

专注APT攻击与防御

<https://micropoor.blogspot.com/>

从xp开始默认有.net framework,在powershell后，调用起来更方便。

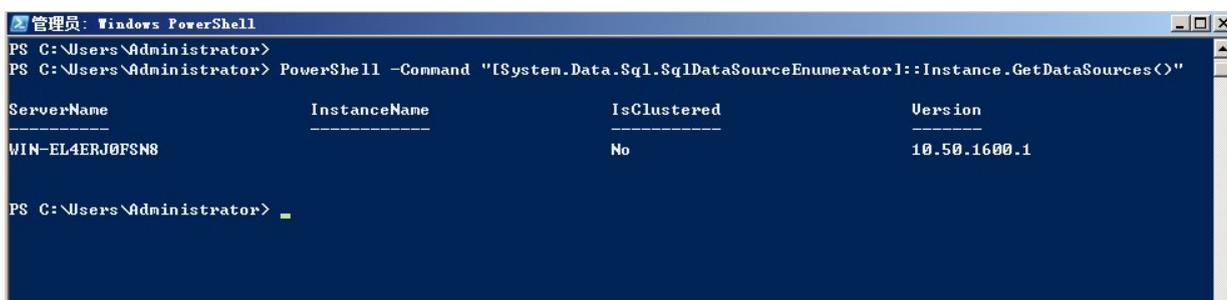
连载1

System.Data.SqlClient 命名空间是用于 SQL Server 的 .NET 数据提供程序。在net framework2.0中新增加SqlDataSourceEnumerator类。提供了一种枚举本地网络内的所有可用SQL Server实例机制。微软官方是这样解释的：

SQL Server 2000 和 SQL Server 2005 进行应用程序可以确定在当前网络中的 SQL Server 实例存在。 SqlDataSourceEnumerator类公开给应用程序开发人员，提供此信息 DataTable包含所有可用的服务器的信息。 返回此表列出了与列表匹配提供当用户尝试创建新的连接的服务器实例以及Connection Properties对话框中，展开下拉列表，其中包含所有可用的服务器。

PowerShell -Command "

[System.Data.Sql.SqlDataSourceEnumerator]::Instance.GetDataSources()"



```
管理员: Windows PowerShell
PS C:\Users\Administrator>
PS C:\Users\Administrator> PowerShell -Command "[System.Data.Sql.SqlDataSourceEnumerator]::Instance.GetDataSources()"

ServerName          InstanceName        IsClustered        Version
-----
WIN-EL4ERJ0FSN8    (blank)            No                  10.50.1600.1

PS C:\Users\Administrator> _
```

```
Event Log X Beacon 10.124.148.8@10744 X Beacon 10.124.42.248@6192 X Proxy P
[+] received output:

ServerName      InstanceName    IsClustered    Version
-----
FWZXNQFWPT     VIM_SQLEXP     No             10.50.2500.0
QXD XM-SERVER   VIM_SQLEXP     No             9.00.2047.00
QXD XM-SERVER   VIM_SQLEXP     No             10.50.2500.0
DLFW-WIN16     SQLSERVER      No             13.0.1300.275
VCENTER        No             10.0.1600.22
SSD400CTI     No             8.00.194
2015PUBSQL2008
CMCCWAP
JSDIANLINEW
NONGQ-WULIANWAN
ONEKEYPUBLISHDB
PUBLIC_SERVER
TEMPLATEW2008
```

此种方法，在实战中，不留文件痕迹。并且信息准确，发现主机也可。可应对目前主流安全防护产品。

- Micropoor