# Sandman APT | A Mystery Group Targeting Telcos with a LuaJIT Toolkit

Original report published on: September 21, 2023[1]

## Executive Summary

In collaboration with QGroup GmbH, SentinelLabs researcher Aleksandar Milenkoski[1] observed a new threat activity cluster by an unknown threat actor dubbed as Sandman. Sandman primarily targets telecommunication providers in the regions of Middle East, Western Europe, and South Asian subcontinent.

It was observed that Sandman employs stealthy tactics to avoid detection and has introduced a unique malware called LuaDream, by utilising the LuaJIT platform.

LuaDream primarily manages attacker-provided plugins and exfiltrates system and user information, paving a route for further targeted attacks. A total of 36 distinct LuaDream components were identified, indicating a large-scale and sophisticated project supporting multiple communication protocols for Command and Control (C2) operations.

Sandman attribution is unknown, as there is no known threat actor linked to LuaDream. Hypotheses from researchers indicate that Sandman is likely espionage-focused and may be linked to a private contractor or mercenary group.

## Background

A novel advanced persistent threat (APT) actor, dubbed Sandman, relies on strategic lateral movement to targeted workstations and employs minimal engagement to avoid detection.

Sandman utilises a novel modular backdoor, named LuaDream, written in the Lua Programming language and deployed through the LuaJIT platform. LuaJIT is a relatively uncommon platform and the use of LuaJIT as an attack vector, along with the deployment of LuaDream, point to the substantial sophistication and technical prowess of the threat actor.

The LuaDream staging chain is purposefully crafted to avoid detection and hinder analysis, seamlessly injecting the malware into memory.

The discovery of this malicious activity occurred in August 2023, thanks to the collaborative effort between SentinelLabs and QGroup GmbH. They named the threat actor and its corresponding malware after the internal designation of the backdoor, referring to it as the ‘DreamLand client’. This collaboration has shed light on a previously unidentified and highly sophisticated threat actor, highlighting the need for vigilance and proactive cybersecurity measures in the ever-evolving landscape of cyber threats.

## Detection and Mitigation Techniques

- Enhance network security awareness and capabilities and ensure transparency and accountability. Firewall and intrusion detection system/intrusion prevention system (IDS/IPS) are highly recommended to enforce security policies and access controls for your network.

- Ensure that endpoint detection response and/or antivirus are installed and updated on all devices connected to a network.
- Use network segmentation and virtual private network (VPN) to isolate and secure your network traffic.
- Use encryption and authentication methods to protect your data.

## Indicators of Compromise[1]

| SHA1 | File name |
|---|---|
| 1cd0a3dd6354a3d4a29226f5580f8a51ec3837d4 | fax.dat |
| 27894955aaf082a606337ebe29d263263be52154 | fax.Application |
| 5302c39764922f17e4bc14f589fa45408f8a5089 | ualapi.dll |
| 77e00e3067f23df10196412f231e80cec41c5253 | fax.cache |
| b9ea189e2420a29978e4dc73d8d2fd801f6a0db2 | UpdateCheck.dll |
| fb1c6a23e8e0693194a365619b388b09155c2183 | updater.ver |
| ff2802cdbc40d2ef3585357b7e6947d42b875884 | fax.module |

| LuaDream Folder File paths |
|---|
| %ProgramData%\FaxConfig |
| %ProgramData%\FaxLib |

| C2 Server Domains |
|---|
| mode.encagil[.]com |
| ssl.explorecell[.]com |

## MITRE ATT&CK Tactics and Techniques

| Tactic | Technique ID | Technique Name | Details |
|---|---|---|---|
| Phishing | T1566.001 | Spear phishing Attachment | Adversaries may send spear-phishing emails with a malicious attachment in an attempt to gain access to victim systems |
| Command & Scripting Interpreter | T1059.001 | Powershell | Adversaries may abuse PowerShell commands and scripts for execution. |
| Indicator Remover | T1070.004 | File Deletion | Adversaries may delete files left behind by the actions of their intrusion activity. |
| Hijack Execution Flow | T1574.002 | DLL Side Loading | Adversaries may execute their own malicious payload by side-loading DLLs. |
| Process Injection | T1055.012 | Process Hollowing | Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defences. |

| | | | |
|---|---|---|---|
| Defence Evasion | T1027 | Obfuscated Files or Information | Adversaries may attempt to make an executable or file difficult to discover or analyse by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. |
| Valid Accounts | T1078.002 | Domain Accounts | Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defence Evasion. |
| Alternate Authentication Material | T1550.002 | Pass the Hash | Adversaries may “pass the hash” using stolen password hashes to move laterally within an environment, bypassing normal system access controls. |

## References


1. **^** “New ‘Sandman’ APT Group Hitting Telcos With Rare LuaJIT Malware” .