Se ha atribuido a un actor de amenazas previamente no identificado, conocido como «*Sandman*«, una serie de ataques cibernéticos dirigidos a proveedores de telecomunicaciones en Oriente Medio, Europa Occidental y el subcontinente asiático.

Es importante destacar que estas intrusiones hacen uso de un compilador de *«just in time»* (JIT) para el lenguaje de programación Lua, llamado LuaJIT, como medio para desplegar un nuevo implante denominado LuaDream.

> *«Las actividades que hemos observado se caracterizan por un movimiento estratégico hacia estaciones de trabajo específicas y una interacción mínima, lo que sugiere un enfoque deliberado destinado a alcanzar los objetivos establecidos al tiempo que se minimiza el riesgo de detección»,* comentó Aleksandar Milenkoski, investigador de seguridad de SentinelOne, en un análisis publicado en colaboración con QGroup.

> *«La implementación de LuaDream indica un proyecto bien ejecutado, en constante desarrollo y de considerable envergadura».*

Ni la campaña ni sus tácticas se han relacionado con ningún actor o grupo de amenazas conocido, aunque la evidencia disponible apunta a un adversario de ciberespionaje con preferencia por el sector de las telecomunicaciones en diferentes regiones geográficas. Los ataques se detectaron por primera vez durante varias semanas en agosto de 2023.

> *«La cadena de puesta en escena de LuaDream está diseñada para evitar la detección y dificultar el análisis al desplegar el malware directamente en la memoria. La implementación y el proceso de puesta en escena de LuaDream utilizan la plataforma LuaJIT, el compilador de «justo a tiempo» para el lenguaje de secuencias Lua. Esto se hace principalmente para complicar la detección del código*

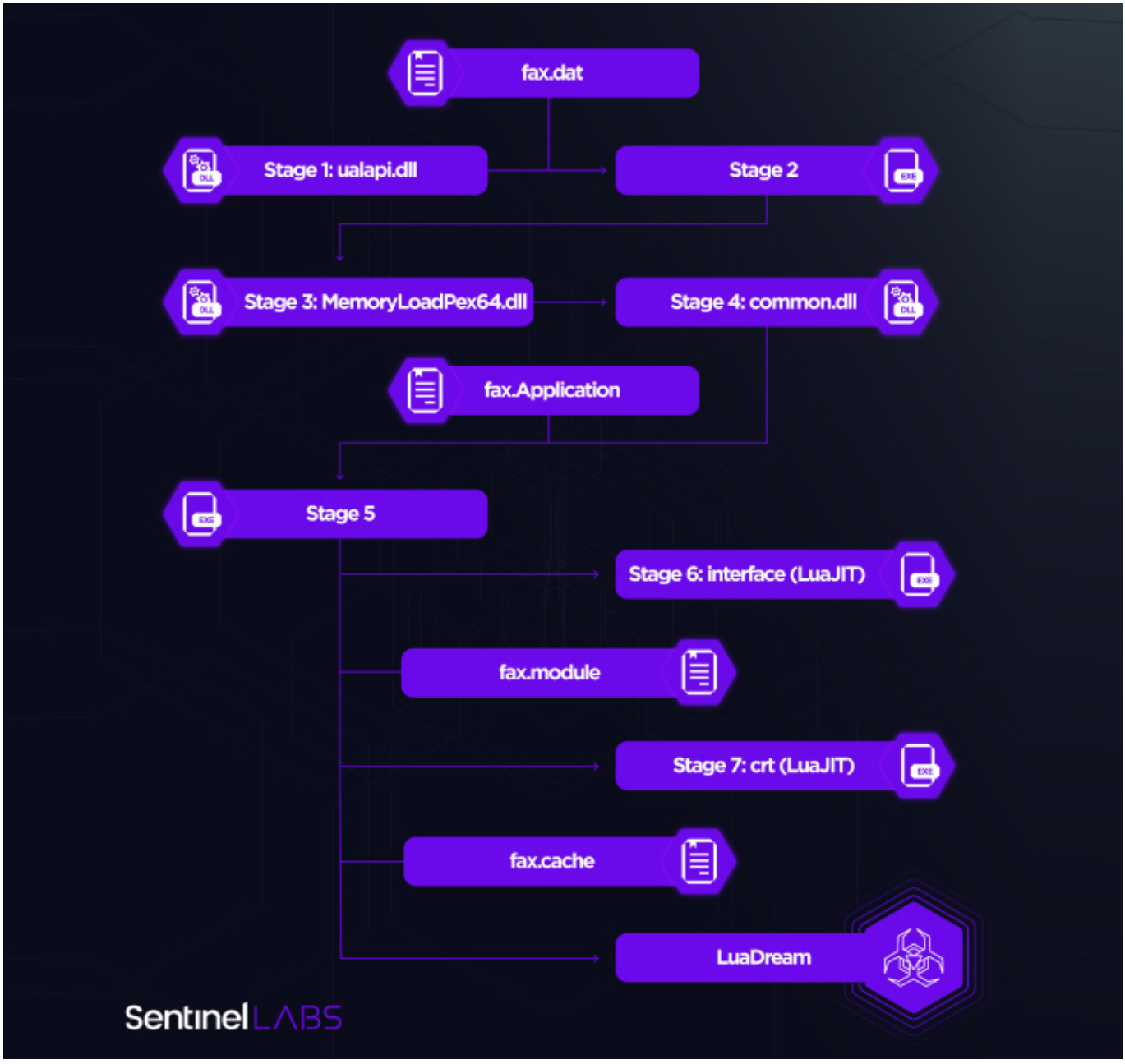
> *de secuencias Lua malicioso»,* explicó Milenkoski.

Los artefactos de cadenas de caracteres contenidos en el código fuente del implante hacen referencia al 3 de junio de 2022, lo que indica que el trabajo preparatorio ha estado en marcha durante más de un año.

Se sospecha que LuaDream es una variante de una nueva cepa de malware denominada *«DreamLand»* por Kaspersky en su informe de tendencias de APT para el primer trimestre de 2023, donde la empresa de ciberseguridad rusa describe su uso del *«lenguaje de secuencias Lua en conjunto con su compilador «justo a tiempo» para ejecutar código malicioso difícil de detectar».*

El uso de malware basado en Lua es poco común en el panorama de amenazas, habiéndose observado solo en tres ocasiones diferentes desde 2012: Flame, Animal Farm (también conocido como SNOWGLOBE) y Project Sauron.

El método exacto de acceso inicial sigue sin estar claro, pero se ha observado el robo de credenciales de administración y la realización de reconocimiento para comprometer estaciones de trabajo de interés y, en última instancia, entregar LuaDream.




LuaDream es una puerta trasera modular y multi-protocolo con 13 componentes principales y 21 de soporte, diseñada principalmente para extraer información del sistema y del usuario, así como para gestionar complementos proporcionados por el atacante que amplían sus capacidades, como la ejecución de comandos. También cuenta con diversas capacidades de

evasión de depuración para evitar la detección y dificultar el análisis.

La comunicación de control y comando (C2) se lleva a cabo estableciendo contacto con un dominio llamado *«mode.encagil[.]com»* utilizando el protocolo WebSocket. Pero también puede escuchar conexiones entrantes a través de los protocolos TCP, HTTPS y QUIC.

Los módulos centrales implementan todas las características mencionadas anteriormente, mientras que los componentes de soporte se encargan de ampliar las capacidades de la puerta trasera para esperar conexiones basadas en la API del servidor HTTP de Windows y ejecutar comandos.

> *«LuaDream es un ejemplo convincente de la continua innovación y los esfuerzos de avance que los actores de amenazas de ciberespionaje dedican a su arsenal de malware en constante evolución»,* comentó Milenkoski.

Esta divulgación coincide con un informe paralelo de SentinelOne que detalla intrusiones estratégicas sostenidas por actores de amenazas chinos en África, incluyendo ataques dirigidos a sectores de telecomunicaciones, finanzas y gobierno en África, como parte de grupos de actividad denominados BackdoorDiplomacy, Earth Estries y Operation Tainted Love.

El objetivo, según la compañía, es extender la influencia en todo el continente y aprovechar tales ofensivas como parte de su agenda de poder blando.

SentinelOne informó que detectó una compromiso de una entidad de telecomunicaciones con sede en el norte de África por el mismo actor de amenazas detrás de Operation Tainted Love, y señaló que el momento del ataque coincidía con las negociaciones privadas de la organización para una expansión regional adicional.

> *«Las intrusiones dirigidas por el APT BackdoorDiplomacy y el grupo de amenazas*

> *que orquesta Operation Tainted Love indican una intención dirigida a apoyar a China en sus esfuerzos para dar forma a políticas y narrativas alineadas con sus ambiciones geoestratégicas, estableciéndose como una fuerza pivotal y definitoria en la evolución digital de África»*, comentó el investigador de seguridad Tom Hegel.

Esto ocurre días después de que Cisco Talos revelara que los proveedores de servicios de telecomunicaciones en Oriente Medio son el objetivo de un nuevo conjunto de intrusiones llamado ShroudedSnooper que emplea un conjunto de puertas traseras sigilosas llamadas HTTPSnoop y PipeSnoop.