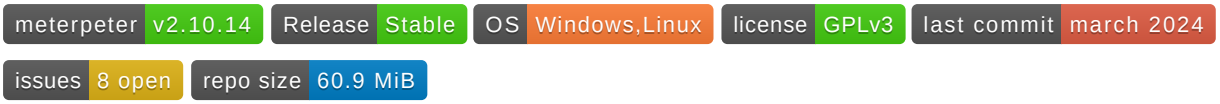
GitHub - r00t-3xp10it/meterpeter: C2 Powershell Command & Control Framework with BuiltIn Commands

By r00t-3xp10it

Archived: 2026-04-06 03:18:59 UTC



Quick Jump List

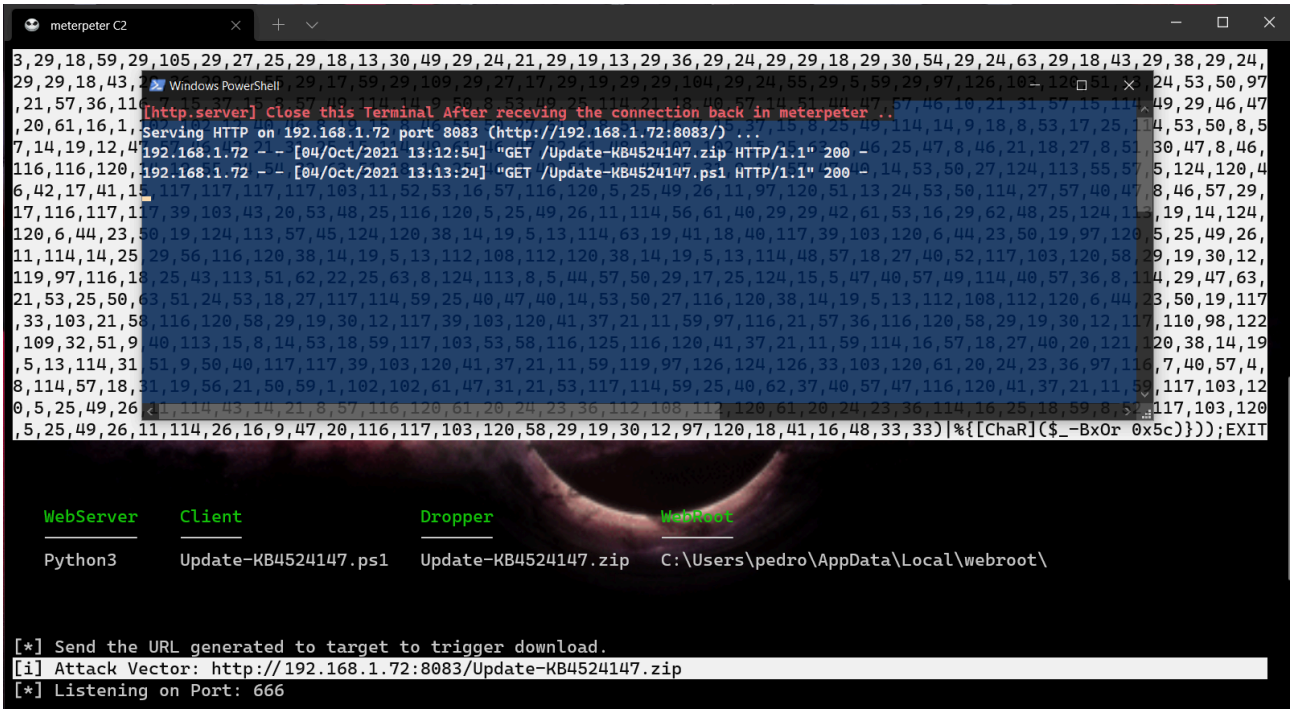
Project Description

This PS1 starts a listener Server on a Windows|Linux attacker machine and generates oneliner PS reverse shell payloads obfuscated in BXOR with a random secret key and another layer of Characters/Variables Obfuscation to be executed on the victim machine (The payload will also execute AMSI reflection bypass in current session to evade AMSI detection while working). You can also recive the generated oneliner reverse shell connection via netcat. (in this case you will lose the C2 functionalities like screenshot, upload, download files, Keylogger, AdvInfo, PostExploit, etc)

meterpeter payloads/droppers can be executed using User or Administrator Privileges depending of the cenario (executing the Client as Administrator will unlock ALL Server Modules, amsi bypasses, etc.). Droppers mimic a fake KB Security Update while in background download\exec Client in '***$Env:TMP***' trusted location, with the intent of evading Windows Defender Exploit Guard. meterpeter payloads|droppers are FUD (please dont test samples on VirusTotal).

Under Linux users required to install **powershell** and **apache2** webserver, Under Windows its optional the install of **python3** http.server to deliver payloads under LAN networks. If this requirements are **NOT** met, then the

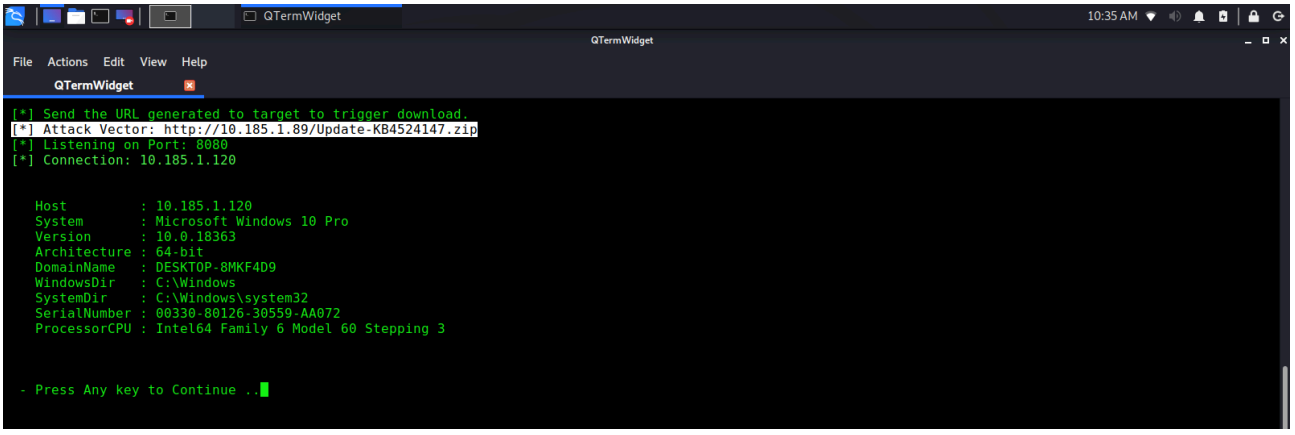
Client (***Update-KB4524147.ps1***) will be written in meterpeter working directory for manual deliver.



[Quick Jump List]

ATTACKER MACHINE: [Linux Kali]

```
Warning: powershell under linux distributions its only available for x64 bits archs ..
```



Install Powershell (Linux x64 bits)

```
apt-get update && apt-get install -y powershell
```

Install Apache2

```
apt-get install Apache2
```

Start Apache2 WebServer

```
service apache2 start
```

Start C2 Server (Local)

```
cd meterpeter
pwsh -File meterpeter.ps1
```

Deliver Dropper/Payload To Target Machine (apache2)

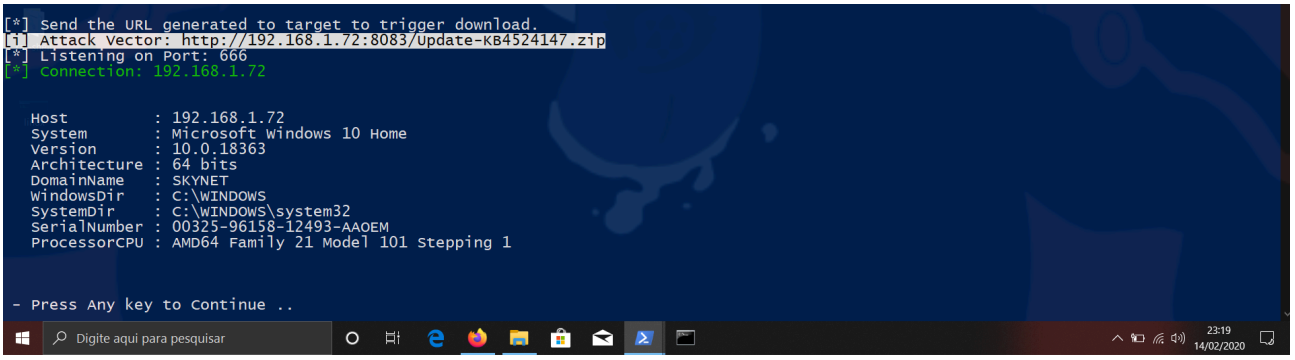
```
USE THE 'Attack Vector URL' TO DELIVER 'Update-KB4524147.zip' (dropper) TO TARGET ..
UNZIP (IN DESKTOP) AND EXECUTE 'Update-KB4524147.bat' (Run As Administrator)..
```

Remark:

```
IF dropper.bat its executed: Then the Client will use $env:tmp has its working directory ('recomended')..
IF Attacker decided to manualy execute Client: Then Client remote location (pwd) will be used has working dir
```

[Quick Jump List]

ATTACKER MACHINER: [Windows PC]



Install Python3 (optional)

Install Python3 (http.Server) to deliver payloads under LAN networks ..

```
https://www.python.org/downloads/release/python-381/
```

Check if python **http.server** its installed

```
 $Local_Host = ((ipconfig | findstr [0-9].\.)[0]).Split()[-1]
python -m http.server 8080 --bind $Local_Host
CTRL+C # Exit webserver console
```

Start C2 Server (Local)

```
 cd meterpeter
powershell Set-ExecutionPolicy Unrestricted -Scope CurrentUser
powershell -File meterpeter.ps1
```

Remark

- meterpeter.ps1 delivers Dropper/Payload using python3 http.server. IF attacker has python3 installed. **'If NOT then the payload (Client) its written in Server Local Working Directory to be Manualy Deliver'** ..
- Remmnenber to close the http.server terminal after the target have recived the two files (Dropper & Client) **'And we have recived the connection in our meterpeter Server { to prevent Server|Client connection errors }'**

Deliver Dropper/Payload To Target Machine (manual OR python3)

```
DELIVER 'Update-KB4524147' (.ps1=manual) OR (.zip=automated|silentExec) TO TARGET ..
```

Remark:

```
 IF dropper.bat its executed: Then the Client will use $env:tmp has its working directory ('recomended')..
IF Attacker decided to manualy execute Client: Then Client remote location (pwd) will be used has working dir
```

Quick Jump List

Video Tutorials:

Special Thanks:

@ZHacker13 (Original Rev Shell) | **@tedburke** (CommandCam.exe binary)
@codings9 (debugging modules) | @ShantyDamayanti (debugging Modules)
@AHLASaad (debugging Modules) | **@gtworek** (EnableAllParentPrivileges)

- **meterpeter WIKI pages (Oficial Documentation)**

- **Jump To Top of this readme File**

Source: https://github.com/r00t-3xp10it/meterpeter