

勒索病毒危及全球

为何中国医院幸免于难？

在刚刚过去的5月，一种名为 WannaCry 的电脑勒索病毒席卷全球，近150个国家超过30万台电脑遭受严重攻击，感染病毒的电脑会被黑客恶意加密文件，需要支付价值相当于300美元的比特币才可解锁。一时间，全球风声鹤唳，谈“毒”色变。

出乎意料的是，让国外很多高校、医院、企业等纷纷中招的 WannaCry 病毒，却似乎并没有对中国的多数医院造成实质性的威胁。有人戏言，这是因为中国的医院不联网，所以才逃过一劫。那么中国医院安然度过本次勒索病毒袭击的根本原因是什么？医师报特邀中国医科大学附属盛京医院计算机中心主任、网络管理中心主任全宇和复旦大学附属华山医院信息中心主任黄虹，为大家深度剖析本次勒索病毒事件背后的真相。



点赞

一项好政策为中国医院筑起安全“防火墙”

▲ 医师报评论员 张广有

近几年来，国内外一些医院系统宕机、遭受黑客攻击、重要数据泄露等信息安全事件时有发生，这让舆论对于医院信息系统安全问题存在普遍担忧的看法。为此，早在2011年，原卫生部就下发了《关于全面开展卫生行业信息安全等级保护工作的通知》，要求三级甲等医院的核心业务信息系统信息安全保护等级不低于第三级（第三级为安

全标记保护级，它要求对访问者和访问对象指定不同安全标记，监督、限制访问者的权限，实现对访问对象的强制访问控制），同时要求各医院于2015年12月30日前完成信息安全等级保护建设整改工作，并通过等级测评。

原卫生部这个未雨绸缪的谨慎举措，意外地为中国医院筑起一道安全的“防火墙”，对于核心系统的高等级保护

让中国的绝大部分医院安然度过勒索病毒的攻击。因此，勒索病毒事件中，中国多数医院幸免于难的根本原因并不是网友戏言的中国医院不联网才逃过一劫，而是国家卫计委和国内各大医院早在2015年底就完成了对医院核心信息系统的高等级防护工作，这才是本次勒索病毒事件中我国医院没有发生大规模感染的真相。

支招

重要的事件说三遍：备份！备份！备份！

▲ 中国医科大学附属盛京医院计算机中心主任、网络管理中心主任 全宇

我把安全比作是“一丑遮百好”，失去了安全保障，医院就算做再多的宣传工作，医疗水平再高，也无法挽回医院形象和患者信任。实际上，中毒之后再去做杀毒软件和安装补丁是“亡羊补牢”的做法，信息安全工作以防为主，要把防护做到前面。信息安全领域，有个最笨也最有效的万能办法就备份，重要的事情说三遍：备份！备份！备份！盛京医院就是以不变应万变，我们的电子病历、挂号系统、数据库等核心系统都做了多重备份。

即使医院的服务器发生故障，因为有多重备份机制，我们的数据也不会丢失。

客观来说，目前还有不少医院在信息安全防护投入和认识不足，完全跟不上医疗信息化飞速发展的步伐。所以，建议从以下四个方面来做好信息安全防护工作。

第一，通过舆论导向，让医院管理层、临床医生和患者认识到医院信息安全的重要性和紧迫性，这对医患双方都很重要。

第二，信息安全不是喊口号，不是靠几个人

就可以管起来的，还是得靠技术和工具来防护，建议在医院所有电脑安装防火墙、防病毒软件，进行定期的更新和维护。

第三，制定并贯彻落实医院信息安全管理规定，向所有医护人员定期强化信息安全的意识，从源头堵住人为造成的信息安全事件。

第四，从法律层面约束接触医院敏感信息的人员。盛京医院和所有能接触到医院信息数据的人员都签订了信息保密协议，这从法律层面来保障医院信息数据的安全使用。

提醒

医院信息 最忧安全隐患

▲ 复旦大学附属华山医院信息中心主任 黄虹

医师报：有医生认为信息安全是信息科的事，跟医生无关，您怎么看待？医护人员的哪些上网习惯会对医院的信息安全带来隐患？

黄虹主任：信息安全，人人有责！医生的两个工作习惯会对医院的信息安全带来很大的隐患：一是U盘的随意插拔，U盘在此次病毒传播中发挥着很重要的作用，可以将病毒传播到内部电脑实施摆渡攻击，这对于医院隔离外部互联网的信息系统安全危害很大。二是随意打开不明来源的邮件附件，一打开就中毒了，病毒还会给送邮箱通讯录中所有的人发送一份带病毒的邮件，造成更广泛的传播。此外，在微信群中讨论患者影像资料，将重要数据存储在公用电脑中，对电脑不设密码或密码设置成简单口令，这些行为都会危及医院信息安全。

医师报：如果电脑感染病毒，应采取哪些措施来拯救宝贵的数据？

黄虹主任：电脑中毒是低概率、高风险的事件，一旦中毒再去补救，难度较大。因此，最好的防范手段是备

份。常用的电脑要安装一些防病毒软件、防火墙，定期更新，及时安装补丁。在工作中，我们会查看终端的防病毒软件是否安装，病毒库是否及时更新，如果发现达不到安全要求，我们会把这个问题终端从内网中踢掉，避免感染其他电脑的风险。

医师报：在未来的医院网络安全工作中，我们如何应对越来越严峻的信息安全和数据安全方面的挑战？

黄虹主任：移动互联网时代，医院信息安全的工作重点跟以前不太一样，以前主要是解决医院内部网络和终端的安全问题，现在更多的是对外面入口的防护。我们的防护分为两大体系，一是核心系统的防护，二是数据的安全，特别是患者的数据安全。医院是公民信息的汇聚地，一旦泄露，面临的危险和影响很大。数据安全方面，我们有一套严格的管控体系，对于核心数据和敏感数据，我们进行实时监控。如果这些数据要到公共区域，我们会将这些数据进行脱敏处理，这样就能避免患者数据的泄露。

微言大义

《北医六院田成华：我放弃临床型研究生导师资格，因为它不伦不类》

@巍巍昆仑：为田成华教授的正义行为点赞！医学生、医学研究生培养岂可儿戏？研究生培养制度岂可儿戏？临床型研究生培养计划出于何处？是在培养后继医学人才？还是在摧残中国医学事业？

《我加班你过节，别和我谈医德！一位医生：我拒谈医德的N个原因！》

@韩：从一开始我就感觉所谓医德，就是用道德舆论给医务工作者施加的一种压力。欺负你又怎样？待遇不公又怎样？反正你得在乎你的医德嘛！

《儿童节！别忘了儿科医生的忧伤》

@Mars：大多数人只有在孩子病了才想起来找儿科医生，而且事实上根本没有人管医院有几个儿科医生看病。

《医学和医者》

@观雪：向有人文关怀精神的医护人员致敬，你们面对的不仅仅是病，更是人。

《8000支阿托品刷爆朋友圈，还有你不知道的救命药市场乱象》

@洋芋丝：1999年抢救有机磷中毒病人，我和另外一个实习医生连续7个小时掰阿托品安剖瓶，手指都割破了。



扫一扫，关注 DAY12006

时评版稿约

《医师报》时评版欢迎广大读者针砭医疗行业时弊、赐稿。希望大家对医药卫生体制改革、医师执业环境、医患关系、医师职业道德建设、当前行业热点问题等展开评论。

稿件请注明新闻来源，并附作者真实姓名、单位、地址、邮编、电话。投稿邮箱：ysbzgy@163.com