Questions:

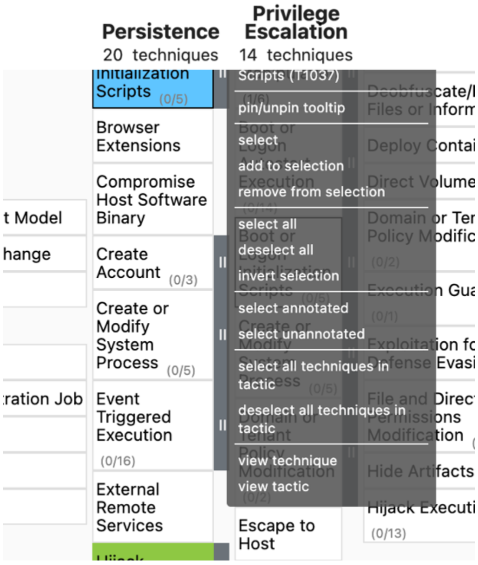
1. **What are the most common TTPs in three attack actors? If not, why?**
2. **What are the unique TTPs for each attack actors?**
3. **What procedures are utilised for the unique techniques in each case (listing 3 procedures with one procedure for each technique, in other words, 3 techniques for one attack actor)?**
4. **Following the above question (Q3), what might be the mitigation and detection methods? (List 2-3 techniques for each technique)**

Solutions:

1. There is no overlapped TTPs involved. Because different attack actors may have different characteristics, for instance, APT29 has gained access to a global administrator account in Azure AD and has used Service Principal credentials in Exchange (**T1078.004 Cloud Account**), while adversaries utilized two vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways to implant web shells, including GLASSTOKEN and GIFTEDVISITOR on internal and external-facing web servers (**T1203 Exploitation for Client Execution**).

2. **APT29:** *T1110 Brute Force etc.*
   Infamous Chisel: *T1569 System Services etc.*
   Ivanti: *T1059.001 Scripting Interpreter: PowerShell etc.*

3. You may find the detailed introduction of the techniques when you right-click the button on that technique and select the "view technique".



APT29: *T1110 Brute Force etc.*

- ***Procedures:*** using Ncrack to reveal credentials; used the tool GET2 Penetrator to look for remote login and hard-coded credentials; using John the Ripper to crack the password of the system.

Infamous Chisel: *T1569 System Services etc.*

- ***Procedures:*** using svchost.exe to execute a malicious DLL; using Windows services as a way to execute its malicious payload; using PsExec to perform remote service manipulation to execute a copy of itself as part of lateral movement

Ivanti: *T1059.001 Scripting Interpreter: PowerShell etc.*

- ***Procedures:*** executing PowerShell commands to delete system volume shadow copies; using PowerShell on victim systems to download and run payloads after exploitation; using PowerShell to execute malicious code.

4. **APT29:** *T1110 Brute Force*

- ***Mitigations:*** Account Use Policies; Multi-factor Authentication; Password Policies.
- ***Detections:*** Application Log; Executed Command Monitor; User Account Authentication.

Infamous Chisel: *T1569 System Services*

- ***Mitigations:*** Antivirus/Antimalware; Disable or Remove Feature or Program; Privileged Account Management
- ***Detection:*** File Modification Monitor; Process Creation Monitor; Service Creation Monitor

Ivanti: *T1059.001 Scripting Interpreter: PowerShell*

- ***Mitigations:*** Privileged Account Management; Restrict File and Directory Permissions; User Account Management
- ***Detection:*** Script Execution Monitor; Process Creation Monitor; Module Load Monitor.

Questions:

5. **What are the most common TTPs in ransomware attacks?**
6. **What are the unique TTPs for each ransomware attack case?**
7. **What procedures are utilised for the unique techniques in each case (listing 3 procedures with one procedure for each technique, in other words, 3 techniques for one attack actor)?**
8. **Following the above question (Q3), what might be the mitigation and detection methods? (List 2-3 techniques for each technique)**

5. The common TTPs involved in three cases are:
T1133 External Remote Services, *T1078 Valid Accounts* for **Initial Access**
and *T1486 Data Encrypted* for Impact under the **Impact** tactic.

6. **Lockbit:** *T1189 Drive-by Compromise (Under Initial Access)*
Play: *T1570 Lateral Tool Transfer (Under Lateral Movement)*
BianLian: *T1098 Account Manipulation (Under Persistence)*

In different ransomware threat cases, the adversary may exploit different strategies based on their prior knowledge. For instance, in the Lockbit ransomware case, LockBit affiliates gain access to a system through a user visiting a website over the normal course of browsing, which is unique to this case.

7. **Lockbit:** *T1189 Drive-by Compromise (Under Initial Access)*
   - ***Procedures:*** using watering hole attacks, often with zero-day exploits, to gain initial access to victims within a specific IP range; leverating a watering hole to serve up malicious code; compromising targets via strategic web compromise (SWC) utilizing a custom exploit kit.

Play: *T1570 Lateral Tool Transfer (Under Lateral Movement)*
   - ***Procedures:*** using uses remote shares to move and remotely execute payloads during lateral movement; copying tools between compromised hosts using SMB; copying files to other machines on a compromised network.

BianLian: *T1098 Account Manipulation (Under Persistence)*
   - ***Procedures:*** adding permissions and remote logins to all users.; granting privileges to domain accounts; adding a user named DefaultAccount to the Administrators and Remote Desktop Users groups.

8. **Lockbit:** *T1189 Drive-by Compromise (Under Initial Access)*
   - ***Mitigations:*** Application Isolation and Sandboxing; Restrict Web-Based Content; Update Software
   - ***Detection:*** Application Log; Network Traffic; File Creation Monitor

Play: *T1570 Lateral Tool Transfer (Under Lateral Movement)*
   - ***Mitigations:*** Filter Network Traffic; Network Intrusion Prevention
   - ***Detection:*** Command Execution Monitor; Network Traffic Flow Monitor; Process Creation Monitor;

BianLian: *T1098 Account Manipulation (Under Persistence)*
   - ***Mitigations:*** Multi-factor Authentication; Network Segmentation; User Account Management
   - ***Detection:*** File Modification Monitor; File Modification Monitor; User Account Modification Monitor

Questions:

9. **Comparing it with the previous two combined layers, what techniques are also listed in the layer we just created for the summary?**
10. **What procedures are utilised to implement these techniques, if possible, list with procedure examples?**
11. **Following the above question, what might be the mitigation and detection methods? (List 2-3 defence techniques for each)**

9. For instance, ***T1068 Exploitation for Privilege Escalation*** (Under Privilege Escalation tactic). The ACSC has identified the use of the *RottenPotato* exploit to gain SYSTEM level privileges on vulnerable systems. The exploit works by tricking the *NT AUTHORITY\SYSTEM* account into authenticating via *NTLM* to a compromised TCP endpoint. A man-in-the-middle attack is performed on the authentication process, allowing an actor to impersonate the SYSTEM security token.[1]

10. ***T1068 Exploitation for Privilege Escalation***

    - ***Procedures:*** deploying a malicious kernel driver through exploitation of CVE-2015-2291 in the Intel Ethernet diagnostics driver for Windows (iqvw64.sys); leveraing leveraging a vulnerability in Windows containers to perform an Escape to Host; exploiting vulnerabilities in the VBoxDrv.sys driver to obtain kernel mode privileges.

11. ***T1068 Exploitation for Privilege Escalation***

    - ***Mitigations:*** Application Isolation and Sandboxing; Threat Intelligence Program; Exploit Protection
    - ***Detection:*** Driver Load Detection; Process Creation Monitor.

[1] https://www.cyber.gov.au/about-us/advisories/summary-tactics-techniques-and-procedures-used-target-australian-networks