移动闪存盘 摄像头 当心日常设备被攻击

网络安全问题一直牵动着人们敏感的神经，也让大家越来越认识到信息安全的重要性。虽然电脑都安装了防毒软件、防火墙，也会定期进行系统更新、修补漏洞，可还是会莫名其妙地蓝屏甚至黑屏，原因究竟在哪里呢？据澳洲媒体报道，很多恶意攻击可能就从哪些我们一直使用的、再平常不过的设备“下手”，比如一个小小的移动闪存盘，或者网络摄像头。

日常攻击来源——移动闪存盘
捡到便携设备别插电脑

根据澳大利亚解释型新闻网（The Conversation）报道，虽然现在有了各种云存储平台，许多人还是习惯使用U盘，尤其是当网络不太给力，不想为了线上数据传输干着急的时候。不过，网络安全专家几年前就曾警告，这个值得信赖的“小朋友”有可能会背叛我们，因为它存在着挺大的“缺陷”。

许多文件可以在USB上“隐身”，如果不是特别留意的话，很多人都不会发现它们的存在。当电脑检测到我们插入USB设备时，它很可能会尝试自动运行在上面找到的任何代码。而这一特性可以追溯到CD-ROM时代——我们插入一张光盘，计算机会自动运行，不需要我们点击任何图标。

USB导致的“网络威胁”大部分都与缺乏戒心，或者粗心有关。有时，网络罪犯攻击某家公司的方法很简单，甚至看上去很“蠢”——往停在停车场的汽车边上扔一个U盘。总有些“好奇”的员工会把U盘捡回去，插进办公室的电脑里试一试，而这一试，在他们意识到可能坏事之前，电脑早已经“中招”了。

这一“作案手法”听上去不可思议，但是谷歌研究人员进行了一项实验告诉我们，很多人都缺少戒心。2016年4月，研究人员特意将300个U盘“扔”到了美国伊利诺伊大学校园的不同角落。结果发现，一半的U盘被人们拾起，连接上了他们自己的电脑，而U盘里的文件也被大家打开了。而这一切都发生在第一个U盘被捡起的6分钟里。尽管以这种方式进行网络攻击看上去有些异想天开，但是，一些看似无害的便携式外围设备确实有可能引发大规模的网络攻击。

国际空间站也曾被感染

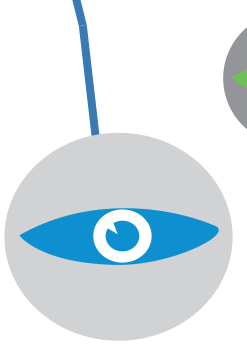
在不检查、不“扫描”的情况下使用U盘可能让系统暴露在许多危险下：病毒、有针对性的恶意软件、数据泄露或损坏等。

黑客可以靠编写代码，将U盘化作“鼠标”或“键盘”，远程控制人们的电脑，访问文件和个人信息。而借助U盘储存在电脑上的代码会把人们网络冲浪的一切内容截屏发送给黑客，如果网速够快的话，人们可能完全没有意识到宽带被这些操作占用了。

据澳大利亚媒体2013年披露，2008年，国际空间站的系统就曾经因为一个感染病毒的U盘被意外“传染”了。该病毒先是起源于一名俄罗斯宇航员随身携带的笔记本电脑，随后在整个空间站的电脑网络中传播开来。好在受“感染”的电脑都是负责收发电子邮件和执行行政任务的，如果是负责空间站运行或进行试验的电脑被感染，造成的后果不堪设想。

对于这次意外，安全公司的首席技术官埃里克·拜尔斯在2013年的自动化会议上给的回应是：以国际空间站的安全性和安全协议，还有极其有限的访客数量，都能通过USB感染病毒，以为家用或企业电脑能更安全的想法都是“愚蠢”的。

这个例子也说明了企业确实应当认真对待被U盘病毒“污染”的风险，即使系统与外部网络隔离，也不能保证信息系统的绝对安全。因为员工和客户们习惯使用U盘和个人电脑，而这些都可能成为风险来源。



日常攻击来源——摄像头
更改默认密码防止入侵

被“利用”的联网设备远不止这些，网络摄像头原本是用来保护我们的，但我们也要费心保护这一摄像系统。事实证明，我们的摄像机在充满网络威胁的环境中非常“脆弱”。

2016年后半年，一次大规模DDoS攻击（分布式拒绝服务攻击）阻止了用户访问亚马逊和Twitter等主要网页。黑客们利用了许多联网设备来参与攻击，其中就包括网络摄像头。不幸的是，许多网络摄像头都没有修改默认密码或者仅设置了非常简单的密码，这让病毒很容易“穿透”摄像头形成攻击。要知道，如果没有改过密码，黑客可以很容易地登录摄像头，一些默认的用户名和密码甚至就列在了制造商的网站上。其实，通过设置靠谱的密码，并且经常更换密码，就可以阻止大多数的黑客“入侵”。

专家提醒，如果有条件，最好为所有的网络摄像头配备一个单独的网络，视频录制系统应当同时连接两个网络：一个是摄像头独立网，一个是另外电子产品用的网。当网络摄像被集体安置在某个独立网络上时，不仅能减少网络的带宽占用，还能防止外部连接到摄像机。

日常攻击来源——网络连接
一台受攻击牵连全系统

我们都知道最好不要把鸡蛋放在同一个篮子里，不过，电脑用户却越来越倾向于将所有信息放在同一个网络里，这样的风险在于，如果一台计算机受到攻击，那么整个系统可能面临着向攻击者“敞开大门”的危险。

试想一下某公司正在进行电话会议，而正在使用的，具有网络功能的“电话”有一个没有被发觉的内置“故障”，能让攻击者监听到“电话”附近的任何对话，该是多么可怕，而同样的事件在2012年确实发生过。当时，美国思科公司推出的大热IP电话中，共有16个版本受到影响。之后，思科公司急忙发布了补丁，多亏各家公司的安全部门，补丁得以安装成功。

2017年，类似的问题又发生在医院里，起因在于某品牌医院级别的洗碗机受到了不安全网络服务器的影响。而医院情况相对更复杂，因为这有可能关系到大量的私人数据和专业设备，而且当补丁终于发布后，还需要专门的技术人员来操作。

■出招

个人怎么防 记得多扫描

对于普通用户，防住U盘风险还是很容易的，需要的只有细心，还有就是不要有侥幸心理。首先，每次使用外部储存设备时，都应当确保杀毒软件自动扫描，虽然还是会有大约20%的病毒侥幸躲过杀毒软件的扫描，但这一步至少能阻止被感染的U盘自动运行。

其次，当使用新外接设备时，可以尝试禁止让操作系统自动安装驱动程序和其他软件。不同操作系统的设置有所不同，但大多数都有这一选项。Windows用户的这一步相对简单，Linux用户有许多不同方法，Mac用户可以不用担心这一点，因为系统不支持自动运行。

另外，尽管我们很信任自己的同事和朋友，但是最好不要“爱屋及乌”，无条件地信任他们的U盘。他们自己可能都不知道U盘被感染了，当然也不会及时告诉你要多加小心。最保险的方法还是每次都扫描，再打开U盘。

企业怎么防 设条新网络

为了保护企业不受“感染”影响，需要建立基本的网络“卫生”程序：

经常杀毒，购买、安装最新版本的杀毒软件，在保护模式下运行它，扫描机器上的所有东西，因为即使是以安全著称的Mac电脑也会感染病毒。

监控外接设备时，避免使用U盘这样容易被感染的设备，不管接入任何设备，都设置成“阻止自动运行”。

隔离网络，如果公司有重要的基础设施，不要让它和每天日常使用的、可供公共或访客使用的网络放在一起。

定期更新，修补系统中的已知漏洞。

本版编译 陈小丹