Detection Rule Pack

DETECTION RULE PACK

1. PowerShell Downloader

Condition: ProcessCommandLine contains IEX/DownloadString/-enc

2. LSASS Dump Attempt

Condition: procdump/lsass/MiniDump

3. Inbox Rule Creation Abuse

Operation=New-InboxRule and rule contains forward/delete

4. Kerberoasting

EventID 4769 with RC4 (0x17)

5. Password Spray

Failed login from single IP targeting many accounts