We're continuing to fight for universal access to quality information—and you can help as we continue to make improvements. Will you chip in?



https://blog.menasec.net/2019/02/threat-hunting-rdp-hijacking-via.html



Applied Security Research

Home About us

Thursday, 7 February 2019

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

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:

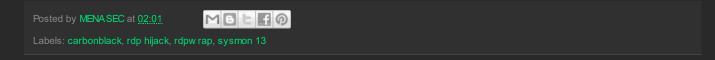
It's also very important to watch for any unusual modification of the Terminal Server registry values fSingleSessionPerUser to allow multiple simultaneous Windows sessions using the same account, and fDenyTSConnections to allow Terminal Services connections.:

CarbonBlack:

- $\bullet \quad \text{regmod: HKLM} \\ \textbf{SYSTEM} \\ \textbf{CurrentControlSet} \\ \textbf{Control} \\ \textbf{Terminal Server} \\ \textbf{fSingleSessionPerUser} \\ \textbf{Server} \\ \textbf{fSingleSessionPerUser} \\ \textbf{fSingleSessionPerUser}$
- regmod: HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\fDenyTSConnections

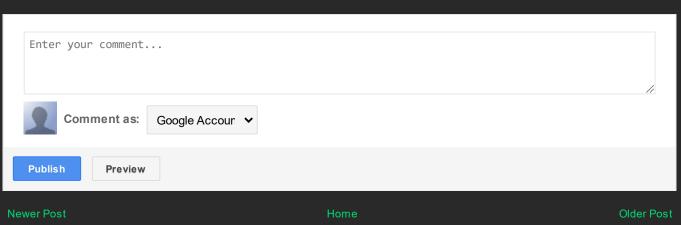
References:

https://github.com/stascorp/rdpwrap



No comments:

Post a comment



Subscribe to: Post Comments (Atom)

Blog Archive

Go

- **2020 (3)**
- ▼ 2019 (39)
 - ► November (2)
- **▶** July (1)
- ► April (3)
- ► March (7)
- ▼ February (26)

Threat Hunting #24 - RDP over a Reverse SSH Tunnel

Windows DNS Server ...

Archives

Threat Hunting #22 - Detecting user accounts set w...

plain sights with r...

IronPort: Blacklisted
Attachments

Threat Hunting #20 - Detecting
Process Doppelgängi...

Threat Hunting #19 Procdump or Taskmgr -

Threat Hunting #18 -Run/RunOnce - Shell-Core El...

Suspicious System Time Change

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

Threat Hunting #10 Renamed/Modified
Windows (ab)

Passwords

Threat Huting #9 - Impacket\Secretdump remote exec...

Fhreat Hunting #8 - Detecting traces of Boot Confi...

Threat Hunting #7 - Detecting BloodHound\Sharphoun

Threat Hunting #6 - Hiding ir plain sights with re...

Threat Hunting #5 - Detecting

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

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

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

Hijacking traces - Part 1

MENASEC - Applied Security Research: Threat Hunting #14 - RDP Hijacking via RDPWRAP | fDenyTSConnections | fSingleSessionPerUser - 02/11/2024 17:53 https://web.archive.org/web/20200929062532/https://blog.menasec.net/2019/02/threat-hunting-rdp-hijacking-via.html

