综合防范 不断提升网络安全防护能力

□ 黎 佳 马景毅

随着我国信息化进程的不断深入，信息安全问题成为政府、企业和个人广泛关注的焦点问题。计算机的硬件性能与网络带宽的不断提高，近几年来，个人电脑中存储的信息的安全问题也被人们逐渐开始重视。

对于信息保护的防范手段也从最早的杀毒软件慢慢转变为主动发现与计算机深度学习的方向发展，可以通过以下几个方向进行网络安全防范。

初始密码重置 升级路由器固件

现阶段，家庭使用的路由器已经从传统的“家庭路由网关”慢慢发展到了“智能网关+与智能终端的控制器”，而且路由器的功能也在不断增加。

据统计，全球98%的路由器都来自中国或是由中国工厂代加工，像MTK等这样的芯片集成公司，让生产路由器基本没有任何技术难度，但是，越简单的生产流程，也越容易暴露出安全问题，比如WIFI密码破解，而导致路由器被盗用；路由器被入侵，导致信息被泄露等。

家庭路由器安全风险可以从以下几方面把握。国内一个企业的论坛统计，国内主流路由器的用户账号密码默认为非常简单的：123456789、root、admin等弱口令。因此，路由器攻击者完全可以通过穷举的方式进行路由器密码破解，即简单的猜测密码等方式，从而拿到ROOT最高管理权限。在拿到路由器权限后，攻击者就可以通过DNS等方式对路由器连接的设备进行密码爆破的攻击行为。

所以，在购买路由器后，路由器必须要在第一时间，对密码进行设置，如果有条件，可以对管理端口与SSH等端口进行修改。

同时要及时升级路由器固件，因为针对WIFI的安全，现在一般路由器都支持双模工作模式，那就意味着可以设置：访问模式与自用模式，那这样的话就能够把他们进行有效分离。同时建议开启ARP攻击防御功能，这样会有效防止内网APR攻击。

硬件方面，因为现在一般的路由器设备都是基于OPEN-WRT，因此，如果有条件，建议选择大工厂生产的路由器，比如，小米、联想、TPLINK等。

另外，可以选择自身带安全防护功能的路由器，比如“铁幕护盾”，“360路由器”等，路由器固件建议进行初次设定时就选择自动升级。

安装主流软件 守护个人电脑安全

这几年，随着计算机系统的发展，计算机系统安全防护功能也进行了相应地提高。但是不可否认的是，互联网中的病毒与木马也进行了相应升级，一些网络安全团队也在部分最新的病毒与木马中发现了杀毒软件免查杀技术（免查杀技术是指，通过一定的技术手段把一个木马进行修改，让杀毒软件或是安全软件认为这个病毒或木马是安全的软件，而不存在威胁）。

针对免查杀木马的防范，建议安装主流的安全软件。同时，进行病毒库升级，因为木马都有个共同的特性，就是会通过端口的开放，然后进入特定的文件进行复制或是远程操作行为。所以，建议通过安全软件的进程管理方式监控进程，如发现非法进程要第一时间进行结束。同时，要定位文件的位置，如果发现文件存在异常，需要进行清理与删除。

而现在很多木马也会通过U盘或是移动硬件方式进行传播，针对这种木马传播方式要对软件USB端口进行监控。一般主流的杀毒软件都有这项功能，当在特定的环境，重要的文件要进行加密或是进行HASH（哈希值）的生成。加密文件方式主要是防止攻击者拿到文件权限后进行读取，市面上也有一些推荐的免费加密软件，用户可以在下载后，进行简单设置就可以正常使用，生成“哈希值”主要是为了防止文件被病毒或是木马感染，所以可以通过“哈希值比对”方式对软件安全进行验证。

最后一个安全风险，就是网页木马。虽然最近很少报道有新型的EXPLOIT，但是我们的安全团队确实发现了一批网页木马。

网页木马主要是攻击者通过入侵一些网站，然后在网站中植入特定的木马病毒，当访客对网站进行访问的时候就中了木马，或是在网站下载文件的过程中下载到了木马。

针对这种情况，用户要定期设置自动升级安全系统补丁，这样能起到一定的防御作用，而浏览器建议使用CHMOD或是拥有CHMOD内核的浏览器，同时要记得安装安全控件。

MAC地址绑定 保证智能终端安全

随着传感器与人工智能的一些技术的开源，当下很多智能终端设备也进入了普通老百姓的家。但是，很多人没有考虑到这些智能终端中存在的安全问题，以下我们就智能终端的本身与手机智能终端与连接端的安全进行讨论。

我们先初定手机也属于智能终端，对于手机这样的智能终端，国内很多厂家都会选择比较成熟的芯片解决方式。但是，这些智能手机在软件层面上基本都是使用开源软件，虽然开源软件对软件行为有着推动的作用，但是代码的安全也是一个很大的话题。所以我们建议智能终端包括手机等有条件情况下要选择一些大型厂家生产的手机。那么，如何保证智能终端的安全呢？

笔者因为写代码“目空一切”，洗澡时总忘记提前烧水，所以买了一个智能的热水器，该热水器拥有“蓝牙功能”，也可以与WIFI连接。同时，拥有专属手机APP，可在APP中控制水温，这是厂家为了让用户更方便使用而设计的，但是事实上安全问题也就出来了。攻击者完全可能通过“蓝牙功能”连接到热水器进行控制，所以建议使用“蓝牙功能”时，一定要设置安全连接密码，而不是使用空的或是默认的弱密码。

针对WIFI连接的安全问题，建议在路由器上进行安全设置，因为所有的智能硬件都会主动连接路由器，建议在WIFI连接开启之后要进行MAC地址的绑定或修改默认密码。如果有条件可以通过路由器进行网段的设定隔离，也就是智能家居是一个网段，正常上网是一个网段，这样就更好区分与安全设定，攻击者即使是破解了WIFI也无法进入智能硬件进行控制。

杀毒引擎扫描 做好新型病毒防御

因BITCOIN（比特币）ETH（以太币）等价格的暴升，所以现在很多黑客或是有组织的黑客团队，在进行研究新型的病毒木马的研究。

中了这类病毒，病毒会主动进行挖矿。中病毒后，很明显的现象就是进行在挖矿时CPU进程使用会非常高，所以，建议当发现CPU进程使用90%以上而又第三方无认证的软件进行操作时，那就要安全通过软件进行定位，查看是不是挖矿木马。

还有一种方法更简单，先让本地网络断网，再查看CPU使用数会不会下降。因为挖矿病毒在挖到矿后会第一时间连网打到指定的黑客账户，如果断网了，那就无法进行，所以这也是识别是否中了新型挖矿病毒的一个方式。

如何防范这类病毒呢？

用户在下载软件时，一定要选有安全认证过的安全网站，然后在使用软件过程中发现CPU进程有异常就要第一时间进行全盘查杀。这里要注意的是，从安全卫士下载的软件一般下载后，都要下载专业的杀毒引擎进行扫描才可以使用，因为安全卫士就本身并不具有杀毒能力。

发展网络安全事业，为建设网络强国贡献力量。

市场点睛

设定证券期货从业人员廉洁“红线”非常有必要

□ 安 宁

近日，证券行业迎来廉洁从业的新规，《证券期货经营机构及其工作人员廉洁从业规定》和《关于加强证券公司在投资银行类业务中聘请第三方等廉洁从业风险防控的意见》正式发布实施。这两个文件的发布，不仅进一步加强了对证券期货行业的廉洁从业监管，而且也设定了证券期货从业人员廉洁的“红线”，夯实了新阶段证券期货行业规范发展的基础。

上述文件尤其突出了对券商重点业务领域的廉洁从业要求，对投资银行类业务加以重点规范，并对“围猎”监管工作人员、探听保密信息、干扰审核工作、唆使或协助他人行贿、PE腐败等突出问题作出了细化规定。

廉洁从业，不仅是适应金融业扩大开放，提升营商环境的要求，也是金融“防风险”不可或缺的重要一环。

近年来，随着金融体制改革不断深化，直接融资规模日益扩大，一些证券期货经营机构在各类业务快速发展中出现了内部管理失控、未勤勉尽责、直接或间接进行利益输送、商业贿赂等廉洁问题。

特别是随着行业规模的扩大，干扰发行审核工作、债券交易中的利益输送、基金经理从事“老鼠仓”交易等多起违法违规案件被查处，这些不当行为严重破坏了行业生态，扰乱了市场秩序，损害了投资者利益，同时也损害了所在公司的形象和整个行业的公信力。

尽管我国高度重视证券期货行业廉洁从业风险防控，现行的《证券法》和《证券投资基金法》等也对证券期货行业从业人员提出原则性要求，但是有关廉洁从业的规定较为分散，缺乏统一要求和安排，且部分条款较为原则，缺乏细化、明确的罚则。因而有必要以部门规章的形式颁布新规，统一行业认识、明确经营机构及其工作人员廉洁从业的专项要求。

为此，证监会深刻认识到证券期货行业反腐的必要性和紧迫性，通过制定上述规定，旨在统一行业认识，铲除行业毒瘤，通过督促经营机构建立健全廉洁从业内部控制管理体系，严肃处理廉洁从业管控不到位的行为，进一步提高行业机构执业质量。

笔者认为，当前资本市场的监管主基调仍是防范风险，维护资本市场稳定运行，在此过程中，证券期货从业人员的廉洁自律，直接关系“防风险”制度执行的有效性。因此，加强证券期货从业人员的廉洁自律管理，坚持反腐无禁区、全覆盖、零容忍，非常有必要。