

CLEARTEXT PASSWORDS IN FILES

The attackers love people who share and save passwords in files everyone else can read. This attack works because people (often admins and developers) create documents and spreadsheets with passwords in them. Then, they put them on shares that are readable to everyone in the domain.

DETECTION

User and Entity Behavior Analytics
Cyber Deception
Endpoint Analysis

TOOLS

Snaffler
PowerShellEmpire



<https://github.com/SnaffCon/Snaffler>

<https://www.blackhillsinfosec.com/power-posing-powerops>



PIVOT and ESCALATE

Created by: **BLACK HILLS** | Information Security