



Sign in

RedSiege / WMIImplant Public

 Notifications

Fork 143



☆ Star 802

[Code](#)
[Issues](#)
[Pull requests](#)
[1](#)
[Actions](#)
[Projects](#)
[Wiki](#)
[Security](#)
[Insights](#)

master ▼



Go to file



<> Code ▼

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. WMIImplant is WMI based.

 LICENSE

 Readme.md

WMImplant.ps1

 **README**

 GPL-3.0 license



WMImplant

WMIImplant 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. WMIImplant will likely require local administrator permissions on the targeted machine.

Developed by @chrstruncer

WMImplant Functions:

Meta Functions

 [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

change_user	-	Change · 
exit	-	Exits WMI
gen_cli	-	Generates
set_default	-	Sets the
help	-	View the



ChrisTruncer ChrisTruncer



r-smith Ryan Smith

Languages

● PowerShell 100.0%

File Operations

cat	-	Reads the · 
copy	-	Copies a
download	-	Download
ls	-	File/Di
search	-	Search
upload	-	Upload

Lateral Movement Facilitation

command_exec	-	Run a co · 
disable_wdigest	-	Removes
disable_winrm	-	Disable
enable_wdigest	-	Adds req
enable_winrm	-	Enables
registry_mod	-	Modify
remote_posh	-	Run a Po
sched_job	-	Manipul
service_mod	-	Create,

Process Operations

process_kill	-	Kill a p · 
process_start	-	Start a
ps	-	Process

System Operations

active_users	-	List do	
basic_info	-	Used to	
drive_list	-	List lo	
ifconfig	-	Receive	
installed_programs	-	Receive	
logoff	-	Log use	
reboot	-	Reboot	
power_off	-	Power o	
vacant_system	-	Determi	

Log Operations

logon_events	-	Identify	
--------------	---	----------	-----------------------------------------------------------------------------------

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

