Atitit.制作远程管理以及 木马病毒可利用的接口

Shell接口，gui接口

WMIC扩展[WMI](http://baike.baidu.com/view/442461.htm" \t "http://baike.baidu.com/_blank)（Windows Management Instrumentation，Windows管理工具） ，提供了从命令行接口和批命令脚本执行系统管理的支持。

# WMI

[编辑](http://baike.baidu.com/javascript:;)

WMI，是Windows 2K/XP管理系统的核心；对于其他的Win32操作系统，WMI是一个有用的插件。WMI以CIMOM为基础，CIMOM即[公共信息模型](http://baike.baidu.com/view/1608239.htm" \t "http://baike.baidu.com/_blank)对象管理器（Common Information Model Object Manager），是一个描述操作系统构成单元的对象数据库，为MMC和[脚本程序](http://baike.baidu.com/view/69991.htm" \t "http://baike.baidu.com/_blank)提供了一个访问操作系统构成单元的公共接口。有了WMI，[工具软件](http://baike.baidu.com/view/1928598.htm" \t "http://baike.baidu.com/_blank)和脚本程序访问操作系统的不同部分时不需要使用不同的API；相反，操作系统的不同部分都可以插入WMI，如图所示，工具软件和脚本程序可以方便地读写WMI

如前所述，WMI允许通过一个公共的接口访问多种操作系统构成单元，因此不必分别对待各种底层接口或所谓的“提供者”。利用WMI可以高效地管理远程和本地的计算机；与此相对，并非所有的Windows 2K/XP命令行工具都支持远程运行。

WMI是WBEM模型的一种实现。WBEM即Web-Based Enterprise Management，或基于Web的企业管理，WBEM由DMTF（Distributed Management Task Force，分布式管理任务组）在许多厂商的帮助下创立，包括Compaq、Sun、Microsoft等。WBEM的目标是，为管理企业环境开发一个标准的接口集。WBEM模型最关键的部分是它的数据模型（或描述和定义对象的方式）、编码规范（Encoding Specification），以及在客户端和服务器端之间传输数据的模式。

WBEM的数据模型是CIM（Common Information Model，[公共信息模型](http://baike.baidu.com/view/1608239.htm" \t "http://baike.baidu.com/_blank)）。CIM是一个用来命名计算机的物理和[逻辑单元](http://baike.baidu.com/view/1520672.htm" \t "http://baike.baidu.com/_blank)的标准的命名系统（或称为命名模式），例如硬盘的[逻辑分区](http://baike.baidu.com/view/143399.htm" \t "http://baike.baidu.com/_blank)、正在运行的应用的一个实例，或者一条电缆。

CIM是一个[面向对象](http://baike.baidu.com/view/125370.htm" \t "http://baike.baidu.com/_blank)的模型，使用一组面向对象的术语进行描述。CIM包含类（Class)，类是被管理单元的模板。类的实例称为对象（Object），对象代表着底层系统的一个具体单元。[名称空间](http://baike.baidu.com/view/94227.htm" \t "http://baike.baidu.com/_blank)（Namespace）是一个类的集合，每个名称空间面向一个特定的管理领域。类包含属性（Property）和方法（Method）。

CIM分三层。第一层是核心模型（Core Model），这一层包含的类定义对于所有管理领域来说都是共同的。第二层是公共模型（Common Model），这一层包含的类定义对于特定的管理领域来说是公共的，但与具体的操作系统和系统设计无关。第三层是扩展模型（Extension model），这一层包含的类定义与特定的操作系统或技术有关。

WMI是Microsoft扩展CIM 2.0得到的面向Win32系统的扩展模型。引用WMI类和属性的形式是“扩展前缀\_类名称.属性名称”，例如Win32\_ComputerSystem. Name，其中Win32是CIM模式cimv2[名称空间](http://baike.baidu.com/view/94227.htm" \t "http://baike.baidu.com/_blank)内WMI扩展类的前缀，ComputerSystem是类，Name是属性。