


Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

🔍

Sign in

Sign up

 RedSiege / WMImplant

Public

🔔 Notifications

🍴 Fork 143

★ Star 802

<> Code

🕒 Issues

🔗 Pull requests 1

🎬 Actions

📁 Projects

📖 Wiki

🛡 Security

📈 Insights

🔗 master ▾

🔗

📁

<> Code ▾

LICENSE

Readme.md

WMImplant.ps1

🕒 129 Commits

📖 README

📄 GPL-3.0 license

☰

# WMImplant

WMImplant is a PowerShell based tool that leverages WMI to both perform actions against targeted machines, but also as the C2 channel for issuing commands and receiving results. WMImplant will likely require local administrator permissions on the targeted machine.

Developed by [@christruncer](#)

## WMImplant Functions:

### Meta Functions

change\_user

exit

gen\_cli

set\_default

help

-

Change the context of the user

-

Exits WMImplant

-

Generate the command line code

-

Sets the targeted system's WMI namespace

-

View the list of commands and their descriptions

### File Operations

cat

copy

download

ls

search

upload

-

Reads the contents of a file

-

Copies a file from one location to another

-

Download a file from the target

-

File/Directory listing of a path

-

Search for a file on a user's system

-

Upload a file to the target

### Lateral Movement Facilitation

command\_exec

disable\_wdigest

disable\_winrm

enable\_wdigest

enable\_winrm

registry\_mod

remote\_posh

-

Run a command line command as user

-

Removes registry value UseLogon

-

Disables WinRM on the target

-

Adds registry value UseLogon

-

Enables WinRM on the target

-

Modify the registry on the target

-

Run a PowerShell script on a target

About

This is a PowerShell based tool that is designed to act like a RAT. Its interface is that of a shell where any command that is supported is translated into a WMI-equivalent for use on a network/remote machine. WMImplant is WMI based.

📖 Readme

📄 GPL-3.0 license

📈 Activity

📁 Custom properties

★ 802 stars

👁 54 watching

🍴 143 forks

Report repository


Releases


No releases published

Packages

No packages published

Contributors 2

 **ChrisTruncer** ChrisTruncer

 **r-smith** Ryan Smith

Languages

PowerShell 100.0%

sched_job	- Manipulate scheduled jobs
service_mod	- Create, delete, or modify sy:

## Process Operations

process_kill	- Kill a process via name or pi	📄
process_start	- Start a process on the targe	
ps	- Process listing	

## System Operations

active_users	- List domain users with activ	📄
basic_info	- Used to enumerate basic meta	
drive_list	- List local and network drive:	
ifconfig	- Receive IP info from NICs wi	
installed_programs	- Receive a list of the instal	
logoff	- Log users off the targeted m	
reboot	- Reboot the targeted machine	
power_off	- Power off the targeted machi	
vacant_system	- Determine if a user is away	

## Log Operations

logon_events	- Identify users that have log	📄
--------------	--------------------------------	---

## Usage

The easiest way to get up and running with WMIimplant is to import the script and run Invoke-WMIimplant. This will present you with the main menu and you can instantly start choosing a command to run. Within the main menu, you can also choose to have WMIimplant output the command line command you would need to use in order to run WMIimplant in a non-interactive manner.

Thanks to: [@evan\\_Pena2003](#) - For your help with code reviews and adding functionality into the tool [@danielbohannon](#) - For your help with code obfuscation