Un investigador de seguridad que tiene una larga línea de trabajo demostrando métodos novedosos de exfiltración de datos de sistemas con espacio de aire, ideó otra técnica que implica el envío de señales de código Morse por medio de LED en tarjetas de interfaz de red (NIC).

El enfoque, cuyo nombre en código es ETHERLED, proviene del Dr. Mordechai Guri, jefe del I+D en el Centro de Investigación de Seguridad Cibernética de la Universidad Ben Gurion del Negev, en Israel. Recientemente describió GAIROSCOPE, un método para transmitir datos ultrasónicamente a giroscopios de teléfonos inteligentes.

> *«El malware instalado en el dispositivo podría controlar mediante programación el LED de estado parpadeando o alternando sus colores, usando métodos documentados o comandos de firmware no documentados»,* dijo el Dr. Guri.

> *«La información se puede codificar a través de una codificación simple, como el código Morse, y modularse sobre estas señales ópticas. Un atacante puede interceptar y decodificar estas señales desde decenas a cientos de metros de distancia».*

Una tarjeta de interfaz de red, también conocida como controlador de interfaz de red o adaptador de red, es un componente de hardware de computadora que conecta una computadora a una red de computadoras. Los LED integrados en el conector de red notifican al usuario si la red está conectada y cuándo ocurre la actividad de datos.

ETHERLED, al igual que otros enfoques contradictorios contra los sistemas con brechas de aire, requiere que el intruso infrinja el entorno de destino y plante un código malicioso que

permita controlar los LED de la NIC.

Después viene la fase de recopilación y exfiltración de datos del ataque, durante la cual la información confidencial, como credenciales y datos biométricos, se codifica y envía por medio de un canal óptico encubierto utilizando los indicadores LED de estado de la tarjeta de red.

En la etapa final, las señales ópticas se reciben por medio de una cámara oculta que se coloca en un lugar con una línea de visión directa con la computadora transmisora comprometida. Alternativamente, la cámara también podría ser una cámara de vigilancia que sea vulnerable a la explotación remota o un teléfono inteligente que involucre a un infiltrado interno.

El ataque se puede usar para filtrar varios tipos de información, incluyendo contraseñas, claves de cifrado RSA, pulsaciones de teclas y contenido de texto, a cámaras ubicadas en cualquier lugar entre 10 y 50 metros, una distancia que se puede extender aún más a unos pocos cientos de metros usando un telescopio y lentes de enfoque especial.

Además, el método ETHERLED está diseñado para funcionar con cualquier periférico o hardware que se envíe con tarjetas Ethernet, como impresoras, cámaras de red, dispositivos de almacenamiento conectado a la red (NAS), sistemas integrados y otros dispositivos IoT.

Las contramedidas incluyen restringir cámaras y grabadoras de video en zonas sensibles, cubrir los LED de estado con cinta negra para bloquear físicamente la emanación óptica, reprogramar el software para anular el esquema de codificación y bloquear el entorno para agregar ruido aleatorio a las señales moduladas.