Investigadores de seguridad cibernética advierten sobre una campaña en curso de malware para Android, que ha estado activa desde 2016 y se informó públicamente por primera vez en agosto de 2018.

ViceLeaker es el nombre que los investigadores de Kaspersky dieron a la campaña, misma que se encontró recientemente en los ciudadanos israelíes y algunos países del Medio Oriente con un poderoso malware de vigilancia diseñado para robar toda la información sensible.

Además de estas funcionalidades de espionaje tradicionales, el malware también tienen capacidades de puerta trasera que incluyen cargar, descargar y eliminar archivos, grabar audio circundante, cámaras de toma de control y hacer llamadas o enviar mensajes a números específicos.

El malware utilizado en estas campañas se denominó Triout, en un informe publicado por Bitdefender en 2018, que es una especie de marco de malware que los atacantes están utilizando para convertir aplicaciones legítimas en spyware al inyectarles una carga útil maliciosa.

En un nuevo informe publicado hoy, Kaspersky Lab reveló que los atacantes utilizan activamente la herramienta Baksmali para desensamblar y luego volver a ensamblar el código de una aplicación legítima, después de inyectar su código malicioso, una técnica conocida como inyección Smali.

> *«Sobre la base de nuestras estadísticas de detección, el principal vector de infección es la propagación de aplicaciones troyanas directamente a las víctimas por medio de los mensajeros de Telegram y WhatsApp»*, dijeron los investigadores.

Además de esto, los investigadores también encontraron que el código utilizado en el malware para analizar los comandos del servidor de comando y control se parece a las versiones modificadas de un cliente de código abierto XMPP / Jabber para la plataforma

Android, llamada *«Conversations».*

> *«Además, no vimos rastros de la inyección de Smali, pero encontramos rastros de compiladores dx/dexmerge, lo que significa que, esta vez los atacantes solo importaron la fuente original del código en un IDE de Android y lo compilaron con sus propias modificaciones»*, agregaron los investigadores.

Sin embargo, esas versiones modificadas de la aplicación Conversations, no contienen ningún código malicioso, pero parecen ser utilizadas por el mismo grupo de hackers para un propósito que no ha sido descubierto.

> *«Esto nos trajo la hipótesis de que esta podría ser la versión utilizada por el grupo detrás de ViceLeaker para la comunicación interna o para otros fines poco claros. Toda la detección de esta aplicación de puerta trasera se geolocalizó en Irán»,* dijeron los investigadores.

Según su informe, la campaña de ataque ViceLeaker aún está en curso, y los atacantes podrían distribuir versiones mal empaquetadas de aplicaciones legítimas por medio de tiendas de aplicaciones de terceros, mensajeros instantáneos o páginas web en línea controladas por piratas informáticos.

Debido a que estas apps se disfrazan de aplicaciones legítimas o populares, se recomienda a los usuarios de Android que siempre descarguen apps de fuentes confiables, como Google PlayStore.