

全球“想哭”：近百国家遭勒索软件攻击

据称该病毒软件来自美国病毒武器库 英国小伙“意外”阻拦该软件传播

5月12日,全球99个国家和地区发生超过75万起电脑病毒攻击事件,罪魁祸首是一个名为“想哭”(WNCRY)的勒索软件。该软件感染电脑后,会将电脑文件加密锁住,支付黑客赎金后方能解密恢复。俄罗斯、英国、中国等国“中招”。

这款病毒源自上月遭泄密的美国国家安全局病毒武器库。不少网络专家和电脑安全公司批评,美国网络项目开支的90%用于研发黑客攻击武器,一旦该“武器库”遭泄密,势必殃及全球。

不过,这种软件并非没有弱点,英国一名年轻的网络工程师5月13日“无意中”阻拦了勒索软件的疯狂传播。

■ 恶意勒索 限时交付赎金,逾期涨价

据捷克网络安全企业爱维士公司统计,全球99个国家和地区12日共遭遇超过75万次电脑病毒攻击,其中俄罗斯、乌克兰等国受灾尤其严重。

这款病毒名为“想哭”,属于一种勒索软件。电脑用户会收到一封电子邮件,往往是打着工作邀约、发货清单、安全警告等“幌子”,但一旦打开相关链接,就会导致电脑中招。

该勒索软件随即会对电脑储存的文件进行加密,使用户无法打开。电脑屏幕上弹出警告语:“你或许会试图夺回文件,还是别浪费时间了!”

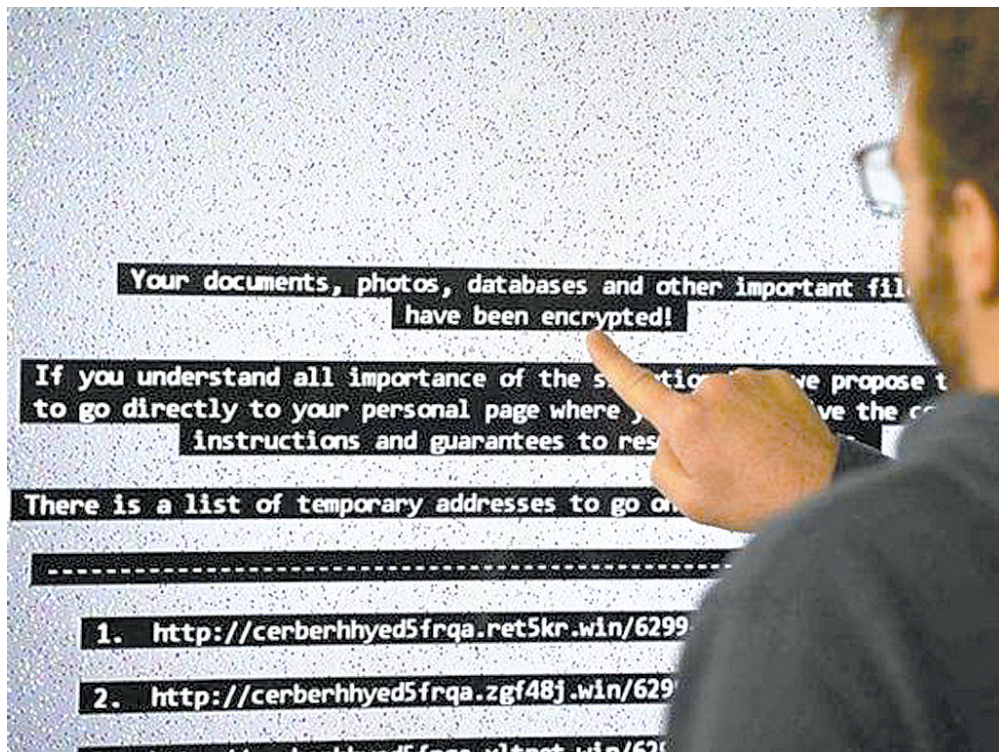
接着,电脑提示用户在规定期限内支付300美元赎金,便可恢复电脑资料;每耽搁数小时,赎金额度就会上涨一些,最高涨至600美元。

据俄罗斯卡巴斯实验室研究员库尔特·鲍姆加特纳观察:“在支付赎金的用户中,多数人在最初几小时内就乖乖掏出300美元。”

■ 多国遭殃 英国多家医院电脑瘫痪

据Splunk网络安全公司主管里奇·巴杰描述,“这是全球迄今最大的勒索软件攻击事件之一”。

卡巴斯全球研究和分析团队表示,俄罗斯所受攻击远远超过其



该软件感染电脑后,会将电脑文件加密锁住,支付黑客赎金后方能解密恢复。

他受害者,而中国大陆和台湾地区也受到较多攻击。

英国公共卫生体系国民保健制度的服务系统12日被病毒入侵后,多家医院电脑瘫痪,不得不停止接待病人,一些救护车等医疗服务也受影响。英国首相特雷莎·梅当天说,英国国家网络安全中心正与国民保健制度联手应对这次危机。

法国雷诺集团5月13日向媒体表示,该集团也受到本轮网络攻击,已暂停法国境内多家工厂的生产工作,避免勒索软件进一步蔓延。罗马尼亚最大的汽车制造企业、雷诺旗下的达契亚汽车厂当天也宣布,该厂因信息系统遭到勒索软件攻击而部分停产。

西班牙、葡萄牙、阿根廷等多国电信企业以及美国联邦快递公司均受这款病毒侵袭。

俄罗斯内务部、梅加丰电信公司遭遇同种病毒攻击,据信已控制住病毒扩散规模。俄罗斯国际文传

电讯社援引俄内务部发言人伊琳娜·沃尔克的话报道,俄内务部大约1000台电脑被感染,不到该部门电脑总数的1%。另一名消息人士称,俄政府文件未在此次攻击中泄密。

■ 波及中国 校园网络成重灾区

中国的校园网络已成为重灾区,全国多所高校出现病毒感染。大量学生的毕业论文等重要资料被病毒加密,只有支付赎金才能恢复。据悉,勒索金额最高达5个比特币,目前价值人民币5万多元。

据了解,目前,“想哭”传播的勒索病毒以ONION和WNCRY两个家族为主,受害终端的磁盘文件会被篡改相应的后缀,图片、文档、视频、压缩包等各类资料都无法正常打开。正值高校毕业季,勒索病毒已造成一些应届毕业生的论文被加密篡改,影响到毕业答辩。

■ 美国挨批 国安局病毒武器泄露

目前,尚未有黑客组织认领这次袭击。但业界人士的共识是,这款“想哭”病毒来源于美国国安局的病毒武器库。上个月,美国国安局遭遇泄密事件,其研发的病毒武器库被曝光于网上。

不少网络安全专家指责,美国斥巨资研发黑客攻击工具而非自卫机制,结果造成全球网络环境“更不安全”。

路透社援引美国联邦政府公布的数据以及情报部门官员的话报道,美国网络项目开支中,90%用于研发黑客攻击武器,例如侵入“敌人”的电脑网络、监听民众、设法让基础设施瘫痪或受阻等。

得知最新攻击事件后,“棱镜”监听项目曝光者、美国前防务承包商雇员爱德华·斯诺登12日发推文

说,“尽管多次被警告,(美国国安局)仍然研制了危险的攻击工具。今天,我们见到代价……医院里的病人生命受到威胁”。

面对外界批评,美国国安局尚未作出回应。美国国土安全部计算机紧急应对小组表示,正密切关注这起波及全球的黑客攻击事件。

■ 应对之策 英小伙“意外”阻拦其传播

英国媒体13日报道,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。

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85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。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置的“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,勒索软件在每次发件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,完全不知道它能停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件和传播,但帮不了那些勒索软件已经发件的用户,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。

(综合新华社中新网报道)

马克龙正式就任法国总统

本报讯 巴黎时间5月14日上午,法国新任总统就职仪式在爱丽舍宫举行。当选总统马克龙与奥朗德完成交接,正式就任总统。

在本月7日举行的大选第二轮投票中,马克龙以66.1%的得票率击败右翼“国民阵线”候选人玛丽娜·勒庞,当选法国总统。39岁的他也由此成为法国历史上最年轻的总统。

当地时间14日上午10点,法国新任总统马克龙到达爱丽舍宫,开启持续一整天的就职仪式。

他首先受到卸任总统奥朗德的接待,两人在总统办公室闭门交流。在奥朗德离开之后,他在爱丽舍宫的宴会厅参加就职典礼,随后在花园里检阅共和国卫队,与此同时,两公里以外的荣军院将响起21响礼炮。

中午12点,马克龙乘车离开爱丽舍宫,前往凯旋门下的无名烈士墓敬献鲜花,为长明火添火。17点,他按照传统前往巴黎市政厅,与巴黎市长伊达尔戈会面并发表演说,以此为一整天的就职“马拉松”画上句号。(中新)



法国当选总统马克龙与奥朗德完成交接,正式就任总统。(中新)

文在寅拟派亲信 出任驻华大使 旨在修复中韩关系

本报讯 据报道,韩国执政党核心相关人士透露,文在寅总统打算任命前共同民主党议员卢英敏担任驻华大使。

韩国《中央日报》网站刊登《文在寅总统内定亲信卢英敏担任驻华大使》的报道,其中称,“文总统将自己最信任的亲信任命为驻华大使,这件事本身就是向中国释放出一种意味深长的信号”“据悉,文总统最近曾对卢前议员说,由于部署末段高空区域防御系统(即‘萨德’系统)和中国的经济报复等问题,韩中关系经历了一些挫折,有必要处理好这一情况,因此希望卢前议员担任驻华大使”。

报道称,文总统认为,为了解决朝核问题,在周围四大强国中,尤其要任命分量较重的人士担任驻美与驻华大使。卢前议员曾在2012年大选时担任文在寅候选人的秘书室室长,是文总统钦点的“最信任的亲信”。这次大选中,他曾在文在寅的竞选对策委员会担任组织本部部长。(中新)