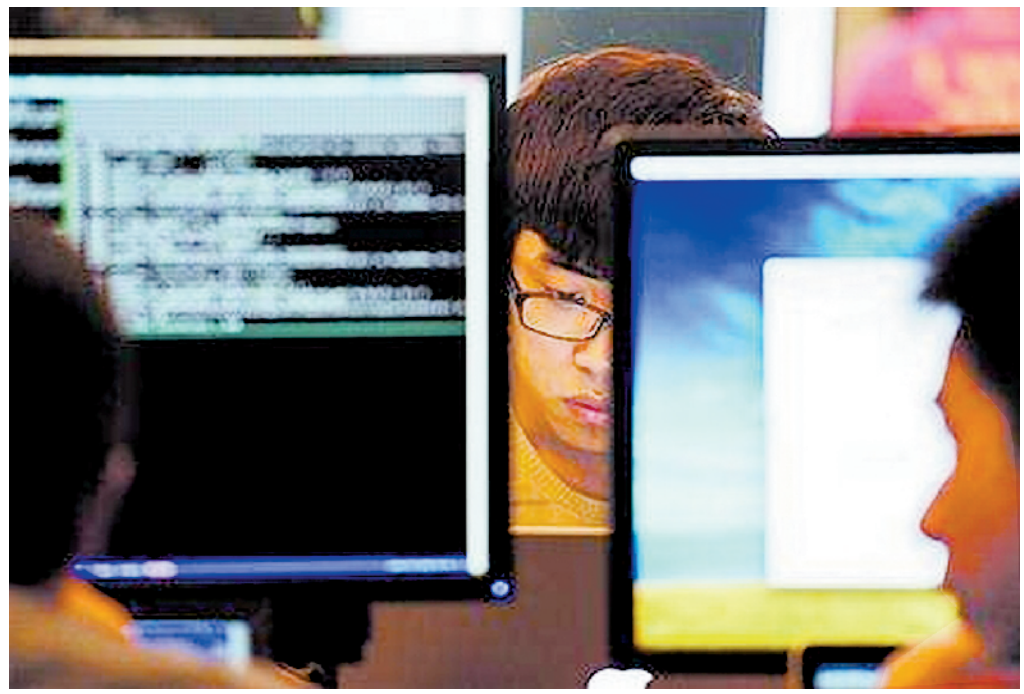
晚报广告咨询热线：6263965
投稿邮箱：xywbnews@126.com

小心黑客用电源线顺走数据

定期清理涉密计算机，加密重要数据



电脑是上班族的办公必备，为防止黑客攻击、信息泄露，很多人隔三差五就会对其进行杀毒或清理，可谓爱护有加。而对给它提供电力支持的电源线，却鲜有人关注。但就是这根“默默无闻”的线，最近却赚足了眼球。

“通过电源线可以从隔离的电脑中窃取数据，从而实现攻击。”日前，以色列本古里安大学的研究人员撰写了一篇题为《PowerHammer：通过电源线窃取隔离电脑的数据》的论文，详细介绍了这种攻击手段，研究人员将这种数据窃取技术命名为“PowerHammer”。

消息一出，迅速刷爆了朋友圈。我们的信息真会从电线中泄露出去吗？事实究竟是怎样的？

电线如何传输信息

将数据以信号形式加载到电流中

“电源线确实可以泄露数据。”5 月 15 日，北京邮电大学信息与通信工程学院教授牛凯在接受《科技日报》记者采访时说，之前学界已有人提出过类似的技术。

对此，北京理工大学计算机学院网络安全等级保护国家工程实验室副教授闫怀志表示，使用电源线进行攻击是一种典型的针对网络物理隔离设备进行的旁路攻击。物理隔离是指计算机不与任何联网设备相接，与网络完全隔离，从而使数据得到保护。

“日常生活中，利用电线来传输数据和媒体信号是一种常见的数据传输方式，这种方式被称为电力线载波通信。”闫怀志说，载波的电线可以是高压线、中压线或低压配电线。家庭中常用的电线通讯调制解调器（俗称电力猫）就是利用市电电线进行网络 IP 数字信号传输的鲜活实例。若这种方式被恶意利用，就可能带来数据泄露的风险。

据牛凯介绍，“PowerHammer”攻击的核心是将被窃取数据以信号形式加载到电流中。其具体做法主要是，利用恶意软件调控计算机主板上的中央处理器，特别是为了增强隐蔽性去触发未使用的中央处理器内核，使中央处理器总体使用率发生变化。

同时，采用频移键控调制技术，恶意软件可将目标计算机的二进制数据编码成电能消耗模式，进而改变计算机的功耗，引起本地电网电流的波动。

攻击者怎么接收数据

测量电流变化并将其解码

根据“PowerHammer”的攻击原理，攻击者要接收数据，只需测量电线传输数据时电流的变化并将其解码即可。常见的方法是，将分体电流互感器夹在电源线周围来实现电流量的非入侵式感知和检测。

“接收装置感知并检测到这种变化，再通过解码实现隔离设备的数据窃取。中央处理器拥有的核芯越多，可供攻击者调控的中央处理器空间就越大，数据泄露的速度也就越快。”闫怀志说。

具体来讲，“PowerHammer”攻击可以分为“线路 PowerHammer”和“相位 PowerHammer”两种方式。接收装置越靠近攻击目标，数据传输的速率就越高。

“线路 PowerHammer”是直接利用隔离计算机和电源插座之间的电源线，如果目标计算机安装的是英特尔 Haswell 四核处理器芯片，数据读取速度可高达 1000 比特/秒。

而“相位 PowerHammer”攻击则是利用建筑内电力服务配电板的电源线相位，这种攻击方式隐蔽性更强，但是易受其他电磁设备的相位干扰。

该如何防范此类攻击

定期清理涉密计算机，加密重要数据

尽管这种攻击方式尚处在实验阶段，但不排除一些黑客用此类工具获取情报。那么，对于机构或个人用户该如何防范此类攻击？

闫怀志表示，面对此类攻击，有关机构以及个人用户应该从观念和技术两方面来加强防范。首先，在观念上要给予足够重视，破除“只有联网才会导致数据泄露”的传统观念，建立“只要有电磁连接便可被攻击者利用”的观念。

技术方面，第一要从源头上防止攻击者在目标计算机上安装恶意软件。也就是说，要做好被隔离计算机的主机防护工作，防止通过插入 U 盘等方式引入病毒。第二，要经常用恶意代码检测工具查杀恶意软件、及时打补丁修复漏洞，不给黑客以可乘之机。

“其次，可以通过使用红黑电源进行滤波屏蔽、去除不必要的电源线电流感应装置、远离金属管线（传统电话线、金属水暖管线等）等方式，让被隔离计算机实现真正的物理‘隔离’。”闫怀志强调。

在牛凯看来，个人用户最基本的防范方法是对涉密的计算机进行定期清理，及时发现黑客攻击。“其次，要对重要数据进行加密，加密是对抗截获信息比较有效的方式。这样即使数据被窃取，对方要破获这些加密文件也要付出很大的代价，有些甚至根本没办法破译。”牛凯说。

（据《科技日报》）