Se encontró una nueva técnica de exfiltración de datos para aprovechar un canal ultrasónico encubierto para filtrar información confidencial de computadoras aisladas y con espacios de aire a un teléfono inteligente cercano que no requiere un micrófono para captar las ondas de sonido.

Nombrado GAIROSCOPE, el modelo contradictorio es la última incorporación a una larga lista de enfoques acústicos, electromagnéticos, ópticos y térmicos ideados por el Dr. Mordechai Guri, jefe de I+D en el Centro de Investigación de Seguridad Cibernética de la Universidad Ben Gurion del Negev en Israel.

> *«Nuestro malware genera tonos ultrasónicos en las frecuencias de resonancia del giroscopio MEMS. Estas frecuencias inaudibles producen pequeñas oscilaciones mecánicas dentro del giroscopio del teléfono inteligente, que pueden demodularse en información binaria»,* dijo el Dr. Guri en un nuevo artículo.

Air-gapping se considera una contramedida de seguridad esencial que implica aislar una computadora o red y evitar que establezca una conexión externa, creando efectivamente una barrera impenetrable entre un activo digital y los actores de amenazas que intentan forjar un camino para los ataques de espionaje.

Al igual que otros ataques contra redes con brechas de aire, GAIROSCOPE no es distinto en el sentido de que confía en la capacidad de un adversario para violar un entorno de destino por medio de estrategias como memorias USB infectadas, pozos de agua o compromisos de la cadena de suministro para entregar el malware.

La novedad ahora es que también requiere infectar los smartphones de los empleados que trabajan en la organización víctima con una aplicación no autorizada que, por su parte, se despliega mediante vectores de ataque como ingeniería social, anuncios maliciosos o sitios web comprometidos, entre otros.

En la siguiente fase de la cadena de destrucción, el atacante abusa del punto de apoyo

establecido para recopilar datos confidenciales (es decir, claves de cifrado, credenciales, etc.), codifica y transmite la información en forma de ondas de sonido acústicas sigilosas por medio del altavoz de la máquina.

Después, la transmisión es detectada por un teléfono inteligente infectado que está muy cerca físicamente y que escucha por medio del sensor del giroscopio integrado en el dispositivo, luego de lo cual los datos se demodulan, decodifican y transfieren al atacante a través de Internet mediante WiFi.

Esto es posible gracias a un fenómeno llamado corrupción ultrasónica que afecta a los giroscopios MEMS en frecuencias de resonancia. *«Cuando este sonido inaudible se reproduce cerca del giroscopio, crea una interrupción interna en la salida de la señal. Los errores en la salida se pueden usar para codificar y decodificar información»,* dijo el Dr. Guri.

Los resultados experimentales muestran que el canal encubierto se puede utilizar para transferir datos con tasas de bits de 1 a 8 bits/s a distancias de 0 a 600 cm, con el transmisor alcanzando una distancia de 800 cm en habitaciones estrechas.

Si los empleados colocan sus teléfonos móviles cerca de sus estaciones de trabajo en el escritorio, el método podría usarse para intercambiar datos, incluyendo textos breves, claves de cifrado, contraseñas o pulsaciones de teclas.

El método de exfiltración de datos se destaca por el hecho de que no requiere que la aplicación maliciosa en el teléfono inteligente receptor (en este caso, One Plus 7, Samsung Galaxy S9 y Samsung Galaxy S10) tenga acceso al micrófono, engañando así a los usuarios para que aprueben acceso al giroscopio.

El canal encubierto de los altavoces al giroscopio también es ventajoso desde el punto de vista del adversario. No solo existen señales visuales en Android e iOS cuando una aplicación usa el giroscopio (como en el caso de la ubicación o el micrófono), sino que también se puede acceder al sensor desde HTML a través de JavaScript estándar.

Esto también significa que el atacante no tiene que instalar una aplicación para lograr los objetivos previstos y, en su lugar, puede inyectar un código JavaScript de puerta trasera en un sitio web legítimo que muestra el giroscopio, recibe señales encubiertas y extrae la información por medio de Internet.

Mitigar GAIROSCOPE requiere que las organizaciones apliquen políticas de separación para mantener los teléfonos inteligentes a una distancia de al menos 800 cm o más de las áreas protegidas, retiren los altavoces y los controladores de audio de los puntos finales, filtren las señales ultrasónicas mediante los cortafuegos SilverDog y SoniControl, y bloqueen el canal encubierto agregando ruidos de fondo al espectro acústico.

El estudio llega poco más de un mes después de que el Dr. Guri demostrara SATAn, un mecanismo para saltar sobre espacios de aire y extraer información aprovechando los cables Serial Advanced Technology Attachment (SATA).