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 – Spearphishing Attachment (T1193)
2. Initial Access – Spearphishing Link (T1192)
3. Initial Access – Valid Accounts (T1078)
4. Execution – Scripting (T1064)
5. Execution – User Execution (T1204)
6. Persistence – Scheduled Task (T1053)
7. Persistence – Shortcut Modification (T1023)
8. Persistence – Registry Run Keys / Startup Folder (T1060)
9. Persistence – Web Shell (T1100)
10. Defense Evasion – Software Packing (T1045)
11. Credential Access – Credential Dumping (T1003)
12. Discovery – Network Service Scanning (T1046)
13. Discovery – System Network Configuration Discovery (T1016)
14. Lateral Movement – Remote Desktop Protocol (T1076)
15. Lateral Movement – Remote Services (T1021)
16. Command and Control – Connection Proxy (T1090)
17. Exfiltration – Data Compressed (T1002)

OceanLotus

1. Initial Access – Spearphishing Attachment (T1193)
2. Initial Access – Spearphishing Link (T1192)
3. Execution – Command-Line Interface (T1059)
4. Execution/Defense Evasion – Mshta (T1170)
5. Execution – PowerShell (T1086)
6. Execution – Regsvr32 (T1117)
7. Execution/Persistence – Scheduled Task (T1053)
8. Execution/Defense Evasion – Scripting (T1064)
9. Execution – User Execution (T1204)
10. Persistence – Modify Existing Service (T1031)
11. Persistence – New Service (T1050)
12. Persistence – Office Application Startup (T1137)
13. Persistence – Registry Run Keys / Startup Folder (T1060)
14. Defense Evasion – Masquerading (T1036)
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 – Commonly Used Port (T1043)
20. Command and Control – Remote File Copy (T1105)
21. Command and Control – Standard Application Layer Protocol (T1071)