

## 【网警说·安全】你用的碎纸机、打印机，可能正在泄露机密！

---

乌鲁木齐网警 2026-05-31 18:26:46 新疆



2024 年，黎巴嫩接连传来巨响，数千人伤亡，这场系列爆炸案的元凶竟是看似普通却被提前动了手脚的寻呼机、对讲机。这些看似“安全”的身边之物，如何成了致命威胁？被预先恶意放置的不是炸药，而是更加微小甚至无形的窃密芯片，又将发生什么？

保密科普系列纪录片《守护：警惕身边的泄密风险》第四集《“芯”怀鬼胎》，揭露了深藏于芯片、操作系统、办公设备中的“隐形内鬼”。

### 你以为安全的设备 可能留了“后门”

现代化的通讯设备、办公设备、高精尖的电脑芯片、操作系统……这些数字时代的加速器，或许正被人通过恶意植入技术后门，变成“失泄密”的导火索。

很多技术后门的设计初衷是方便开发者调试和修改漏洞，但若被恶意攻击者利用，就会变成安全风险。

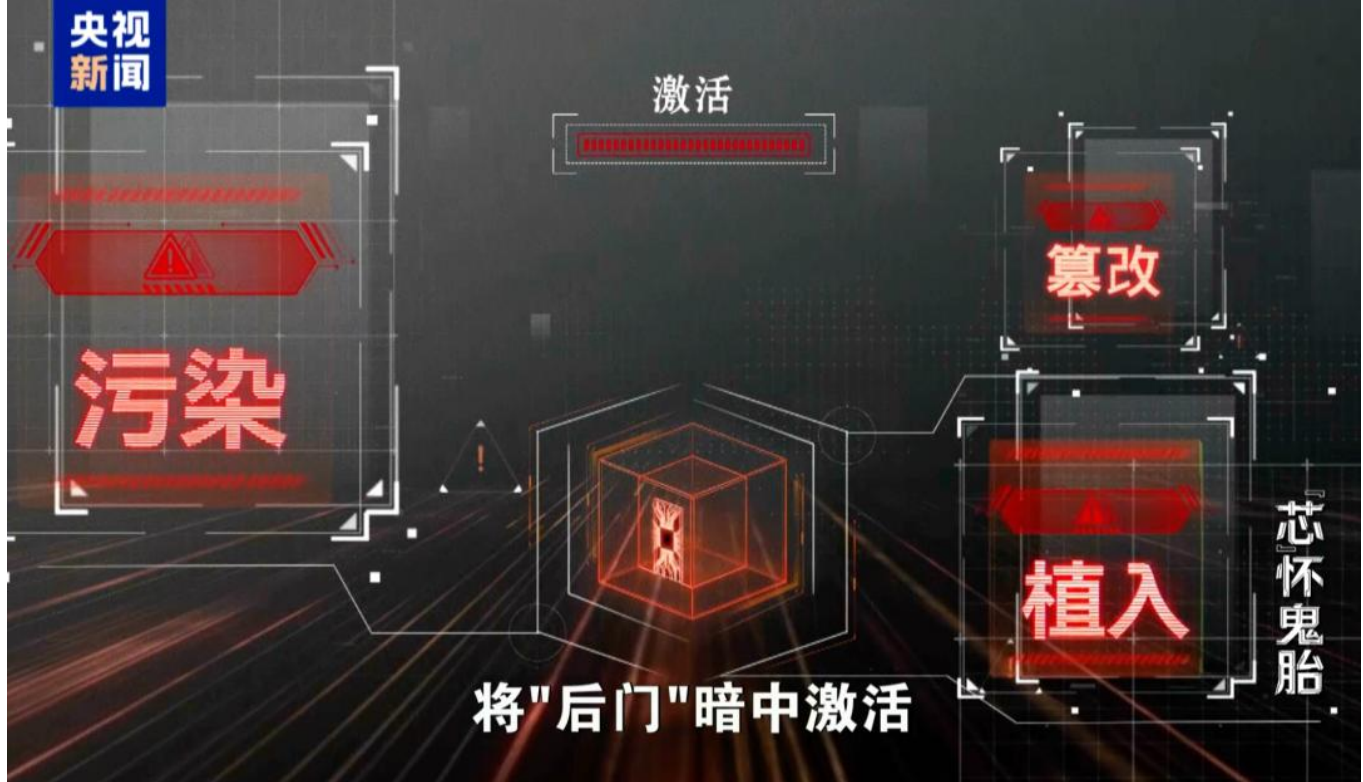
北京航空航天大学教授张悦解释，“后门”是一种形象的比喻，它可以让我们对芯片的控制失灵、失效，是芯片里的隐形内鬼。

如此危险的“后门”，可能来自生产厂商的“恶意自带”、第三方远程访问接口的“恶意破解”、窃密者的“恶意植入”，通过污染开源代码库、篡改软件更新包、供应链环节植入恶意代码，将“后门”暗中激活。

还有些漏洞源于设计缺陷，一旦被境外间谍情报机构锁定、利用，就会沦为国家级攻击者的“无形利器”。它们可以绕过层层防护，在不触发任何警报的前提下窃取国家秘密。

清华大学副研究员吕勇强指出，隐藏在芯片里的“后门”或漏洞，具有很强的隐蔽性。只要用了这款芯片，就可能导致信息泄密。

天津大学副教授陆明远表示，利用“后门”（漏洞）发起的攻击，具有长期潜伏、系统性破坏的特征，“意图在于对一个国家大量的信息进行全方位、长周期、持续的夺取或摧毁”。



你以为可靠的软件  
可能在“悄悄搬运”

除了极其微小、肉眼难辨的硬件漏洞，危险“后门”还可能在各种系统、软件中隐于无形。

2025 年初，当世界将目光聚焦在哈尔滨亚冬会的激烈赛场时，一场网络攻防战也正在打响——短短几天内，我方累计拦截境外网络攻击超过 27 万次！

案件细节显示，网络攻击者曾向黑龙江省内多个基于某国外操作系统的特定设备发送未知加密字节，目的似乎是为了唤醒、激活该操作系统提前预留的特定“后门”。



张悦表示，软件“后门”是一种嵌入指令，当使用软件时，就可以窃取数据、销毁破坏系统，甚至复制我们的操作行为和步骤，软件“后门”比硬件“后门”更加复杂、灵活。

吕勇强指出，和硬件相比，软件“后门”的植入成本、攻击成本更低，植入和攻击相对更容易，造成的危害多样性更显著。如果在操作系统里留下“后门”，它基本可以获得操作系统权限内所有全量的信息。

### 桌上的办公设备 可能正悄悄“出卖”你

一台碎纸机看起来毫无异常，但当你把文件投入碎纸口时，内部一枚微型扫描芯片会在粉碎前的一瞬间完成扫描，并通过无线模块将扫描数据实时发送到窃密者手中。

央视  
新闻



『芯』怀鬼胎

眼前的这台碎纸机看起来毫无异常

央视  
新闻

『芯』怀鬼胎

这枚芯片会在粉碎纸张前的一瞬间完成扫描

这不是虚构剧情，我国有关单位就曾发生真实案例。

吕勇强透露，国外间谍机构大量采用的间谍设备，就包括我们常用的 USB 键盘、USB 鼠标、VGA 连接线、投影连接线等设备，他们悄悄收集用户输入的信息，择机发送出去。

北京航空航天大学教授刘祥龙提醒，我们采购并放到办公室、涉密场所的设备，它很可能在长期监听，比如打印机装了窃听器，插座上装了针孔摄像头。



那么，这些被精心隐藏在办公设备中的“窃密之芯”究竟是何时、何地、被谁以怎样的方式安装的呢？

陆明远表示，从案例看，可能是软硬件的设计师、开发商、制造商、供货商，甚至可能是在运输和后期保养环节——也就是供应链的全周期，任何一个节点都有可能产生“后门”。

大量案例揭示，从生产制造、设备运输到使用、维修，巨大的风险隐患正深藏于国家基础供应链中最隐蔽的角落。任何一个细节，都容不得半点疏忽大意。

只有加强办公设备采购、使用、维修、报废的全周期保密管理，进一步推动硬件、软件全面自主可控，方可让“芯”怀鬼胎的窃密者再无可乘之机。

来源：首都网警

[阅读原文](#)