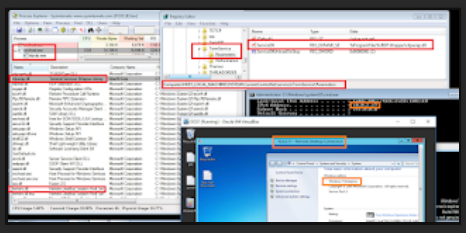
Thursday, 7 February 2019

RDPWrapp is a legit third party utility that enable multiple simultaneous RDP session on non Windows Servers, which is something an attacker will need if he needs to operate interactively while the victim is still active on his machine :

CarbonBlack:

regmod:HKLM\SYSTEM\CurrentControlSet\services\TermService\Parameters\ServiceDll or (process_name:svchost.exe and modload:rdpwrap.dll and modload:termsrv.dll)



Related:

It's also very important to watch for any unusual modification of the Terminal Server registry values fSingleSessionPerUser to allow multiple simultaneous Windows sessions using the same account, and fDenyTSConnections to allow Terminal Services connections.:

CarbonBlack:

- regmod: HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\fSingleSessionPerUser
- regmod: HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\fDenyTSConnections

References:

https://github.com/stascorp/rdpwrap

Posted by MENA SEC at 02:01

Labels: carbonblack, rdp hijack, rdpwrap, sysmon 13

Threat Hunting #5 - Detecting enumeration of users...

Threat Hunting #4 - Detecting Excel/Word documents...

Threat Hunting #3 - Detecting PsExec execution usi...

Threat Hunting #2 - Detecting PsLoggedOn exec usin...

Threat Hunting #1 - RDP Hijacking traces - Part 1

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)