MENA SEC

Applied Security Research

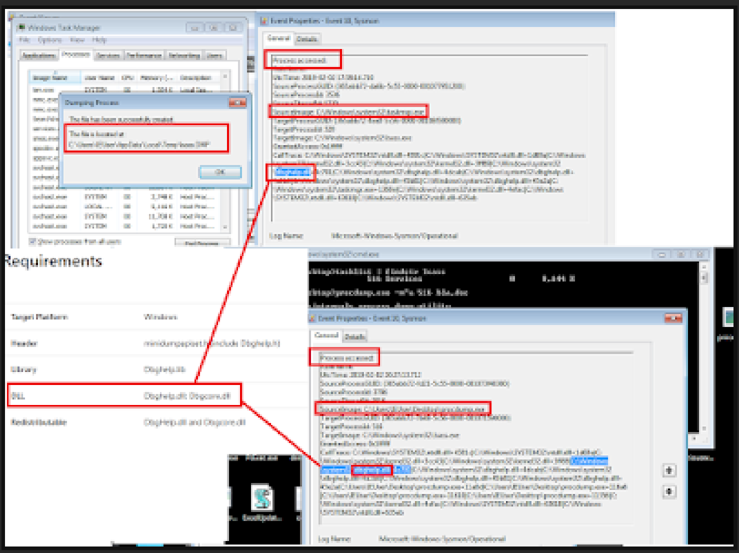
Home About us

Thursday, 7 February 2019

Threat Hunting #19 - Procdump or Taskmgr - memory dump

Dumping lsass.exe process memory using procmon.exe or taskmgr.exe (both are signed and trusted microsoft utilities) and then extracting secrets offline is a bit stealthier than running a rogue program.

Using Sysmon event 10 "Process A accessed Process B" and filtering by **CallTrace**, and **TargetImage** attribute data, we can detect both process memory dumping actions:



As can be seen above, both utilities call APIs exported by dbghelp.dll or dbgcore.dll to invoke memory dump write functions (i.e. MiniDumpWriteDump function).

Detection Logic:

Sysmon: EventID=10 and CallTrace contains "Dbghelp.dll" or "Dbgcore.dll" and TargetImage=="lsass.exe or any other sensitive process (i.e. Point of Sale related processes or alike)"

IBM Qradar AQL example:

select "SourceImage", "TargetImage" from events where eventid=10 and utf8(payload) imatches '(?i)((.*dbghelp.*)|(.*dbgcore.*))' and TargetImage imatches '.*lsass.*'

References:

https://docs.microsoft.com/en-us/sysinternals/downloads/procdump
https://docs.microsoft.com/en-us/windows/desktop/api/minidumpapiset/nf-minidumpapiset-minidumpwritedump

Posted by MENASEC at 02:35

Labels: dbgcore.dll, dbghelp.dll, lsass, memdump, procdump

No comments:

Post a Comment

Blog Archive

- ► 2022 (2)
- ► 2021 (3)
- ► 2020 (4)
- ▼ 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 set w...
    - Threat Hunting #21 - Hiding in plain sights with r...
    - IronPort: Blacklisted Attachments
    - Threat Hunting #20 - Detecting Process Doppelgängi...
    - 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 Huting #9 - Impacket\Secretdump remote exec...
    - Threat Hunting #8 - Detecting traces of Boot Confi...
    - Threat Hunting #7 - Detecting BloodHound\Sharphoun...
    - Threat Hunting #6 - Hiding in plain sights with re...
    - 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...

To leave a comment, click the button below to sign in with Google.

SIGN IN WITH GOOGLE

Threat Hunting #1 - RDP Hijacking traces - Part 1

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)