黑店，又名Darkhotel、APT-C-06，被认为是来自朝鲜半岛方向的具有国家背景的 APT组织，自披露以来一直活跃，长期针对企业、政府机构、国防工业、电子工业等重要机构实施网络间谍攻击活动，其足迹遍布中国、朝鲜、日本、缅甸、俄罗斯等国家。

2020年3-4月，该组织劫持中国境内部分单位的深信服科技股份有限公司（以 下简称“深信服”）SSL VPN设备，下发伪装成升级文件的恶意程序，对中国大量驻外机构、政府相关单位发动定向攻击。CNCERT/CC和北京奇虎科技有限公司监 测发现，攻击者控制了部分单位的VPN服务器，并控制了部分相关单位的计算机终端设备。黑店组织的攻击过程是首先劫持VPN服务器，再通过该服务器下发伪装成升级程序的木马给用户。

攻击者通过密码爆破，猜解SSL VPN后台管理页面登录账号和密码，控制部分SSL VPN服务器。攻击者通过后台管理权限，利用木马文件替换Windows客户端升级程序，模仿正常程序对木马程序进行了签名伪装，使普通人难以察觉。攻击者在此攻击过程中，利用了深信服SSL VPN设备存在的逻辑漏洞来下发木马。VPN客户端启动连接VPN服务器时，默认触发一个升级行为，在固定位置获取升级信息，下载名为SangforUD.exe的升级程序执行。VPN客户端未对下载的升级程序做有效的安全检查，导致被替换成的木马程序可以在客户端中正常启动和运行。木马程序启动后，访问远程的控制端服务器下载shellcode并执行。shellcode会获取终端的IP/MAC/系统版本/进程等软硬件信息，上传至远程的控制端服务器，并下载第二阶段shellcode。该shellcode会加载核心的后门恶意组件（thinmon.dll）； thinmon.dll解密云端下发的另外一个加密文件Sangfor\_tmp\_1.dat，以加载、线程启 动、注入进程3种方式中的一种启动dat文件；最终由dat文件内的恶意代码实现与服务器交互执行恶意操作。

从以上事例可以看出，APT组织多次对攻击目标采用供应链攻击。例如，新冠肺炎疫情防控下的远程办公需求明显增多，虚拟专用网络（VPN）成为远程办公人员接入单位网络的主要技术手段之一。在此背景下，相当多APT组织通过控制VPN服务器，将木马文件伪装成VPN客户端升级包，下发给使用这些VPN服务器的重要单位。

这也提醒着我们要对远程协作环境下的薄弱环节，例如重点使用的工具、协议以及所依赖的信息基础设施引起重视，需要继续加强相关的安全解决措施和手段。