



Applied Security Research

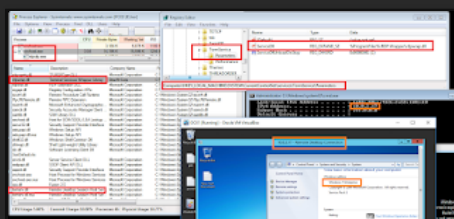
Home About us

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 MENASEC at 02:01

Labels: carbonblack, rdp hijack, rdpw rap, sysmon 13

Blog Archive

- 2020 (3)
- ▼ 2019 (39)
 - November (2)
 - July (1)
 - April (3)
 - March (7)
 - ▼ February (26)
 - Threat Hunting #24 - RDP over a Reverse SSH Tunnel
 - Threat Hunting #23 - Microsoft Windows DNS Server ...
 - IronPort: Password-Protected Archives
 - Threat Hunting #22 - Detecting user accounts setw...
 - Threat Hunting #21 - Hiding in plain sights with r...
 - IronPort: Blacklisted Attachments
 - Threat Hunting #20 - Detecting Process Doppelgänger...
 - Threat Hunting #19 - Procdump or Taskmgr - memory ...
 - Threat Hunting #18 - Run/RunOnce - Shell-Core EL...
 - Threat Hunting #17 - Suspicious System Time Change
 - Threat Hunting #16 - Lateral Movement via DCOM - S...
 - Threat Hunting #15 - Detecting Doc with Macro invo...
 - Threat Hunting #14 - RDP Hijacking via RDPWRAP | f...
 - Threat Hunting #13 - Detecting CACTUSTORCH using S...
 - Threat Hunting #12 - Suspicious strings in Regist...
 - Threat Hunting #11 - Exposed Passwords
 - Threat Hunting #10 - Renamed/Modified Windows (ab)...
 - Threat Hunting #9 - Impacket/Secretdump remote exec...
 - Threat Hunting #8 - Detecting traces of Boot Confi...

12 captures

20 Dec 2019 - 29 Mar 2023

Threat Hunting #14 - RDP Hijacking via RDPWRAP | fDenyTSConnections | fSingleSessionPerUser

29

201920202022

About this capture

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)

Simple theme. Powered by Blogger.