Windows Management Instrumentation, Technique T1047 - Enterprise

Archived: 2026-04-05 16:09:44 UTC

C0025 2016 Ukraine Electric Power Attack

During the 2016 Ukraine Electric Power Attack, WMI in scripts were used for remote execution and system surveys. [5]

S1028 Action RAT

Action RAT can use WMI to gather AV products installed on an infected host.[6]

S0331 Agent Tesla

Agent Tesla has used wmi queries to gather information from the system.[7]

S1129 Akira

Akira will leverage COM objects accessed through WMI during execution to evade detection.[8]

G0016 APT29

APT29 used WMI to steal credentials and execute backdoors at a future time.[9]

G0050 APT32

APT32 used WMI to deploy their tools on remote machines and to gather information about the Outlook process. [10]

G0096 APT41

APT41 used WMI in several ways, including for execution of commands via WMIEXEC as well as for persistence via PowerSploit.[11][12] APT41 has executed files through Windows Management Instrumentation (WMI).[13]

G1044 APT42

APT42 has used Windows Management Instrumentation (WMI) to query anti-virus products.[14]

G0143 Aquatic Panda

Aquatic Panda used WMI for lateral movement in victim environments.[15]

S0373 Astaroth

Astaroth uses WMIC to execute payloads. [16]

S0640 Avaddon

Avaddon uses wmic.exe to delete shadow copies.[17]

S1081 BADHATCH

BADHATCH can utilize WMI to collect system information, create new processes, and run malicious PowerShell scripts on a compromised machine.[18][19]

S0534 Bazar

Bazar can execute a WMI query to gather information about the installed antivirus engine.[20][21]

S1070 Black Basta

Black Basta has used WMI to execute files over the network.[22]

G1043 BlackByte

BlackByte used WMI to delete Volume Shadow Copies on victim machines.[23]

S1068 BlackCat

BlackCat can use `wmic.exe` to delete shadow copies on compromised networks.[24]

S0089 BlackEnergy

A BlackEnergy 2 plug-in uses WMI to gather victim host details.[25]

G0108 Blue Mockingbird

Blue Mockingbird has used wmic.exe to set environment variables.[26]

S1063 Brute Ratel C4

Brute Ratel C4 can use WMI to move laterally.[27]

S1039 Bumblebee

Bumblebee can use WMI to gather system information and to spawn processes for code injection.[28][29][30]

C0015 C0015

During C0015, the threat actors used `wmic` and `rundll32` to load Cobalt Strike onto a target host.[31]

C0018 C0018

During C0018, the threat actors used WMIC to modify administrative settings on both a local and a remote host, likely as part of the first stages for their lateral movement; they also used WMI Provider Host (`wmiprvse.exe`) to execute a variety of encoded PowerShell scripts using the `DownloadString` method.[32][33]

C0027 C0027

During C0027, Scattered Spider used Windows Management Instrumentation (WMI) to move laterally via Impacket.[34]

S0674 CharmPower

CharmPower can use `wmic` to gather information from a system.[35]

G0114 Chimera

Chimera has used WMIC to execute remote commands.[36][37]

G1021 Cinnamon Tempest

Cinnamon Tempest has used Impacket for lateral movement via WMI.[38][39]

S0154 Cobalt Strike

Cobalt Strike can use WMI to deliver a payload to a remote host.[40][41][31]

S1155 Covenant

Covenant can utilize WMI to install new Grunt listeners through XSL files or command one-liners.[42]

S0488 CrackMapExec

CrackMapExec can execute remote commands using Windows Management Instrumentation.[43]

S1111 DarkGate

DarkGate has used WMI to execute files over the network and to obtain information about the domain.[44]

S1066 DarkTortilla

DarkTortilla can use WMI queries to obtain system information.[45]

S0673 DarkWatchman

DarkWatchman can use WMI to execute commands.[46]

S0616 DEATHRANSOM

DEATHRANSOM has the ability to use WMI to delete volume shadow copies.[47]

G0009 Deep Panda

The Deep Panda group is known to utilize WMI for lateral movement.[48]

S0062 DustySky

The DustySky dropper uses Windows Management Instrumentation to extract information about the operating system and whether an anti-virus is active.[49]

G1006 Earth Lusca

Earth Lusca used a VBA script to execute WMI.[50]

S0605 EKANS

EKANS can use Windows Mangement Instrumentation (WMI) calls to execute operations.[51]

G1003 Ember Bear

Ember Bear has used WMI execution with password hashes for command execution and lateral movement.[52]

S0367 Emotet

Emotet has used WMI to execute powershell.exe.[53]

S0363 Empire

Empire can use WMI to deliver a payload to a remote host.[54]

S0396 EvilBunny

EvilBunny has used WMI to gather information about the system.[55]

S0568 EVILNUM

EVILNUM has used the Windows Management Instrumentation (WMI) tool to enumerate infected machines.[56]

S0267 FELIXROOT

FELIXROOT uses WMI to query the Windows Registry.[57]

G1016 FIN13

FIN13 has utilized `WMI` to execute commands and move laterally on compromised Windows machines.[58][59]

G0037 FIN6

FIN6 has used WMI to automate the remote execution of PowerShell scripts.[60]

G0046 FIN7

FIN7 has used WMI to install malware on targeted systems.[61]

G0061 FIN8

FIN8's malicious spearphishing payloads use WMI to launch malware and spawn `cmd.exe` execution. FIN8 has also used WMIC and the Impacket suite for lateral movement, as well as during and post compromise cleanup activities.[62][63][64][65]

S0618 FIVEHANDS

FIVEHANDS can use WMI to delete files on a target machine.[47][66]

S0381 FlawedAmmyy

FlawedAmmyy leverages WMI to enumerate anti-virus on the victim.[67]

C0001 Frankenstein

During Frankenstein, the threat actors used WMI queries to check if various security applications were running as well as to determine the operating system version.[68]

S1044 FunnyDream

FunnyDream can use WMI to open a Windows command shell on a remote machine.[69]

C0007 FunnyDream

During FunnyDream, the threat actors used `wmiexec.vbs` to run remote commands.[69]

G0093 GALLIUM

GALLIUM used WMI for execution to assist in lateral movement as well as for installing tools across multiple assets.[70]

G0047 Gamaredon Group

Gamaredon Group has used WMI to execute scripts used for discovery and for determining the C2 IP address.[71][72][73][74] Gamaredon Group has used the following WMI query to search for a ping record: `Select * From Win32_PingStatus where Address = 'mil.gov.ua'`.[73]

S0237 GravityRAT

GravityRAT collects various information via WMI requests, including CPU information in the Win32_Processor entry (Processor ID, Name, Manufacturer and the clock speed).[75]

S0151 HALFBAKED

HALFBAKED can use WMI queries to gather system information.[76]

S0617 HELLOKITTY

HELLOKITTY can use WMI to delete volume shadow copies.[47]

S0698 HermeticWizard

HermeticWizard can use WMI to create a new process on a remote machine via `C:\windows\system32\cmd.exe /c start C:\windows\system32\\regsvr32.exe /s /iC:\windows\<filename>.dll`.[77]

C0038 HomeLand Justice

During HomeLand Justice, threat actors used WMI to modify Windows Defender settings.[78]

S0376 HOPLIGHT

HOPLIGHT has used WMI to recompile the Managed Object Format (MOF) files in the WMI repository.[79]

S0483 IcedID

IcedID has used WMI to execute binaries.[80][81]

S1152 IMAPLoader

IMAPLoader uses WMI queries to query system information on victim hosts.[82]

S0357 Impacket

Impacket's `wmiexec` module can be used to execute commands through WMI.[83][84]

G1032 INC Ransom

INC Ransom has used WMIC to deploy ransomware.[85][86][87]

S1139 INC Ransomware

INC Ransomware has the ability to use wmic.exe to spread to multiple endpoints within a compromised environment.[86][88]

G0119 Indrik Spider

Indrik Spider has used WMIC to execute commands on remote computers.[89]

S0283 jRAT

jRAT uses WMIC to identify anti-virus products installed on the victim’s machine and to obtain firewall details.[90]

S0265 Kazuar

Kazuar obtains a list of running processes through WMI querying.[91]

S0250 Koadic

Koadic can use WMI to execute commands.[92]

S0156 KOMPROGO

KOMPROGO is capable of running WMI queries.[93]

S1160 Latrodectus

Latrodectus has used WMI in malicious email infection chains to facilitate the installation of remotely-hosted files.[94][95]

G0032 Lazarus Group

Lazarus Group has used WMIC for discovery as well as to execute payloads for persistence and lateral movement.[96][97][98][99]

G0065 Leviathan

Leviathan has used WMI for execution.[100]

S1199 LockBit 2.0

LockBit 2.0 can use wmic.exe to delete volume shadow copies.[101]

G0030 Lotus Blossom

Lotus Blossom has used WMI to enable lateral movement.[102]

S0532 Lucifer

Lucifer can use WMI to log into remote machines for propagation.[103]

S1141 LunarWeb

LunarWeb can use WMI queries for discovery on the victim host.[104]

G0059 Magic Hound

Magic Hound has used a tool to run `cmd /c wmic computersystem get domain` for discovery.[105]

S0449 Maze

Maze has used WMI to attempt to delete the shadow volumes on a machine, and to connect a virtual machine to the network domain of the victim organization's network.[106][107]

G1051 Medusa Group

Medusa Group has utilized Windows Management Instrumentation to query system information.[108][109][110]

G0045 menuPass

menuPass has used a modified version of pentesting script wmiexec.vbs, which logs into a remote machine using WMI.[111][112][113]

S0688 Meteor

Meteor can use `wmic.exe` as part of its effort to delete shadow copies.[114]

S0339 Micropsia

Micropsia searches for anti-virus software and firewall products installed on the victim's machine using WMI.[115][116]

S0553 MoleNet

MoleNet can perform WMI commands on the system.[117]

S0256 Mosquito

Mosquito's installer uses WMI to search for antivirus display names.[118]

G0069 MuddyWater

MuddyWater has used malware that leveraged WMI for execution and querying host information.[119][120][121][122]

G0129 Mustang Panda

Mustang Panda has executed PowerShell scripts via WMI.[123][124]

G0019 Naikon

Naikon has used WMIC.exe for lateral movement.[125]

S0457 Netwalker

Netwalker can use WMI to delete Shadow Volumes.[126]

S0368 NotPetya

NotPetya can use `wmic` to help propagate itself across a network.[127][128]

S0340 Octopus

Octopus has used wmic.exe for local discovery information.[129]

G0049 OilRig

OilRig has used WMI for execution.[130][131]

S0365 Olympic Destroyer

Olympic Destroyer uses WMI to help propagate itself across a network.[132]

S0264 OopsIE

OopsIE uses WMI to perform discovery techniques.[133]

C0022 Operation Dream Job

During Operation Dream Job, Lazarus Group used WMIC to executed a remote XSL script.[134]

C0014 Operation Wocao

During Operation Wocao, threat actors has used WMI to execute commands.[135]

S0378 PoshC2

PoshC2 has a number of modules that use WMI to execute tasks.[136]

S0194 PowerSploit

PowerSploit's `Invoke-WmiCommand` CodeExecution module uses WMI to execute and retrieve the output from a PowerShell payload.[137][138]

S0223 POWERSTATS

POWERSTATS can use WMI queries to retrieve data from compromised hosts.[139][120]

S0184 POWRUNER

POWRUNER may use WMI when collecting information about a victim.[140]

S0654 ProLock

ProLock can use WMIC to execute scripts on targeted hosts.[141]

S1228 PUBLOAD

PUBLOAD has used `wmic` to gather information from the victim device.[142]

S1032 PyDCrypt

PyDCrypt has attempted to execute with WMIC.[143]

S0650 QakBot

QakBot can execute WMI queries to gather information.[144]

S1130 Raspberry Robin

Raspberry Robin can execute via LNK containing a command to run a legitimate executable, such as wmic.exe, to download a malicious Windows Installer (MSI) package.[145]

S0241 RATANKBA

RATANKBA uses WMI to perform process monitoring.[146][147]

S0375 Remexi

Remexi executes received commands with wmic.exe (for WMI commands). [148]

S0496 REvil

REvil can use WMI to monitor for and kill specific processes listed in its configuration file.[149][150]

S0270 RogueRobin

RogueRobin uses various WMI queries to check if the sample is running in a sandbox.[151][152]

G0034 Sandworm Team

Sandworm Team has used Impacket's WMIexec module for remote code execution and VBScript to run WMI queries.[5][153]

S1085 Sardonic

Sardonic can use WMI to execute PowerShell commands on a compromised machine.[154]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors used WMI for execution.[155]

S0546 SharpStage

SharpStage can use WMI for execution.[117][156]

S1178 ShrinkLocker

ShrinkLocker uses WMI to query information about the victim operating system.[157]

S0589 Sibot

Sibot has used WMI to discover network connections and configurations. Sibot has also used the Win32_Process class to execute a malicious DLL.[158]

S0692 SILENTTRINITY

SILENTTRINITY can use WMI for lateral movement.[159]

S1086 Snip3

Snip3 can query the WMI class `Win32_ComputerSystem` to gather information.[160]

S1124 SocGholish

SocGholish has used WMI calls for script execution and system profiling.[161]

C0024 SolarWinds Compromise

During the SolarWinds Compromise, APT29 used WMI for the remote execution of files for lateral movement.[162][163]

G0038 Stealth Falcon

Stealth Falcon malware gathers system information via Windows Management Instrumentation (WMI).[164]

S0380 StoneDrill

StoneDrill has used the WMI command-line (WMIC) utility to run tasks.[165]

S0603 Stuxnet

Stuxnet used WMI with an `explorer.exe` token to execute on a remote share.[166]

S0559 SUNBURST

SUNBURST used the WMI query `Select * From Win32_SystemDriver` to retrieve a driver listing.[167]

S1064 SVCReady

SVCReady can use `WMI` queries to detect the presence of a virtual machine environment.[168]

S0663 SysUpdate

SysUpdate can use WMI for execution on a compromised host.[169]

G1018 TA2541

TA2541 has used WMI to query targeted systems for security products.[170]

S1193 TAMECAT

TAMECAT has used Windows Management Instrumentation (WMI) to query anti-virus products.[14]

G0027 Threat Group-3390

A Threat Group-3390 tool can use WMI to execute a binary.[171]

G1022 ToddyCat

ToddyCat has used WMI to execute scripts for post exploit document collection.[172]

S1239 TONESHELL

TONESHELL has used WMI queries to gather information from the system.[173]

S0386 Ursnif

Ursnif droppers have used WMI classes to execute PowerShell commands.[174]

S0476 Valak

Valak can use `wmic process call create` in a scheduled task to launch plugins and for execution.[175]

G1047 Velvet Ant

Velvet Ant used the `wmiexec.py` tool within Impacket for remote process execution via WMI.[84]

G1017 Volt Typhoon

Volt Typhoon has leveraged WMIC for execution, remote system discovery, and to create and use temporary directories.[176][177][178][179]

S0366 WannaCry

WannaCry utilizes `wmic` to delete shadow copies.[180][181][182]

G0112 Windshift

Windshift has used WMI to collect information about target machines.[183]

G0102 Wizard Spider

Wizard Spider has used WMI and LDAP queries for network discovery and to move laterally. Wizard Spider has also used batch scripts to leverage WMIC to deploy ransomware.[184][185][186][187][188]

S0251 Zebrocy

One variant of Zebrocy uses WMI queries to gather information.[189]

Source: https://attack.mitre.org/techniques/T1047