Indicators of Compromise

actors who operate with impunity. LuaDream stands as a compelling illustration of the continuous innovation and deployments at geographically dispersed victim environments communicating with the same C2 server.

resolves to deploying LuaDream. Some functionalities of this component include:

- The core components implement LuaDream features, such as initialization, gathering system and user information, C2 communication, and system persistence. These functionalities are essential for LuaDream to function as an implant. LuaDream is a multi-component and multi-protocol backdoor, whose main features are managing attacker-provided components and exfiltrating system and user information. The implementation and architecture of LuaDream indicate that it was likely developed by a private contractor.

The backdoor can communicate over the TCP, HTTPS, WebSocket, and QUIC protocols. The LuaDream variant we obtained from the targeted environments consists of 34 components: 13 core and 21 support components. The variants we encountered included the version, assigned IP and MAC addresses, OS version, available memory, and the name, PID, and username associated with the process in whose context LuaDream runs.

The activities we observed are characterized by strategic lateral movement to specific targeted workstations and the characteristics of the deployed malware indicate that it is highly likely this activity has espionage motivations. The activity cluster we observed and examination of C2 netflow data indicate a pronounced focus on targeting the telecommunication sector. The activities have been conducted by a threat actor of unknown origin using a novel combination of fully-formed DLL PE images, code, and LuaJIT bytecode. While we cannot associate LuaDream to any known threat actor, we lean towards the possibility of a private contractor.

The DLL timestamps could have been manipulated by the threat actor, given the proximity to the August 2023 combination of fully-formed DLL PE images, code, and LuaJIT bytecode. SentinelLabs has observed a new threat activity cluster by an unknown threat actor we have dubbed Sandman. Sandman has been primarily targeting telecommunication providers in the Middle East, Western Europe, and the South Asian subcontinent. While the development style is historically associated with a specific type of advanced threat actor, the development paradigm is being embraced by a broader set of threat actors. The Western or Western-aligned. However, this development paradigm is being embraced by a broader set of threat actors.

SentinelLabs has observed a new threat activity cluster by an unknown threat actor we have dubbed Sandman. Sandman has been primarily targeting telecommunication providers in the Middle East, Western Europe, and the South Asian subcontinent. While the development style is historically associated with a specific type of advanced threat actor, the development paradigm is being embraced by a broader set of threat actors.

SentinelLabs has observed a new threat activity cluster by an unknown threat actor we have dubbed Sandman. Sandman has been primarily targeting telecommunication providers in the Middle East, Western Europe, and the South Asian subcontinent. While the development style is historically associated with a specific type of advanced threat actor, the development paradigm is being embraced by a broader set of threat actors.

The activities we observed took place over several weeks in August 2023. After stealing administrative credentials and conducting reconnaissance, Sandman infiltrated specifically targeted workstations using the pass-the-hash technique and the characteristics of the deployed malware indicate that it is highly likely this activity has espionage motivations.

LuaDream is a multi-component and multi-protocol backdoor, whose main features are managing attacker-provided plugins and exfiltrating system and user information. The implementation and architecture of LuaDream indicate that it was likely developed by a private contractor.