APT39 and Cobalt Kitty (Ocean Lotus) techniques

In Exercise 4, you'll compare APT39 techniques to OceanLotus techniques in ATT&CK Navigator. (OceanLotus is the group identified as being behind the Cobalt Kitty campaign according to Cybereason.) If you need a detailed walkthrough, please see the other PDF document. If you're familiar with Navigator, you can use the below list of techniques from the two groups to create layers and identify techniques used by both groups.

APT39

1. Initial Access – Phishing: Spearphishing Attachment (T1566.001)
2. Initial Access – Phishing: Spearphishing Link (T1566.002)
3. Initial Access – Valid Accounts (T1078)
4. Execution – Command and Scripting Interpreter (T1059)
5. Execution – Malicious File: User Execution (T1204.002)
6. Execution – Malicious Link: User Execution (T1204.001)
7. Persistence – Scheduled Task/Job: Scheduled Task (T1053.005)
8. Persistence – Boot or Logon Autostart Execution: Shortcut Modification (T1547.009)
9. Persistence – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
10. Persistence – Server Software Component: Web Shell (T1505.003)
11. Defense Evasion – Obfuscated Files or Information: Software Packing (T1027.002)
12. Credential Access – OS Credential Dumping: LSASS Memory (T1003.001)
13. Discovery – Network Service Scanning (T1046)
14. Discovery – System Network Configuration Discovery (T1016)
15. Lateral Movement – Remote Services: Remote Desktop Protocol (T1021.001)
16. Lateral Movement – Remote Services: SSH (T1021/004)
17. Command and Control – Proxy: External Proxy (T1090.002)
18. Exfiltration – Archive Collected Data: Archive via Utility (T1560.001)

OceanLotus

1. Initial Access – Phishing: Spearphishing Attachment (T1566.001)
2. Initial Access – Phishing: Spearphishing Link (T1566.002)
3. Execution – Command and Scripting Interpreter: Visual Basic (T1059.005)
4. Execution/Defense Evasion – Signed Binary Proxy Execution: Mshta (T1218.005)
5. Execution – Command and Scripting Interpreter: PowerShell (T1059.001)
6. Execution – Signed Binary Proxy Execution: Regsvr32 (T1218.010)
7. Execution/Persistence – Scheduled Task/Job: Scheduled Task (T1053.005)
8. Execution/Defense Evasion – Command and Scripting Interpreter (T1064)
9. Execution – User Execution: Malicious Link (T1204.001)
10. Persistence – System Services: Service Execution (T1569.002)
11. Persistence – Create or Modify System Service: Windows Service (T1543.003)
12. Persistence – Office Application Startup (T1137)
13. Persistence – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)

14. Defense Evasion – Masquerading: Match Legitimate Name or Location (T1036.005)
15. Defense Evasion – Modify Registry (T1112)
16. Defense Evasion – NTFS File Attributes (T1096)
17. Defense Evasion – Obfuscated Files or Information (T1027)
18. Discovery – Network Service Scanning (T1046)
19. Command and Control – Ingress Tool Transfer (T1105)
20. Command and Control – Application Layer Protocol: Web Protocols (T1071.001)