勒索病毒来袭 金融系统急自查

上周末，一场大规模的勒索病毒肆虐全球。受害者的电脑会被病毒锁定，需向黑客支付比特币之后才能解开。5月14日，记者从证监会、银监会等机构证实，证监会和银监会均针对近日全球爆发的大规模比特币勒索病毒感染事件发文要求各地证监局、银监局以及券商、银行、基金等机构进行自查并做好防护。

记者多方证实，证监会、银监会均发文要求各地监管部门和机构自查并做好防护措施

有消息称，在这场病毒侵袭中，高校受到的攻击最为严重，金融系统的安全也引发了广泛关注。这场病毒来自何方？为何会选择比特币作为解锁手段？高校为何“首当其冲”？金融系统是否将遭受冲击？记者采访相关监管部门和企业，追问这场病毒带来的影响。

证监会内部人士称14日停网待打补丁

5月14日，监管部门内部人士向记者表示证监会和银监会首先要求自查并做好技术防护，同时，发文到地方监管局要求其落实文件，并将文件转给分管金融机构自查并做好防护。

证监会内部人士对记者表示，5月14日，会里已下发文件要求自查并做好防护。为了隔离比特币勒索病毒，证监会于5月14日全天停网，并将于15日上班时间进行全方位打“补丁”。不过，“每个电脑安装补丁应该很快就能好”。

14日晚，多地银监局人士向记者确认，5月14日已经收到银监会统一下发的文件，要求银监局做好部署防范。同时，根据批示，在自查自护的同时，要求银监局将文件转给分管金融机构。

记者另从多家银行获悉，银行已经下发《关于防范“蠕虫”式勒索软件（ONION）病毒攻击的通知》（下称《通知》），要求提前做好病毒的防范工作，仔细逐一排查各项信息系统的漏洞隐患，防微杜渐，将信息科技风险降到最低。

记者拿到的多份《通知》显示，多家银行主要采取了网络安全防护措施及终端和数据安全防护措施：检查互联网出口和各区域网络防火墙是否关闭或禁用445端口的访问。要求各个机构电脑联络员第一时间将病毒感染信息发送给所在机构的微信群，并通知所在机构的所有员工，近期尽量避免接入互联网。

同时，上述银行科技信息部为所有Windows操作系统的电脑终端下载安装微软发布的补丁，修复病毒攻击的漏洞。

此外，上述银行还要求，做好备份电脑中的重要文件资料到移动存储介质，备份后脱机保存存储介质。如果发生“蠕虫”中毒事件，科技部第一时间隔离感染，关闭银行互联网出口和445端口，避免“蠕虫”在内网的快速传播。

记者从某券商信息技术总部接到的《通知》看出，证监会机构部、当地证监局和证券业协会已要求券商自查并做好预防保护，并于5月14日中午12点前反馈。

为了应对证监会的《通知》，该券商也发了应对通知，制定相关技术应急处置方案，并进行各业务系统的检查和持续加固。应急处置方案通过邮件、短信、OA系统等发出，提醒各部门、各分公司、子公司、营业部老总安排人员14日中午前完成协同检查，落实防护措施。

支付宝微信称未受影响

相较于传统端口，比特币病毒席卷之下，主要依赖网络进行支付的机构是否受到影响？14日下午，多家网络支付机构向记者表示，目前没有受到病毒的影响。

支付宝方面表示，支付宝“没有受到任何影响”。支付宝相关负责人也向记者回应称，“中石油断网确切原因我们尚不清楚，但可以确认的是支付宝与中石油的支付接口目前无任何问题，可正常提供支付服务。”

相关人士所称的“断网”，源自5月14日，中石油在官网发布公告确认，因受比特币勒索病毒影响，5月12日晚间，公司所属部分加油站正常运行受到波及，导致只能使用加油卡和现金进行支付。

上述支付宝相关负责人表示，支付宝目前并没有受到该病毒任何影响。“支付宝及时发现了此威胁并进行了全面保护。我们会一直为用户提供最好的安全保护。”

此外，腾讯财付通相关人士当日也向记者表示，“没有影响”。

该人士向记者提供一份腾讯安全团队的举措材料显示，在防范上，腾讯安全联合实验室反病毒实验室负责人、腾讯电脑管家安全技术专家马劲松指出，可采取几种手段。一是临时关闭端口；同时，及时更新Windows已发布的安全补丁。此外，可利用腾讯电脑管家“勒索病毒免疫工具”进行修复。另外，重要的资料一定要备份。

5月14日下午，记者分别通过支付宝和微信进行一笔消费支付，支付过程中均未出现异常。

另外，将苹果iTunes作为最大客户的易联支付董事长朱启文对记者表示，目前公司没有受到影响。在办公环境，易联支付不会接受任何从外界发起的连接。

中石油加油站系统遭攻击，14日起部分恢复

全球比特币勒索病毒爆发，国内部分加油站也成为受害者。

中石油5月14日下午在官网发布公告确认，因全球比特币勒索病毒爆发，公司所属部分加油站正常运行受到波及。截至14日12时80%以上加油站已恢复网络连接，受病毒感染的加油站陆续恢复加油卡、银行卡、第三方支付功能。

中石油称，5月12日22时30分左右，因全球比特币勒索病毒爆发，公司所属部分加油站正常运行受到波及，病毒导致加油站加油卡、银行卡、第三方支付等网络支付功能无法使用。

在国内，中石油为仅次于中石化的第二大加油站运营企业，其他同业企业并未发生被攻击事件。

在加油站管控系统服务商喂车科技官微发布的一篇文章中，喂车科技表示，传统油站系统更容易遭受病毒攻击的原因在于时间久远，缺乏有效的安全维护，更容易被病毒利用，而且网络方案陈旧，隔离度不足，更容易引起病毒传播。

不过，另一位加油站行业人士表示，客观而言，如果没有这次攻击的话，中石油的系统在行业内并不算太差。这次中石油支付系统出事其实有些“倒霉”，因为跟别的同行业企业相比，就他们使用了Windows系统。

5月14日，一位加油站企业负责人对记者表示，中石油支付系统，因为建立在Windows系统上，未做相关端口的安全防范及补丁修复，由漏洞工具“永恒之蓝”攻击导致中毒。喂车科技等其他同业企业也有部分服务建立在Windows系统之上，不过其及时关注到漏洞发布并做了防范，所以未受影响。

面对突发事件，5月13日，中石油紧急中断所有加油站上连网络端口，并会同有关网络安全专家连夜开展处置工作，全面排查风险，制定技术解决方案。截至14日12时80%以上加油站已恢复网络连接。

5月14日，记者来到位于大兴区小红门路的中石油加油站，有车主正在使用现金支付。工作人员告诉记者，14日上午本站恢复微信等支付功能正常使用，中午时候中石油其他加油站也恢复正常。

对于加油站未来如何规避病毒攻击，上述加油站企业负责人建议，系统安全是支付系统关注的重点，首先秉着最小权限和最小开放的原则，需要对整个系统进行权限设置管理，关闭不必要的端口及服务。其次，对于运行程序的基础系统需要随时关注其动态与世界同步信息，第一时间发现问题解决问题。

■抗毒一线

“开始很蒙，不知病毒怎么进来的”

外界意识到永恒之蓝病毒是在上周末，对于从事安全工作的工程师，早在上周前两天，就已经开始忙碌起来了。

在最近一周的病毒狙击战中，安全工程师们历经失落与兴奋，心情会随着病毒的一波波攻击而跌宕。

“失落感是上周前几天，从对系统日志等的观察中已经发现了一些异常，但那段时间很蒙，不知道病毒怎么进来的，经过几天跟踪后查到原因，反而豁然开朗，因为这就有目标了，只要找到原因，一步一步向前推导来排查，就不害怕了”，在一家互联网安全软件公司工作的反病毒人员刘海粟，向记者讲述了他近一周的病毒狙击战的过程。

在病毒爆发的周五（12日）晚上，刘海粟接到同事朋友的求助，朋友遭遇的这场严重的入侵行为，恰好是之前该公司团队就已经在跟进的入侵方法，那时候觉得“这已经是不幸中的万幸”，知道病毒是如何来的，不用再从零开始复盘，可以有的放矢，跟团队一起提出应对策略。

在与勒索病毒交战过程中，刘海粟还记得曙光乍现的那一刻。在帮助用户远程看电脑Windows系统日志的过程中，因为日志很粗略，起初没抱太大希望，但突然看到服务启动这一项，凭经验看不是正常程序，从而锁定病毒样本。锁定病毒样本之后，后续的分析就有迹可循，相对简单多了。

据该公司团队中的首席安全工程师回忆，公司在12日晚就紧急连夜成立联合指挥部，很多安全领域员工24小时都守在公司，“包括查杀蠕虫，帮助用户防护，给用户免疫，用户已经中招的，要给用户恢复。”

刘海粟2010年开始从事计算机安全相关领域的工作，此次遭遇的病毒是他职业生涯中遇到的最大规模的一次。与2006年流行的熊猫烧香相比，熊猫烧香通过杀毒打补丁就可以解决，而这次增加了勒索软件，即便查杀木马之后，文件被加密了，依然无法恢复，损失更为严重。

“其实安全工程师的工作挺不被理解的。很多中小企业老板认为安全就是花钱后没收益，能达到的极限就是不出事，很多人认为进行安全防护没必要。但这次病毒给他们敲了警钟，一旦公司内部有人中招，网络系统全部崩溃，就什么都来不及了”，刘海粟总结自己的安全防护战时说。

追问1 黑客为何选择比特币？

在本次袭击中，黑客指明要求用比特币进行汇款，为什么选择比特币？

比特币是一种基于区块链技术的“数字货币”，还有去中心化、匿名性的特点。2013年，央行曾明确比特币系一种特定的虚拟商品，不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用。

在此次病毒传播中，不少人把矛头指向了比特币匿名、能够快速全球转账的特征。“比特币一开始也是流通于计算机社区的交易，黑客更能清楚原理。”一位分析人士对记者解释。

浙江大学互联网金融研究院张瑞东教授指出，这种匿名性相对于普通汇款而言，增加了监管对流向监管的难度。

有比特币玩家对记者介绍，实际操作上，在一些平台上用比特币交易，只需输入一串数字地址，等待确认交易后，通过少数几步即可完成提币（将比特币直接从一家平台转移到另外一家平台，目前多家国内平台已经暂停）操作。

相对于传统银行汇款而言，这种汇款方式要比通过银行跨境支付、通过层层机构便捷得多。去年，央行还下调了大额现金交易的申报额度，超过后需向外汇局等部门报备，且个人换汇还有1年5万美元的额度限制。

对此，也有平台人士称，“100%匿名并不准确”。币行一位分析师对记者解释，对于比特币来说，涉及比特币的钱包的每一项交易都将永久保存在相应的区块链中。

“发送和接收比特币就像作者用笔名发表作品一样，如果一个作者的化名和他们的身份联系在一起，他们曾经写下的任何东西都会与他们联系在一起。”他解释，交易并非无法完全追溯，Haobtc一位挖矿负责人也对记者表达了同样看法。

不过，也有分析人士认为，如果勒索者收到比特币后并不使用和交易，追踪身份仍然具有相当难度。

14日，在病毒传播影响下，比特币仍保持了稳健态势，长时间在1万元／人民币的价位上游走，截至记者发稿报10771元／枚。据币行的行情显示，从4月开始比特币“牛市”启动，从4月上旬的一枚比特币兑换7000元人民币的价位，火箭般冲破1万人民币兑换1枚比特币的大关。

今年1、2月份，比特币曾经遭遇了监管风暴。央行对币行、比特币中国以及火币网（据称占领了国内95%市场的三家平台）进行了现场检查，并直指融资融币等违规问题。

在监管风暴过后，几家平台陆续暂停了融资融币和提币业务，并宣布开始征收交易费。

追问2 中国高校何以成重灾区？

互联网分析人士何帅认为，从本次中国高校成勒索病毒重灾区可以反映出我国信息化建设中出现的两个极端现象，即信息化程度高，但缺乏统一规划和科学管理。

有一个不容忽视的现象是，XP系统在中国高校以及民企、国企、大型机构有很高的市场占有率。尽管微软操作系统早已推出Vista、7、8、10四代，国际权威评测机构StatCounter统计，2017年1月份XP系统依然在中国市场保持17.79%的占有率，其中大部分份额集中在上述提到的机构。

360反病毒人员刘海粟认为，上述分析有一定道理，但版本陈旧并不是这次病毒蔓延的全部原因，用户不重视更新同样是不可忽略的原因。这次受到病毒感染的也有一些XP以后的系统，Windows7用户量很大，但如果用户对打补丁等安全措施不敏感，没有及时更新，也依然可能遭遇病毒攻击。

那么，Windows系统是否需要反思呢？

在此次勒索病毒规模爆发后，5月13日，微软发言人称，所有使用最新操作系统（含免费杀毒软件）并开启Windows更新的用户都已经得到保护，不被此次攻击影响。与此同时，为了更好地保护所有Windows用户，我们也已经特别为使用早期软件的用户，包括WindowsXP、Windows8和Windows Server2003提供了紧急更新。此外，其表示已在第一时间，将更新分享给国内所有杀毒软件和安全软件公司。以便于他们为所有Windows的用户提供保护。

在刘海粟看来，微软在这次病毒大爆发之后虽然采取了特事特办的措施，但是从重视安全角度方面也有一定责任。

这次的漏洞从Windows XP版本时就已经存在，而微软不再给XP系统更新，宣布停止服务，在这次如此严重的漏洞面前没有及时给XP系统提供补丁，而是在病毒大爆发之后才给XP用户追加补丁，有点后知后觉的感觉。微软不是专业安全公司，作为普通公司，在这点上没有过错可言，但是确实存在一些疏忽。

就此次事件，对于用户而言，要提高安全防护意识。很多人认为杀毒软件、打补丁会拖慢系统，所以不做相关的安全措施。这样尽管系统感觉清爽，但一旦出现问题，结果就不可挽回。

据《新京报》

勒索软件袭击百余国仍在发酵 损失或达千万美元

一个名为“想哭”的勒索软件12日袭击了全球上百个国家和地区使用微软视窗操作系统的电脑。相关危害还在扩散，对公共设施的危害风险暂难估量，上千万美元的损失或在所难免。

欧盟刑警组织人士14日说，这次网络病毒袭击“达到史无前例的级别”，涉及超过150个国家和20万用户，要找到元凶需要进行复杂的国际调查。

病毒在周末扩散两天后，各地的生产生活都受到不同程度影响，中招的包括政府部门、医疗服务、公共交通、邮政、通信、汽车制造等多个领域。专家警告称，随着新的一周的到来，该病毒产生危害可能继续发酵，尤其是在亚洲。网络安全公司赛门铁克专家估计，目前该病毒造成的损失接近千万美元级别，未来的损失可能继续上升。

“想哭”进入电脑后，会锁住用户的文件，要求用户支付赎金以换回文件。用户中该病毒后，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。俄罗斯卡巴斯基实验室研究员库尔特·鲍姆加特纳说：“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。”

微软3月就已发布针对此类勒索软件的补丁，但许多用户尚未安装。13日，微软宣布这一补丁完全免费使用，所有用户都可下载安装。

俄罗斯卡巴斯基实验室和捷克网络安全企业爱维士公司均认为，此次受攻击最严重的是俄罗斯。俄内务部、卫生部、俄罗斯储蓄银行、铁路系统均报告受到攻击。内务部1000台电脑被攻击，但发言人说没有造成泄密；卫生部说攻击“被有效压制”；俄央行说，银行机构的数据没有泄露；俄铁路系统表示，铁路运行未受到影响。

英国公共卫生体系国民保健制度（NHS）则受到严重影响。该国的技术专家13日仍在忙碌，以尽快恢复NHS的运转。英国内政大臣安伯·拉德13日说，45个公共医疗组织受到黑客病毒攻击，但病人数据未被盗取。受攻击影响，除急症外，病人被要求不要到医院就医，就连化疗部门也暂停了医疗服务。

英国媒体报道，大部分公共医疗组织的电脑操作系统陈旧，没有更新安全程序。

受此次病毒攻击影响的还包括中国的一些校园网络、印度尼西亚的数家医院、美国联邦快递公司、西班牙电话公司、日产汽车公司位于英国的工厂、法国雷诺汽车公司工厂、挪威和瑞典的几家足球俱乐部等。德国铁路系统运行未受影响，但车站显示出发、到达车次信息的屏幕受到影响，为此，德国铁路公司加派人手在车站为旅客提供信息。

多国当局正敦促各大组织机构及时更新安全软件，运行防病毒程序，并将数据备份到其他地方。

多家网络安全企业认定，“想哭”源自几周前遭泄密的美国国家安全局病毒武器库。

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。

据《经济参考报》

做好备份 是IT时代永恒的生存智慧

个人用户在这些危险面前，除了做好防护，似乎很难有其他办法。

这么厉害的“武器”，是源于美国国家安全局（NSA）旗下的“方程式黑客组织”使用的部分网络武器泄露出来。虽然从法律上讲，如果NSA没有尽到安全保管的责任，是对此事件有一定的责任。但是，首先，安全保管的义务，并不意味着一定不会发生盗窃、泄露事故；其次，要证明NSA，这样一个高度敏感的国家安全机关未尽到义务的调查与取证，在国际社会某种程度上是从林社会的今天，实际上是不可能操作的。

个人用户在这些危险面前，除了做好防护，似乎很难有其他办法。对于具体的勒索病毒，相关防范方法已经很多了，但更长远地看，备份数据，是IT时代的生存智慧。

我们时常在家里发现那些几十年前的老照片，即便发黄模糊了，但总还夹在相册中，时不时被翻起。但是，我们现在的相片虽然是数字化的，永不会发黄，但在40年、50年的时间中，却很难保证能躲过各种数据丢失与损坏，一旦丢失，就永远找不回来。

你的数据比你的电脑值钱。这一点大家都知道，但是，却很少有人真正按这句话去对待自己的数据。大多数人，会小心翼翼地爱护他们新买的电脑，但却舍不得花钱花精力去把数据保存好。直到数据丢失，那些珍贵的照片、资料再也找不回来时才意识到，数据比电脑更值钱，更值得守护。

那么该如何保存你的数据？如果自己备份数据，什么方式好呢？首先，刻录光盘是靠不住的。U盘与固态硬盘也是靠不住的。在现阶段，唯一靠得住的是机械硬盘。但是，把数据从C盘复制一份，拷贝到D盘，这不是在备份，就如同把100万现金从冰箱搬到床下面，不是在隐匿现金一样。此次黑客勒索事件中，有些人在C盘上的数据沦陷了，慌忙中去看D盘E盘上的，才发现同样被加密了。即便不是同样被病毒加密或破坏，放在同一个硬盘，也很容易因为硬盘损坏而同时丢失。所以，备份一定要用另一个硬盘保存。

从这一次事件来看，仅仅用另一个硬盘保存也是不安全的，这个硬盘还得离线，或者断电。仅在需要恢复或者拷进文件的时候才连接上电脑。如果考虑到同时连接电脑的哪一段时间内出现故障，造成同时损坏的风险，最好有第一备份盘和第二备份盘。现在硬盘价格很便宜，这么做的费用其实不大，一千元完全够了。

用硬盘备份数据，还要值得注意的是，如果你的数据有保密价值，那么，要么放保险柜，要么进行磁盘加密，而后者比前者其实更安全。Windows本身就自带了BitLocker驱动器加密功能，通过加密整个驱动器来保护数据，其目标是让Windows用户摆脱因电脑硬件丢失、被盗而导致由数据失窃或泄露构成的威胁。由于使用了AES 128位或256位的加密算法进行加密，通常情况下，只要用户的密码有足够强度，这种加密就很难被破解。

据《新京报》