Los teléfonos inteligentes de gama baja que se venden a estadounidenses de bajos recursos por medio de un programa subsidiado por el gobierno, contienen malware que no se puede remover, según confirmó Malwarebytes en un informe.

El modelo de dispositivo afectado es el Unimax (UMX) U686CL, un smartphone de gama baja basado en Android, fabricado en China y vendido por Assurance Wireless, un proveedor de servicios de telefonía celular que forma parte del grupo Virgin Mobile.

La compañía de telecomunicaciones vende teléfonos celulares por parte de Lifeline, un programa gubernamental que subsidia el servicio telefónico para estadounidenses de bajos ingresos.

> *«A fines de 2019, vimos varias quejas en nuestro sistema de soporte de usuarios con un teléfono emitido por el gobierno que informaba que algunas de sus aplicaciones preinstaladas eran maliciosas»*, dijo Malwarebytes.

La compañía afirmó que adquirió un teléfono UMX U686CL y lo analizó para confirmar los informes que estaba recibiendo.

ADUPS Backdoor

Malwarebytes afirmó haber descubierto que uno de los componentes del teléfono, una aplicación llamada Wireless Update, contenía el malware Adups.

Adups fue descubierto en 2017 por Kryptowire, se trata de un componente de firmware malicioso creado por una compañía china con el mismo nombre.

El malware proporciona el componente como un sistema de actualización de firmware por aire (FOTA) a distintos fabricantes de teléfonos inteligentes y proveedores de firmware.

Dicho componente permite a los proveedores de firmware una forma de actualizar su código, pero en 2017, el equipo de Kryptowire descubrió que la compañía Adups también tenía la capacidad de enviar actualizaciones a smartphones de los usuarios, evitando a los vendedores de teléfonos y a los usuarios.

Malwarebytes afirma que este componente estaba actualmente en uso en dispositivos UMX y se está utilizando para instalar aplicaciones sin el conocimiento del usuario.

> *«Desde el momento en que inicia sesión en el dispositivo móvil, Wireless Update inicia la instalación automática de aplicaciones. Para repetir: no se ha obtenido el consentimiento del usuario para hacerlo, no hay botones para aceptar las instalaciones, solo instala las aplicaciones por sí mismo»,* dijo Malwarebytes.

> *«Si bien las aplicaciones que instala inicialmente están limpias y libres de malware, es importante tener en cuenta que estas aplicaciones se agregan al dispositivo con cero notificaciones o permisos requeridos por el usuario. Esto abre la posibilidad de que se instale malware sin saberlo en una actualización futura a cualquiera de las aplicaciones agregadas por Wireless Update en cualquier momento».*

Además, Malwarebytes informó que existe un segundo componente peligroso incluido en estos teléfonos. Los investigadores dijeron que encontraron código sospechosos en la aplicación de configuración del teléfono.

La aplicación estaba contaminada con lo que parecía ser una variedad de malware demasiado ofuscado, que se cree, es de origen chino, debido al uso intensivo de caracteres chinos como nombres de variables.

Según los investigadores, el malware fue codificado para funcionar como un gotero para una carga útil de malware de segunda etapa, una cepa de adware conocida como HiddenAds.

> *«Aunque todavía tenemos que reproducir la caída de malware adicional, nuestros usuarios han informado que, una variante de HiddenAds se instala de forma repentina en su dispositivo móvil UMX»*, dijo Malwarebytes.

Los investigadores dijeron que no podían confirmar que Unimax fue la parte que agregó el malware a los dispositivos. Podría tratarse de otro caso en el que terceros agregaron el malware por medio de la cadena de suministro del smartphone, mientras que los dispositivos viajan del fabricante al usuario final.

Esto hace que aunque el modelo del teléfono no sea malo, la presencia de ambas apps infectadas hacen que el teléfono sea inútil y peligroso para los usuarios.

Por si fuera poco, las aplicaciones afectadas no se pueden desinstalar. Los usuarios podrían deshabilitar la aplicación Wireless Update, pero eso provocaría que el teléfono pierda actualizaciones críticas de seguridad para los componentes de firmware.

Malwarebytes informó sobre lo sucedido a Assurance Wireless, pero no obtuvo noticias de la compañía. Por otro lado, ZDNet asegura haber obtenido comentarios:

> *«Estamos al tanto del problema y estamos en contacto con el fabricante del dispositivo Unimax, para comprender la causa raíz, sin embargo, después de nuestras pruebas iniciales, no creemos que las aplicaciones descritas en los medios sean malware».*