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?

Go N







Applied Security Research

Home

11 captures 24 Apr 2020 - 29 Mar 2023

About us

https://blog.menasec.net/2019/02/threat-huting-10-impacketsecretdump.html

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.



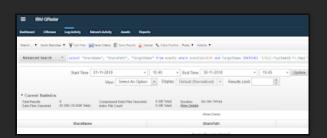
Detection Logic:

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)'



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 <u>01:15</u>



No comments:

Blog Archive

- **▶** 2022 (2)
- **▶** 2021 (3)
- **2020 (4)**
- **2019** (39)
 - ► November (2)
- ► July (1)
- ► April (3)
- ► March (7)

▼ February (26)

Threat Hunting #24 - RDP ove a Reverse SSH Tunnel

Threat Hunting #23 - Microsoft Windows DNS Server ...

Archives

user accounts set w...

Threat Hunting #21 - Hiding in plain sights with r...

IronPort: Blacklisted
Attachments

Threat Hunting #20 - Detecting Process Doppelgängi...

Procdump or Taskmgr memory ...

Run/RunOnce - Shell-Core

Change
Threat Hunting #16 - Lateral

Threat Hunting #15 Detection

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

Threat Hunting #11 - Exposed
Passwords

Threat Hunting #10 Renamed/Modified

Threat Huting #9 Impacket\Secretdump

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...

