ID：T1091

策略：横向移动，初始进入

平台：Windows

所需权限：用户

数据源：文件监控、数据丢失预防

Replication Through Removable Media 通过可移动媒体传播

攻击者可以通过将恶意软件复制到可移动介质上，并利用介质插入系统时自动执行的功能，将恶意软件转移到系统上，包括那些处于隔离网络上的系统。在横向移动的情况下，这个战术可以通过修改存储在可移动媒体上的可执行文件或通过复制恶意软件并将其重命名为合法文件来欺骗用户在隔离的系统上执行。在初始访问的情况下，可能通过手动操作介质、修改用于初始格式化介质的系统或修改介质固件本身来实现。

缓解

如果不必要，请禁用自动运行功能。[11]如果业务操作不需要可移动介质，则在组织策略级别上禁用或限制可移动介质。〔12〕
识别可能用于感染可移动介质或可能由受污染的可移动介质传播的潜在恶意软件，并通过使用白名单[13]工具（如 AppLocker，[14][15]或软件限制策略[16]）进行审计和/或阻止。〔17〕

检测

监视可移动介质上的文件访问。检测在装入可移动介质后或由用户启动时从该介质执行的进程。如果以这种方式使用远程访问工具进行横向移动，那么执行之后可能会发生其他操作，例如打开网络连接以进行命令和控制以及系统和网络信息发现。