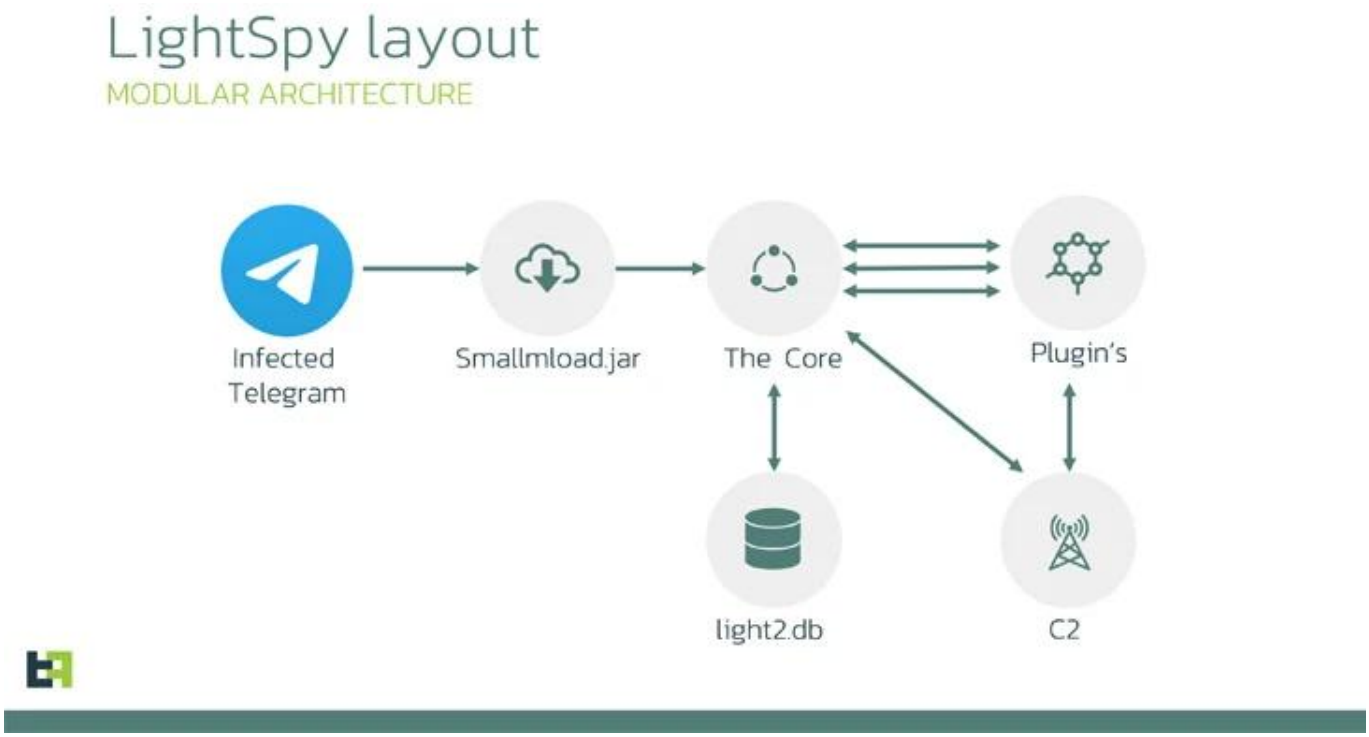
Nuevos hallazgos han revelado conexiones entre un programa espía para Android llamado DragonEgg y otra herramienta avanzada de vigilancia modular para iOS conocida como LightSpy.

DragonEgg, junto con WyrmSpy (también llamado AndroidControl), fue inicialmente expuesto por Lookout en julio de 2023 como una variante de software malicioso capaz de recopilar información delicada de dispositivos Android. Se atribuyó a APT41, un grupo estatal chino.

Por otro lado, detalles sobre LightSpy salieron a la luz en marzo de 2020 como parte de una campaña llamada Operación Noticias Envenenadas, en la cual se dirigieron ataques a usuarios de iPhone de Apple en Hong Kong a través de agujeros de seguridad para instalar el software de espionaje.

Ahora, según la empresa holandesa de seguridad móvil ThreatFabric, las cadenas de ataque involucran el uso de una aplicación de Telegram que ha sido alterada para descargar una segunda etapa de carga (smallmload.jar), la cual, a su vez, está configurada para descargar un tercer componente con el nombre en clave Core.

Un análisis más profundo de los elementos reveló que este implante ha estado siendo actualizado y mantenido activamente desde al menos el 11 de diciembre de 2018, con la versión más reciente lanzada el 13 de julio de 2023.



El módulo principal de LightSpy (es decir, DragonEgg) funciona como un complemento orquestador encargado de recolectar la identificación del dispositivo, establecer conexión con un servidor remoto, esperar instrucciones adicionales y actualizar tanto a sí mismo como a los complementos.

> *«LightSpy Core es extremadamente adaptable en términos de configuración: los operadores pueden controlar con precisión el programa de espionaje mediante una configuración que se puede actualizar»*, señaló ThreatFabric, destacando que WebSocket se utiliza para la entrega de comandos y HTTPS se emplea para la extracción de datos.

Entre los complementos más notables se incluye un módulo de localización que rastrea las ubicaciones precisas de las víctimas, una función de grabación de sonido capaz de capturar audio ambiental, así como conversaciones de audio de WeChat VOIP, y un módulo de registro

de facturación para recopilar el historial de pagos de WeChat Pay.

El centro de comando y control (C2) de LightSpy consiste en varios servidores ubicados en China continental, Hong Kong, Taiwán, Singapur y Rusia, y tanto el malware como WyrmSpy comparten la misma infraestructura.

ThreatFabric también informó que identificó un servidor que alojaba datos de 13 números de teléfono únicos pertenecientes a operadores de telefonía móvil chinos, lo que plantea la posibilidad de que estos números representen números de prueba de los desarrolladores de LightSpy o de las víctimas.

Las conexiones entre DragonEgg y LightSpy se basan en similitudes en patrones de configuración, estructura en tiempo de ejecución y complementos, así como en el formato de comunicación C2.

PLUGIN	VERSION	BRIEF DESCRIPTION
softlist	3.3.3	Exfiltrates the list of installed/running applications and active usernames using toolbox/toybox utility and superuser access
baseinfo	2.3.4	Exfiltrates contact list, call history, and SMS messages. C an send and delete SMS messages by the command
bill	1.2.18	Exfiltrates payment history from WeChat Pay
cameramodule	2.6.1	Takes camera shots. Can do one shot, continuous shot, or some event-related shot (for instance phone call)
chatfile	1.3.4	Exfiltrates data from different messengers' folders
filemanager	3.0.5	File exfiltration plugin
locationmodule	2.6.5	Precision location tracking plugin
locationBaidu	2.6.6	Another location-tracking plugin using different frame works and Android native APIs
qq	5.1.71	Tencent QQ messenger database parsing and exfiltratio n plugin
shell	2.2.4	Remote shell plugin
soundrecord	2.7.4	Sound recording plugin: environment, calls, VOIP calls audio exfiltration
telegram	7.3.221	Telegram messenger data exfiltration plugin
wechat	6.7.271	WeChat data exfiltration plugin
wifi	2.3.3	Wi-Fi network data exfiltration plugin

> *«La manera en que el grupo de actores de amenazas distribuyó la etapa inicial maliciosa dentro de una aplicación de mensajería ampliamente utilizada fue un truco ingenioso»,* destacó la empresa.

> *«Esto conllevó varios beneficios, ya que el implante heredó todos los permisos de acceso que tenía la aplicación portadora. En el caso de la aplicación de mensajería,*

> *se obtuvieron muchos permisos privados, incluido el acceso a la cámara y al almacenamiento».*