勒索病毒全球爆发 网络安全响起红色警报

国家互联网应急中心提醒:尽快安装安全补丁

《北京青年报》

连日来,全球范围多个国家遭到大规模网络攻击,被攻击者的电脑遭锁定后被要求支付比特币解锁。多家安全软件制造商表示,已经在近百个国家观察到感染案例,受害方包括中国一些高校和英国多家医院。

5月13日,国家互联网应急中心发布通告称,目前,安全业界暂未能有效破除该勒索软件的恶意加密行为,用户电脑主机一旦被勒索软件渗透,只能通过重装操作系统的方式来解除勒索行为,但用户重要数据文件不能直接恢复。"建议广大用户及时更新Windows已发布的安全补丁,做好信息系统业务和个人数据的备份。"

网络袭击波及整个世界

恶意软件的传播最早是从英国开始的。英国公共卫生体系国民保健制度的服务系统12日遭大规模黑客网络袭击,黑客植入的勒索软件感染了英格兰和苏格兰地区的部分医院和卫生部门电脑上的文件并且进行加密,然后要求对方付费进行解密。医院电脑系统的瘫痪导致预约取消、电话断线、患者无法看病。

公开报道显示,意大利、葡萄牙、俄罗斯和乌克兰等多个国家也出现了受到感染的报告。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7.5万次电脑病毒攻击,电脑在感染后即被锁定,用户还被要求支付价值300美元至600美元的比特币。

俄罗斯网络安全企业卡巴斯基实验室12日发布一份报告说,当时已发现全球74个国家和地区遭受了此次攻击,实际范围可能更广。该机构说,在受攻击最多的20个国家和地区中,俄罗斯所受攻击远远超过其他受害者,中国大陆排在第五。

"永恒之蓝"病毒系美国网络武器

据业界人士表示,这次大规模网络攻击采用了美国国家安全局(NSA)开发的黑客工具。几个私立网络安全公司的研究人员表示,黑客通过利用名为"永恒之蓝(Eternal Blue)"的NSA代码,导致软件能够自我传播。

卡巴斯基则强调,这次网络攻击所用的黑客工具"永恒之蓝",来源于美国国家安全局的网络武器库。今年4月,黑客组织"影子经纪人"在网上披露一批美国国安局的黑客工具,其中就包括这个漏洞工具。

美国国土安全部12日发表声明称,已获悉上述勒索软件影响全球多个实体。但是,声明除介绍勒索软件的定义、微软已针对这个漏洞发布补丁、提醒用户应安装补丁外,没有说明更多情况。

国内多所高校中招 目前暂时无解

从5月12日晚上起,陆续有国内高校的学生反映,电脑遭遇到病毒攻击,文档被加密。遭遇到攻击的电脑桌面会显示,如要解锁需支付一定金额的比特币。

某大学城市学院的学生小白告诉记者,与她同寝室楼中,就有多名同学的电脑遭受到了攻击,"现在很多同学都不敢开机使用电脑,怕被黑"。

桂林理工大学的一名学生说,目前他们学校有超过100台电脑遭受到了勒索病毒的攻击。被攻击的电脑大多为使用校园网的用户,"现在都不敢连校园网,怕被攻击"。广西师范大学的一名学生称,12日晚,他正在修改论文的时候,电脑突然中了该病毒,电脑操作受影响,文件被加密。这名学生告诉北记者,电脑被攻击后,会出现一个红白色相间的对话框,对话框里会告诉你发生了什么,如何恢复、如何付款。

12日晚上起,山东大学、南昌大学、广西师范大学、东北财经大学、华东交通大学、中国民航大学等多所大学都对勒索病毒入侵校园网一事发布了相关防范公告。

网络安全公司360首席安全工程师郑文彬告诉记者,这次校园网勒索病毒是不法分子将黑客武器改造的远程"蠕虫病毒",可以远程攻击Windows的445端口(文件共享),一旦感染上勒索病毒,电脑的磁盘文件会被加密锁住,图片、文档、视频、压缩包等各类资料都无法正常打开。

郑文彬说,国内出现过利用445端口传播的蠕虫病毒,因此部分运营商对个人用户封掉了445端口,但因为教育网并没有这个限制,所以这次校园网成为受到勒索病毒攻击的"重灾区"。

如何防御该病毒?

国家互联网应急中心建议,用户及时更新Windows已发布的安全补丁更新,同时在网络边界、内部网络区域、主机资产、数据备份方面做好如下工作:

1。关闭445等端口(其他关联端口如:135、137、139)的外部网络访问权限,在服务器上关闭不必要的上述服务端口;

2.加强对445等端口的内部网络区域访问审计,及时发现非授权行为或潜在的攻击行为;

3.及时更新操作系统补丁;

4.安装并及时更新杀毒软件;

5.不要轻易打开来源不明的电子邮件;

6.定期在不同的存储介质上备份信息系统业务和个人数据。

8.5英镑拯救了多少台电脑啊?

英国小伙"意外"阻拦勒索软件传播

新华社

全球近百个国家和地区12日遭受勒索软件攻击。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。

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。

今年第1000列中欧班列发车

新华社 龚献明 摄

5月13日,2017年第1000列中欧班列从义乌西站驶出。

当日,X8024次中欧班列(义乌-马德里)从浙江义乌铁路西站鸣笛驶出。这列满载小商品、服装等货物的列车是2017年开行的第1000列中欧班列。中国铁路总公司统计显示,2017年中欧班列开行数量较去年同期增加612列,增长158%。

浙江:食品安全纳入地方领导班子考核

新华社 岳德亮

浙江省政府决定强化食品安全工作的督查考核,把食品安全工作纳入地方领导班子及领导干部综合考核评价。

浙江省政府办公厅在近日印发的《年度食品安全工作要点》中指出,要修订食品安全考核评价办法和考核细则,并抓好组织实施。把食品安全工作纳入年度目标责任制考核、地方领导班子及领导干部综合考核评价、平安浙江建设等考核内容,并适当提高权重。

同时,探索差异化考核和第三方评价考核机制,改进日常考核和暗访工作方式方法,推动各项任务落实。

浙江省政府指出,实行综合执法的地方要把食品药品安全监管作为首要职责,积极探索建立职业化检查员队伍制度。