保护Windows更新服务免遭恶意利用 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/272/2021_2022__E4_BF_9D_E6_8A_A4Wind_c100_272176.htm 如果您是一位Windows的用户，就需要注意到微软网站上看一下，您就会发现评述一个称为Win32/Jowspry的恶意程序的报告。这个恶意程序利用了Windows的自动更新服务将文件下载到用户的计算机上，对用户的计算机系统大肆进行破坏。当然，你可能会想到，一个理智的做法是停止使用Windows的更新服务，这可以防止恶意软件的安装。虽然“ 防守是最好的攻击。 ”但如何保障一台Windows计算机在更新时免受新的安全威胁呢？ 任何问题总有解决的办法。我们知道，计算机系统要与Windows的更新站点进行交互，就必须使用后台智能传输服务，即所谓的BITS.BITS利用用户系统未用的带宽来下载补丁和更新文档。它还使得Windows服务器更新服务、系统管理服务器以及微软的即时通信产品的文件传输更加容易。在许多系统中包含BITS功能，如Windows XP Service Pack 1、Windows 2000 Service Pack 3以及现在最新的Windows操作系统。 我们发现，作为当前操作系统（如Windows XP和Windows Vista等）一部分的Windows防火墙允许BITS发送和接收来自互联网的数据，却不会激发任何警告。很显明，通过劫持这种服务，在试图利用 Windows漏洞时，恶意软件的作者能够快速地绕过其主要的障碍。绕过防火墙的过滤器能够在无需警告用户的情况下实现恶意文件的安装。即使用户采用了基于网络的防火墙，并尽力区分BITS可以下载的数据和绝对不能下载的数据。BITS活动的低带宽消耗和异步传输特性也会使得防火墙难

于检测任何恶意活动。 事实上，这种攻击并不是由Windows更新的缺陷引起的。任何攻击者都没有也不可能将恶意文件上传到微软的网站上用于BITS下载。要让攻击工作，用户必须先下载Win32/Jowspry并执行它。也只有这样这种特洛伊木马程序才能BITS安装额外的恶意软件。想要恶意地使用BITS，特洛伊木马程序需要存在于用户计算机上。BITS并非最初感染的攻击源。一旦将自身安装到计算机上，恶意软件就用这样一种机制绕过防火墙技术。 我们权且将这种攻击称之为Windows更新攻击，迎战这种攻击的最佳方法在于在公司的用户中增强防范意识，教育他们如何处理来自未知或意外的源站点的信息（包括链接和文档、程序等）。这就会减少用户下载Jowspry或其它能够感染计算机的恶意程序的机会。一些安全专家建议将BITS限制为只能给经核准的或可信任的站点或链接。然而，许多第三方的软件厂商用它来发布软件更新，这种限制就会引起不少麻烦，你需要仔细维护经认可的站点，需要筹划该将哪些站点列入优良者名单。 虽然这种攻击只不过是众多攻击中的小菜一碟，不过却向我们展示了各种攻击日益增加的复杂性和惊人的发展速度，并可以帮助我们深入理解Windows操作系统本身。 