Summary:

Key Takeaways:

1. An unknown threat actor, named Sandman, has been detected primarily targeting telecommunication providers in the Middle East, Western Europe, and the South Asian subcontinent.
2. Sandman utilizes a novel modular backdoor named LuaDream, based on the LuaJIT platform. The staging chain is designed to evade detection and thwart analysis.
3. Strategic lateral movements and minimal engagements are characterizing Sandman's activities, likely to minimize the risk of detection.
4. Sandman's operation possibly has espionage motivations, with this being suggested by the TTPs, victimology and the deployed malware's characteristics.
5. Evidence points towards Sandman being likely a private contractor or mercenary group, given the high-end development of their malware and their poor segmentation practices.

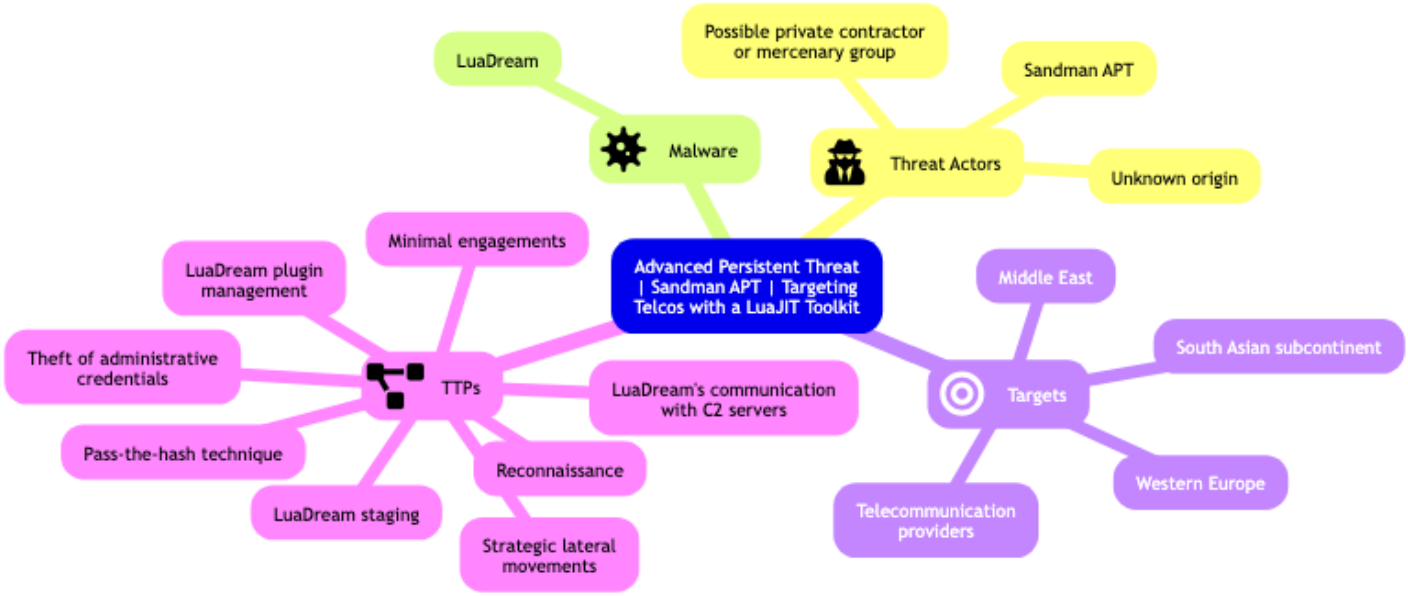
Summary and Analysis:

The Sandman APT is a new threat actor that mainly targets telecommunication providers in the Middle East, Western Europe, and the South Asian subcontinent. This group employs an advanced threat technique characterized by strategic lateral movements and minimal engagements - this is likely done in an attempt to minimize their activity's potential of detection. They use a new modular backdoor called LuaDream, utilizing the LuaJIT platform, designed to

execute its malicious activities directly into memory, thus further hiding its operations. The malware is still in active development and is capable of managing attacker-provided plugins and exfiltrating system and user information.

The actor's tools and techniques suggest espionage motivations, and their focus on the telecommunications sector aligns with their focus on obtaining sensitive data. There is some evidence that points to the possibility of Sandman being a private contractor or mercenary group due to inconsistent quality in their operations, showing a high level of sophistication in malware development but poor segmentation practices. LuaDream does not appear to be associated with any known threat actors. Though, it is noteworthy that LuaJIT usage in APT malware is relatively rare.

MITRE ATT&CK TTPs:
- Persistence - TA0003 - T1055 - Process Injection
- Credential Access - TA0006 - T1003 - OS Credential Dumping
- Command and Control - TA0011 - T1027 - Obfuscated Files or Information
- Defense Evasion - TA0005 - T1055 - Process Injection
- Reconnaissance - TA0043 - T1595 - Active Scanning
- Lateral Movement - TA0040 - T1560 - Archive Collected Data
- Exfiltration - TA0010 - T1560 - Archive Collected Data


Advanced Persistent Threat | Sandman APT | Targeting Telcos with a LuaJIT Toolkit
Malware
LuaDream
Threat Actors
Possible private contractor or mercenary group
Sandman APT
Unknown origin
TTPs
Minimal engagements
LuaDream plugin management
Theft of administrative credentials
Pass-the-hash technique
LuaDream staging
Reconnaissance
Strategic lateral movements
LuaDream's communication with C2 servers
Targets
Middle East
South Asian subcontinent
Western Europe
Telecommunication providers