Una campaña de *watering-hole* fue descubierta recientemente y está dirigida a los usuarios de iPhone en Hong Kong mediante el uso de enlaces maliciosos a sitios web como un señuelo para instalar spyware en los dispositivos.

Según una investigación publicada por Trend Micro y Kaspersky, el ataque *«Operation Poisoned News»*, aprovecha una cadena remota de exploits de iOS para realizar un implante rico en funciones denominado *«LightSpy»*, por medio de enlaces a sitios web de noticias locales, que al hacer clic, ejecuta la carga de malware y permite que un intruso extraiga datos confidenciales del dispositivo afectado e incluso tome el control total.

Los ataques de tipo pozo de agua generalmente permiten que un atacante comprometa a un grupo específico de usuarios finales al infectar sitios web que se sabe que visitan, con la intención de obtener acceso al dispositivo de la víctima y cargarlo con malware.

El grupo APT, denominado TwoSail Junk por Kaspersky, se está aprovechando de las vulnerabilidades presentes en iOS 12.1 y 12.2 que abarcan todos los modelos desde el iPhone 6 al iPhone X, con los ataques identificados por primera vez el 10 de enero, antes de intensificarse alrededor del 18 de febrero.

La campaña utiliza enlaces falsos publicados en distintos foros, todos populares entre los residentes de Hong Kong, que aseguran conducir a varias noticias relacionadas con temas sobre sexo, clickbait o la actual pandemia de coronavirus COVID-19.

Al hacer clic en las URL, los usuarios acceden a los medios de comunicación legítimos que se han visto comprometidos, además de sitios web configurados específicamente para la campaña. En ambas situaciones, se utiliza un iframe oculto para cargar y ejecutar código malicioso.

> *«Las URL utilizadas condujeron a un sitio web malicioso creado por el atacante, que a su vez contenía tres iframes que apuntaban a sitios diferentes. El único iframe visible conduce a un sitio de noticias legítimo, lo que hace que las personas crean que están visitando dicho sitio. Un iframe se utilizó para el análisis del sitio web, el otro condujo a un sitio que albergaba el script principal de las vulnerabilidades de iOS»,* dijeron los investigadores de Trend Micro.

El malware en cuestión explota una vulnerabilidad de Safari *«parcheada en silencio»*, que cuando se procesa en el navegador conduce a la explotación de un uso luego de una falla de memoria libre (rastreada como CVE-2019-8605), que permite al hacker ejecutar código arbitrario con privilegios de root, luego instala la puerta trasera patentada LightSpy. Desde entonces, el error se resolvió con el lanzamiento de iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3 y watchOS 5.2.1.

El spyware no solo es capaz de ejecutar remotamente comandos de shell y tomar el control total del dispositivo. También contiene una variedad de módulos descargables que permiten la filtración de datos, como listas de contactos, ubicación GPS, historial de conexión WiFi, datos de hardware, llaveros iOS, registros de llamadas telefónicas, historial de Safari móvil y navegador Chrome y mensajes SMS.

Además, LightSpy apunta a aplicaciones de mensajería como Telegram, QQ y WeChat para robar información de cuentas, contactos, grupos, mensajes y archivos adjuntos.

Se sospecha que el grupo TwoSail Jung está conectado o posiblemente sean los mismos operadores de dmsSpy, una variante de Android del mismo malware que se distribuyó el año pasado por medio de canales abiertos de Telegram bajo la apariencia de aplicaciones de calendario de protesta de Hong Kong.

> *«Los servidores de descarga y comando y control de dmsSpy usaron el mismo nombre de dominio (hkrevolution[.]club) que uno de los abrevaderos utilizados por el componente de iOS de Poisoned News»*, dijeron los investigadores.

Una vez instaladas, estas aplicaciones de Android maliciosas cosecharon y extrajeron contactos, mensajes de texto, ubicación del usuario y nombres de archivos almacenados.

> *«Este marco e infraestructura en particular es un ejemplo interesante de un enfoque ágil para desarrollar y desplegar un marco de vigilancia en el sudeste asiático»,* agregaron los investigadores.

Trend Micro, por su parte, sugirió que el diseño y la funcionalidad de la campaña tienen como objetivo comprometer tantos dispositivos móviles como sea posible para permitir la backdoor y la vigilancia del dispositivo.

Para mitigar esas amenazas, es esencial que los usuarios mantengan sus dispositivos actualizados y eviten cargar aplicaciones en Android de fuentes no autorizadas.