Credential Stuffing

Valid Active Directory credentials have been discovered on open shares and files within your environment. These are used by the attackers.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics
Cyber Deception

TOOLS

PowerSploit:
- Invoke-ShareFinder
- Invoke-FileFinder
- Find-InterestingFile

ADExplorer.exe
MailSniper
Snaffler
CrackMapExec

https://github.com/Exploit-install/PowerSploit

https://www.blackhillsinfosec.com/domain-goodness-learned-love-ad-explorer

https://www.blackhillsinfosec.com/abusing-exchange-mailbox-permissions-mailsniper

Backdoors & Breaches™

PIVOT and ESCALATE

Created by: BLACK HILLS | Information Security