Weaponizing Active Directory

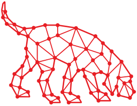
The attackers map domain trust relationships, group policies, user/group privileges, and object access control lists (ACLs) in your Active Directory.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics
Endpoint Security Protection Analysis
Cyber Deception

TOOLS

BloodHound
DeathStar
CrackMapExec



https://github.com/BloodHoundAD/BloodHound

https://github.com/byt3bl33d3r/DeathStar

https://github.com/byt3bl33d3r/CrackMapExec

https://www.blackhillsinfosec.com/webcast-weaponizing-active-directory

Backdoors & Breaches™

PIVOT and ESCALATE

Created by: BLACK HILLS | Information Security