ID：T1200

策略：初始访问

平台：Windows、Linux、MacOS

数据来源：资产管理、数据丢失预防

硬件添加(Hardware Additions)

计算机附件、计算机或网络硬件可以作为一种媒介引入系统以获得执行。虽然 APT 组使用此方法的公开参考很少，但许多渗透测试人员利用硬件添加进行初始访问。商业和开源产品经常被使用，他们有如下的功能：passive network tapping [1]、中间人加密破解[2]、键盘输入注入[3]、通过 DMA 读取内核内存[4]、为现有网络添加新的无线访问[5]等功能。

缓解

建立网络访问控制策略，例如使用设备证书和 802.1X 标准。[6]限制对已注册设备使用 DHCP，以防止未注册设备与受信任系统通信。
通过端点安全配置和监视代理阻止未知设备和附件。

检测

资产管理系统可能有助于检测不应存在于网络内的计算机系统或网络设备。
端点安全设备可以检测通过 USB、Thunderbolt 和其他外部设备通信端口添加的新设备。