MENA SEC Applied Security Research

Home About us

Thursday, 7 February 2019

Threat Huting #9 - Impacket\Secretdump remote execution using EventId 5145

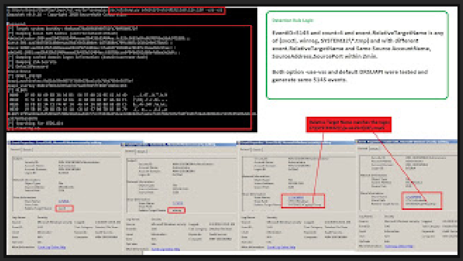
Secretdump.py performs various techniques to dump hashes from the remote machine without executing any agent there. If executed against a AD with domain admin privileges, all accounts hashes will be leaked.

For SAM and LSA Secrets (including cached creds) it reads from the registry and then save the hives in the target system (%SYSTEMROOT%\\Temp dir) and read the rest of the data from there.

For NTDS.dit :
a. Get the domain users list and get its hashes and Kerberos keys using [MS-DRDS] DRSGetNCChanges() call, replicating just the attributes we need. [artifact: connect to srvsvc named pipe]
b. Extract NTDS.dit via vssadmin executed with the smbexec approach.

It's copied on the temp dir and parsed remotely. The script initiates the services required for its working if they are not available (e.g. Remote Registry, even if it is disabled). -> [artifact: connect to winreg named pipe]

Below a summarized view of the traces left at the destination host. We recommend to enable 5145 on you DC and member windows servers.



Detection Rule Logic:

EventID=5145 and count=4 and event.RelativeTargetName is any of {svcctl, winreg, SYSTEM32*.tmp} and with different event.RelativeTargetName and Same Source AccountName, SourceAddress,SourcePort within 2min.

Both option -use-vss and default DRSUAPI were tested and generate same 5145 events.

Detection Logic:

EventId=5145 and count=4 and event.RelativeTargetName is any of {svcctl, winreg, system32*.tmp) and with different RelativeTargetName and Same AccountName, SourceAddress, SourcePort within 2 min

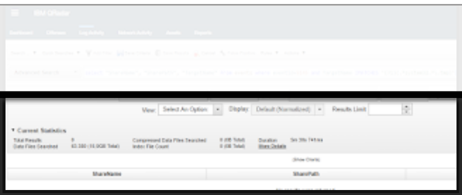
You can also hunt with the "system32*.tmp" (quite unique) as a search filter and then confirm manually if it's FP or not by reviewing "winreg" and svcctl" presence from source IP, User and Port.

IBM Qradar AQL hunting query:

select "ShareName", "SharePath", "TargetName" from events where eventid=5145 and TargetName IMATCHES '(?i)(.*system32.*\.tmp)'

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...



References:

https://github.com/SecureAuthCorp/impacket/blob/master/examples/secretsdump.py
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=5145

Posted by MENASEC at 01:15

Labels: 5145, secretdump

No comments:

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

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...
Threat Hunting #1 - RDP Hijacking traces - Part 1