部分仍是敲诈者木马,此类病毒并没有特别的选

择性,内网多存在打补丁不及时的情况。因此病毒一旦进入单位内网,就可以去扫描内网下所有IP地址,一旦发现漏洞,设备就会“中毒”。

英国国家反犯罪局局长琳恩·欧文斯在5月15日发表的一份声明中说,从当前情况看,没有迹象显示英国会出现第二波这类攻击,但这并不意味着已经没有这种可能性。也有观点认为,英国医疗体系在网络攻击面前如此脆弱,主要是因为医疗机构仍大量使用微软“视窗XP”操作系统,这是“视窗”操作系统的一个陈旧版本,微软已停止对它的官方支持。

英国国民保健制度数字中心在一份声明中说,归属英国国民保健制度的医疗机构中,使用“视窗XP”操作系统的设备数量仅占总数的4.7%,并且这一数字还在不断下降。部分医疗机构继续使用这一陈旧的操作系统,主要是因为一些昂贵的医疗设备,如核磁共振扫描仪,还无法马上进行系统升级,因此这些机构需要采取其他措施来规避风险,如将这些硬件设备隔离在整个医院网络之外。

另外,美国总统国土安全与反恐助理托马斯·博塞特5月15

明天起,这种百元钞在鹰城可顶792元花

快看看你的钱包里有没有!!

5月18日起,凡平顶山人,凭任意三位相同号100元钞(例如:000-999位置不限);顺子号或AABB号或ABAB号的百元钞一张(例如:123、321、234、678、3355、8800、5656……位置不限)或吉祥尾号(例如:6、66、666、8、88、888、9、99、999),即可到平顶山日报传媒集团广告营业厅,现场兑换价值792元/箱的杏花村汾酒集团53度盛世家宴美酒一箱(475mlx4瓶)或42度盛世家宴喜庆版美酒一箱(475mlx4瓶)。有多少张这样的钱,可以兑换多少箱这样的酒,让你一次兑到爽!

“借问酒家何处有,牧童遥指杏花村”,唐代大诗人杜牧一句经典绝唱,使得山西杏花村汾酒名扬天下、家喻户晓,奠定了杏花村汾酒在中国千年酒文化中的地位。为了让平顶山市民感受中国酒文化的千年底蕴,品尝醇香四溢的中国名酒,特在我市举行大型百元连号钞兑换汾酒集团盛世家宴酒的品鉴活动!限时又限量;活动只限4天,兑完即止;机会只有一次,请各位爱喝酒的读者朋友千万不要错过这次机会!

需要参加兑换的,赶紧看看你的钱包里有没有符合条件的100元钞,找到后赶紧来兑换吧!详细情况也可以拨打18334839951和18334839915咨询。兑换时间:5月18日至5月21日,兑换地址:平顶山日报传媒集团广告营业厅。



792元/箱



杏花村汾酒集团53度盛世家宴



杏花村汾酒集团42度盛世家宴喜庆版

汾酒集团



盛世家宴酒兑换须知

兑换热线:18334839951 18334839915

凭一张任意位置3位相同号或顺子号AABB号或ABAB号百元钞例如:000、111……999、234、432、678、3355、8800、5656或吉祥尾号(例如:6、66、666、8、88、888、9、99、999)均可兑换价值792元的杏花村汾酒集团盛世家宴酒一箱,53度、42度两款自由选择兑换,有多少这样的钱兑换多少箱这样的酒!让你一次喝个够!!

兑换时间:2017年5月18日-21日

兑换地点:平顶山日报传媒集团广告营业厅(市内乘坐26路、27路、29路、30路、66路、67路、68路、89路公交车到鹰城广场站下车斜对面即到)



微信扫一扫咨询