TELÉFONOS MÓVILES FALSIFICADOS / SUBESTÁNDAR

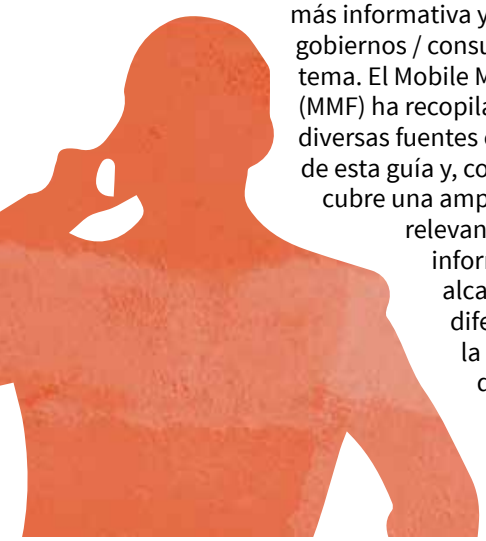
GUÍA DE RECURSOS PARA LOS GOBIERNOS

MMF
Mobile Manufacturers Forum

1 INTRODUCCIÓN

Hubo una proliferación en los últimos años de la fabricación, distribución y venta de los teléfonos móviles del mercado negro (comúnmente conocido como teléfonos falsificados y subestándares). Si bien este problema ha generado consecuencias adversas para la sociedad, los gobiernos todavía no comprenden plenamente el alcance y la naturaleza del problema. Los gobiernos siguen enfrentando importantes desafíos en la búsqueda de soluciones efectivas a este problema debido a las formas innovadoras y creativas utilizadas por las personas y entidades que se dedican a esta actividad ilícita para evadir las medidas de aplicación legales.

A pesar de la gravedad del problema, existen actualmente muy pocos recursos para los gobiernos para comprender el problema y para ayudarles en el desarrollo de soluciones adecuadas. Además, sigue habiendo una escasez de información integral para educar a los consumidores sobre los riesgos de la compra de teléfonos celulares del mercado negro. El objetivo de esta guía de recursos es la creación de la guía de recursos más informativa y completa para los gobiernos / consumidores sobre este tema. El Mobile Manufacturers Forum (MMF) ha recopilado información de diversas fuentes en la preparación de esta guía y, como tal, esta guía cubre una amplia gama de temas relevantes, tales como la información sobre el alcance del problema, los diferentes riesgos para la sociedad, y datos de benchmarking sobre las soluciones legislativas y técnicas.



2 ¿CUÁL ES LA DIFERENCIA ENTRE LOS TELÉFONOS MÓVILES FALSIFICADOS Y LOS SUBESTÁNDAR?

Aunque hay más similitudes que diferencias entre los teléfonos móviles falsificados y los subestándares, es importante que los gobiernos entiendan la diferencia. Teléfonos celulares falsificados y subestándares (conocidos colectivamente como " Shanzhai 'o' productos del mercado negro' 1) son los mismos en los siguientes aspectos significativos: los IMEI de ambas categorías de teléfonos móviles tienden a ser inválidos 2, ambos teléfonos móviles falsificados y subestándares evaden el pago de derechos de patente a los legítimos titulares de los derechos intelectuales, ambos usan chipsets y otros componentes usados o de calidad inferior, y, ambos no cumplen con los requisitos legales aplicables en los países con respecto a la venta y distribución de estos dispositivos. Hay, sin embargo, una diferencia importante entre estos dos subgrupos de teléfonos móviles del mercado negro que los gobiernos tienen que entender ya que señalan la necesidad de crear soluciones diseñadas para controlar la distribución de las dos categorías de dispositivos.

Un **teléfono móvil falsificado** es un producto, que infringe explícitamente la marca o el diseño de un producto original o auténtico. Un teléfono móvil falsificado copia las características (marca) de una marca original reconocida, copia la forma del producto original y / o copia el embalaje del producto original. En otras palabras, un teléfono móvil falsificado es una copia idéntica de la marca original o similar a la marca original (en términos de copia de la marca o del diseño) para todos los propósitos prácticos, puede ser considerado como una "copia" del producto « de marca» original. Esto incluye, por ejemplo, los productos que adoptan una etiqueta que consideran divertida y graciosa jugando con la marca establecida (por ejemplo, " Nokla 'o' SunSang ')

1 El término " Shanzhai " proviene de los caracteres chinos de " bandido " o fuera de la regulación gubernamental y este término se utiliza generalmente para referirse a productos electrónicos falsificados y de imitación y otros productos fabricados en China fuera de las regulaciones gubernamentales que se distribuyen ampliamente dentro y fuera de China. Los productos "Shanzhai" o " productos del mercado negro " se utilizan indistintamente en este documento. Los productos de mercado negro o Shanzhai no deben confundirse con los " productos del mercado gris", también conocido como el mercado paralelo, que es el comercio de un producto a través de canales de distribución que, aunque legales, no son oficiales, no autorizados o no queridos por el fabricante original.

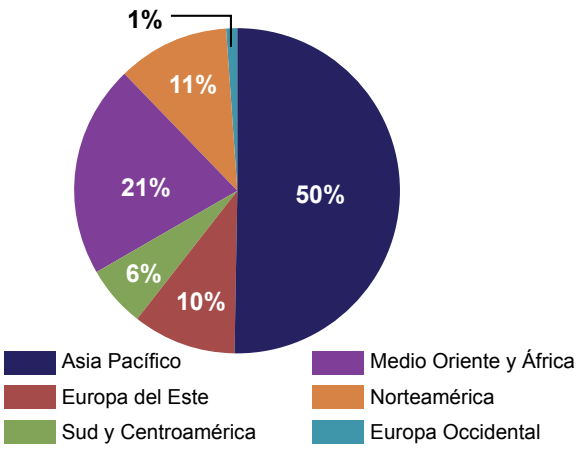
2 GSMA mantiene un sistema único conocido como la base de datos de IMEI (IMEI DB), una base de datos central y global que contiene información básica sobre el número de serie (IMEI) rangos de millones de dispositivos móviles (por ejemplo teléfonos móviles, tarjetas de datos de computadoras portátiles, etc.) que están en uso a través de las redes móviles del mundo. El IMEI es un número de 15 dígitos que se utiliza para identificar el dispositivo en las redes móviles. GSMA proporciona acceso al IMEI DB y sus datos a operadores de redes móviles miembros GSMA en todo el mundo, y para los actores calificados de la industria (es decir, los fabricantes de productos de gestión de dispositivos y las autoridades reguladoras). Los operadores de red utilizan la información del IMEI DB para determinar qué tipos de dispositivos están siendo utilizados por sus clientes en sus redes, y cuales características son compatibles con los dispositivos, para poder ofrecer los últimos servicios a sus clientes a través de sus redes

Un **teléfono móvil subestándares**, por su parte, es una categoría de teléfono móvil que puede parecerse a una marca original, pero es "suficientemente diferente" para que sea definitivamente difícil clasificar este producto como "falsificado" Un teléfono móvil de subestándares incluye, por ejemplo: productos " clones o genéricos " que pueden parecer similares en la forma de la marca auténtica, pero no llevar la marca explícita (es decir, no falsifican de manera explícita la marca legítima, ni aplican su propia marca), y , los productos de 'pequeñas marcas' que tienen una marca desconocida o poco conocida que intentan copiar otras marcas o formas de los productos originales.

Es importante que los gobiernos entiendan, sin embargo, que a excepción de la apariencia un teléfono móvil de subestándares es esencialmente igual a un teléfono móvil falsificado en todos los demás aspectos. Hay una tendencia por parte de los gobiernos de centrarse sólo en teléfonos móviles falsificados, cuando en realidad los teléfonos móviles subestándares presentan los mismos retos sociales.

3 CUANTIFICAR EL PROBLEMA DE LOS PRODUCTOS FALSIFICADOS / SUBESTÁNDARES DEL MERCADO NEGRO: LA PUNTA DEL ICEBERG

Como con cualquier tráfico de productos del mercado negro, es difícil medir el tamaño exacto del mercado negro en el sector de la telefonía móvil. Esto se debe a que muchos de los teléfonos móviles del mercado negro se venden físicamente en el ' mercado negro ' y por lo tanto es intrínsecamente difícil medir el tamaño del mercado de estos productos. Un estudio reciente realizado por ARCchart, sin embargo, proporciona un punto de partida para determinar el tamaño potencial de este problema. En concreto, el estudio concluyó que en 2011 el número de teléfonos falsificados / subestándares vendidos a nivel mundial era de 125 millones y se supone que esta Según ARCchart , Asia Pacífico es la región con mayor proliferación de estos teléfonos seguidos por el Medio Oriente y África , América del Norte, Europa del Este, América Latina y Europa Central y Occidental (véase el gráfico abajo).



Las cifras de ARCchart son, sin duda, conservadoras. Una de las limitaciones de dichas cifras es que sólo representan los productos que se venden en los canales de venta tradicionales y no reflejan los que se venden en los canales no regulados o no oficiales, así como los que se venden en el mercado negro. Dado que la mayoría de estos dispositivos son objeto de tráfico a través del mercado negro, es razonable y lógico suponer que los datos recogidos por ARCchart son sólo la punta del iceberg y que este problema es mucho más grande que lo que se refleja en las cifras ARCchart.

Hay otra prueba anecdótica que arroja luz sobre la magnitud del problema. Durante el año 2012 las cuotas de mercado de teléfonos móviles falsificados en Tanzania han fluctuado entre el 10% y el 20% del volumen total en el mercado. Esto no incluye los dispositivos subestándares, sólo las infracciones de marcas.

Además, Business Day en Johannesburgo (25 de marzo de 2013) informó que la Comisión de Comunicaciones de Kenia declaró que 3 millones de los 30,4 millones de teléfonos móviles en Kenia son falsificados. Según el artículo, la Agencia de Lucha contra la Falsificación desconectó 1 millón de teléfonos falsos y se apoderaron de otros teléfonos de un valor de 5 millones de chelines kenianos (~ 59 000 USD).

El ministro libio de Telecomunicaciones estimó recientemente que el 80 % de los dispositivos en el país fueron introducidos ilegalmente3 mientras que en los Emiratos Árabes Unidos, un operativo reciente resultó en la confiscación de más de 1.900 dispositivos falsos con un valor estimado de alrededor de 460 000 USD4.

La Federación de Cámaras de Comercio e Industria Indias (FICCI) publicó recientemente un informe que muestra que un poco más del 20 % del mercado de la telefonía móvil de la India son productos falsificados / subestandares, costando a la industria 1500 millones de dólares anuales en ventas perdidas, y al gobierno 85 millones de dólares en pérdidas fiscales directas y alrededor de 460 millones en pérdidas fiscales indirectas.

Mientras que en el Reino Unido, el informe anual 2011/12 del IP Crime Group (parte del Ministerio del Interior) reveló que 125.249 accesorios de teléfonos móviles falsos, 2,012 teléfonos móviles falsificados, y 1583 iPhones, iPads y reproductores de MP3 falso fueron embargados por la Fuerza de Fronteras del Reino Unido, y eso no incluye los miles de dispositivos y accesorios embargados por las normas de comercio del Reino Unido.

Otra importante fuente de datos es GFK, una de las empresas de investigación líderes en el mundo. Un estudio especial encargado en China llegó a la conclusión de que el tamaño del mercado negro en China en 2011 era de 33,16 millones de unidades, lo que representa un valor de ventas de 10280 millones de CNY (~ 1.9 mil millones de dólares). Este estudio

[3] http://www.lorientlejour.com/article/817178/sehnaoui-les-douanes-sont-une-passoire.html

[4] http://www.telecompaper.com/news/uae-cracks-down-on-counterfeit-mobile-phones--945597#.UaTVEL13Phg.twitter

también concluyó que el precio medio de venta de estos dispositivos (en China) en el Q4 de 2011 era de 284 CNY (~ 47 USD). La combinación de los datos de volumen (unidades vendidas) compilados por ARCchart con los datos de los precios medios de venta compilados por GFK ilustra que sólo la ' punta del iceberg ' representa un problema global que supera los **6 mil millones de dólares USD.**

A mayor escala, BASCAP (Acción Empresarial contra la Falsificación y Piratería de la Cámara de Comercio Internacional) cita un estudio que estima el valor de productos falsificados y pirateados en USD 1,77 billones para 2015.[5] Asimismo, BASCAP estima que la falsificación y la piratería costarán a los gobiernos del G20 y a los consumidores más de USD135 mil millones por año.[6]

4 ¿CUÁL ES EL IMPACTO NEGATIVO DE TELÉFONOS MÓVILES FALSIFICADOS Y SUBESTÁNDAR SOBRE LA SOCIEDAD?

Hay muchas maneras en las que el problema de teléfonos móviles falsificados/ subestándares se manifiesta negativamente en la sociedad. Como se explica más adelante, este problema afecta considerablemente a los consumidores, los gobiernos y la industria privada en una gran variedad de maneras[7].

A: ¿CUÁL ES EL IMPACTO EN LOS CONSUMIDORES?

1: SUSTANCIAS PELGROSAS EN LOS TELÉFONOS MÓVILES FALSIFICADOS / SUBESTÁNDARES

Un estudio reciente realizado por el Instituto Nokia de Tecnología de Brasil (INDT) sobre sustancias peligrosas ilustra los peligros potenciales de los teléfonos falsificados / subestándares. En concreto, el objetivo era evaluar si los teléfonos falsificados eran compatibles con RoHS, la Directiva de la UE sobre la restricción del uso de ciertas sustancias peligrosas en equipos eléctricos y electrónicos. Esta directiva restringe el uso de seis materiales peligrosos en varios tipos de equipos eléctricos y electrónicos.

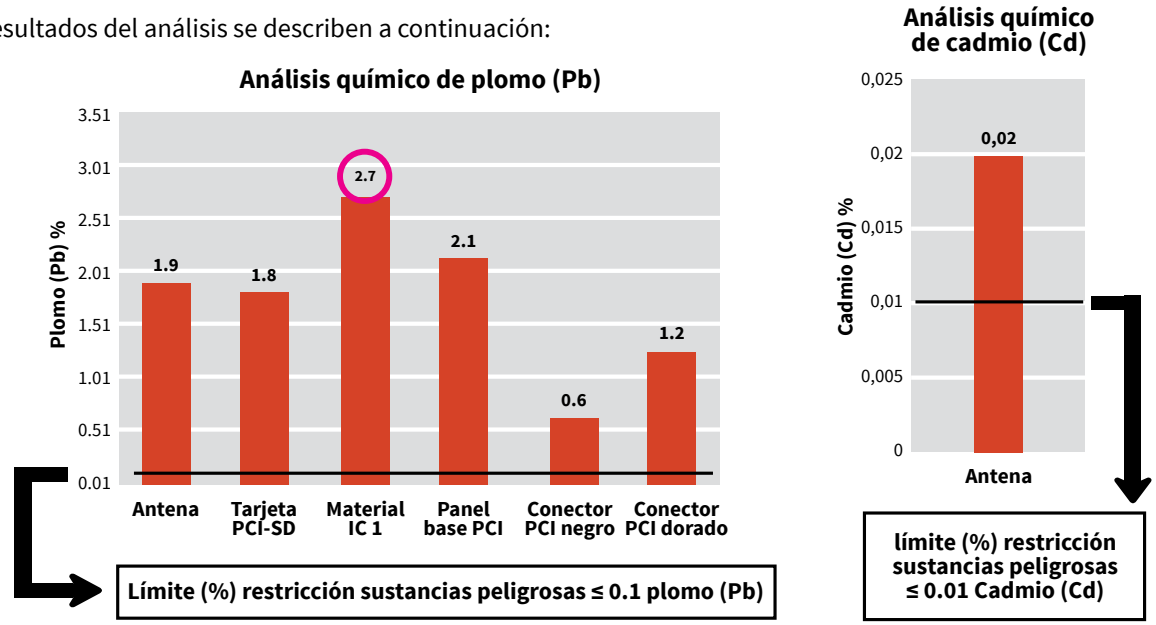
El estudio, utilizando el método de prueba estándar IEC 62321, conllevaba comprobaciones de cinco teléfonos falsificados con 158 piezas (las cubiertas, pantallas, circuitos integrados (IC), el teclado y otros componentes montados en superficie (SMD)). El estudio INDT reveló la presencia de dos sustancias peligrosas (plomo y cadmio) en los componentes internos y externos con concentraciones mucho más altas que los valores máximos permitidos por la RoHS. La **figura A** abajo ilustra el nivel excesivo de plomo y de cadmio encontrado en los componentes internos y externos de los teléfonos móviles probados.

Otros estudios realizados en otros países han confirmado la existencia de sustancias peligrosas en los teléfonos móviles falsificados/subestándares.

FIGURA A: Ensayo: Análisis de químicos peligrosos

El plomo con estaño (PbSn) se utilizó como consumible de procesos desde la década de 1940 para soldar componentes en tarjetas de circuito impreso. Si se encuentra plomo proveniente de las juntas de soldadura de los componentes, es muy probable que se haya utilizado el proceso de tecnología anterior para fabricar productos. Es una violación de la restricción de sustancias peligrosas, que prohíbe utilizar plomo en la fabricación de productos eléctricos y electrónicos.

Los resultados del análisis se describen a continuación:

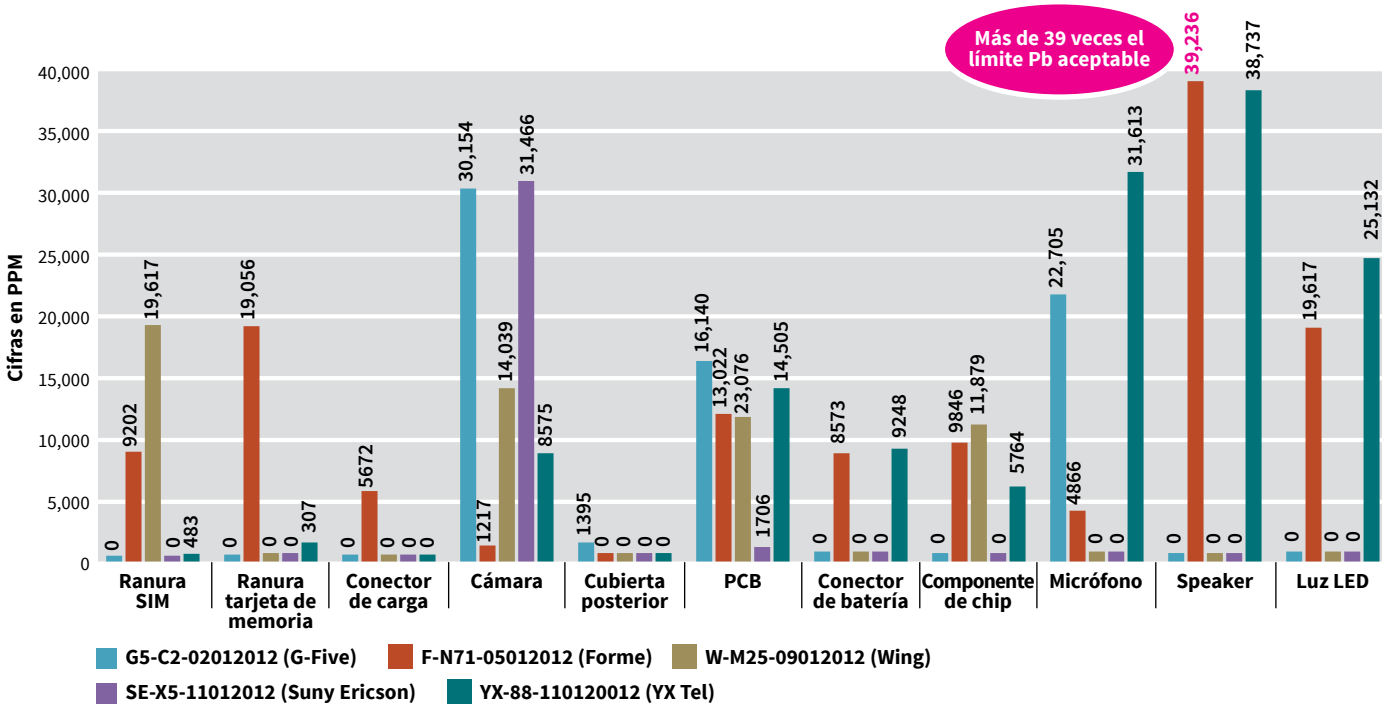


[5] http://iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/BASCAP-Research/Economic-impact/Global-Impacts-Study/

[6] http://iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/BASCAP-Research/Economic-impact/Impacts-on-Governments-and-Jobs/

[7] La Directiva RoHS de la UE fue elegida como el punto de referencia normativo en este estudio para determinar la existencia de sustancias peligrosas porque es la norma más conocida de las restricciones de sustancias en la industria electrónica a nivel mundial y la norma que todos los principales fabricantes de teléfonos móviles respetan. Se ha convertido en el estándar mundial de facto para teléfonos móviles.

FIGURA B: Alto contenido de plomo (Pb) encontrado en todos los terminales probados, lo cual claramente refleja su carácter substandard

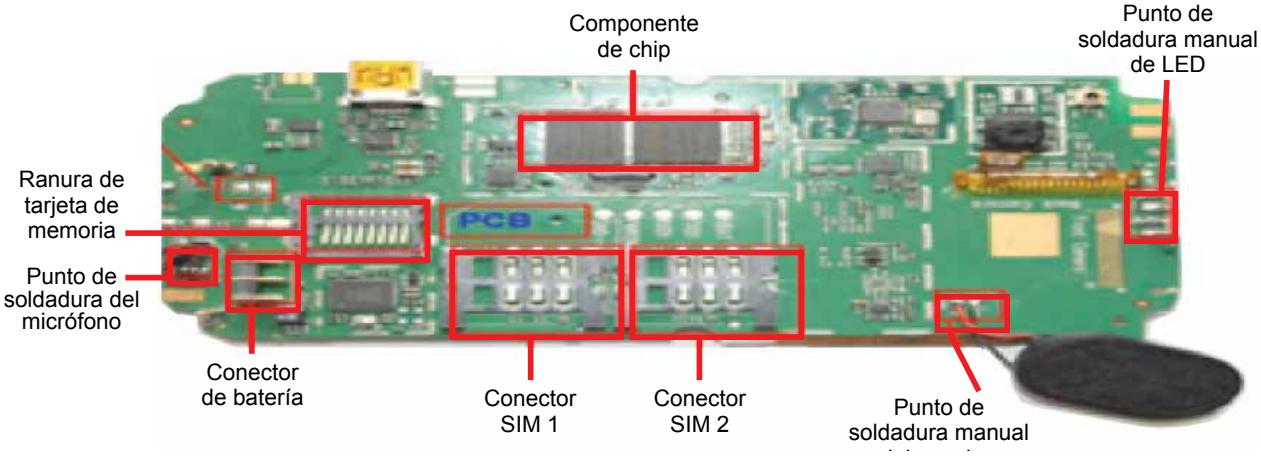


Se realizó un estudio en la India por el Centro de Materiales para la Tecnología Electrónica (C -MET), Hyderabad, para comprobar el cumplimiento de RoHS de los teléfonos móviles introducidos en el mercado indio. Para este estudio (que fue recomendado por el Ministerio de Medio Ambiente y Bosques (MOEF) y apoyado por la Asociación de Celulares de la india (ICA)), el C -MET Hyderabad seleccionó 15 modelos de teléfonos móviles ampliamente disponibles para la prueba. Los teléfonos fueron elegidos en función de su popularidad, demanda y disponibilidad en el mercado. Funcionarios de C- MET participaron personalmente en la adquisición de estos modelos (3 nos. para cada modelo) en las tiendas y teléfonos tanto de las marcas legales y sin marca / marcas chinas fueron recogidos para su análisis. Pruebas detalladas fueron realizadas por los procedimientos IEC 62321:2006 en más de 150 piezas (las cubiertas, pantallas, circuitos integrados (IC), el teclado y otros componentes en superficie (SMD)) que comprenden todos los teléfonos.

Se encontró alarmantes proporciones de sustancias peligrosas en todos los teléfonos móviles sin marca / marca china, especialmente plomo (Pb). En algunos casos, los valores fueron 35-40 veces mayores que los límites aceptables a nivel mundial para Pb. Muchos de los componentes críticos como la ranura para tarjetas de memoria, ranura SIM, cámara, etc…, que entran en contacto físico directo con los consumidores eran los peores en términos de contenido de materiales peligrosos, lo que obviamente aumenta el riesgo mucho más que si los componentes se encontraran dentro de los teléfonos. En contraste, se encontró que los teléfonos móviles de marcas globales y otras marcas reconocidas eran dentro de los límites aceptables de RoHS y por lo tanto seguro para el uso del consumidor. **La Figura B** arriba resume los resultados de este estudio.

La Figura C a continuación muestra visualmente las áreas donde se encontraron altas concentraciones de plomo:

FIGURA C: Partes del teléfono celular donde se encuentran sustancias peligrosas



2: OTROS ASPECTOS DE SEGURIDAD

La existencia de materiales peligrosos en los La existencia de materiales peligrosos en los teléfonos móviles falsificados/subestándares no es el único riesgo para la seguridad que puede potencialmente surgir de la utilización de estos productos. Los fabricantes legítimos deben someter sus productos a evaluaciones de cumplimiento y extensas pruebas antes de que puedan ser vendidos.

Esto puede incluir el cumplimiento de las normativas nacionales, así como los requisitos de seguridad de dispositivos de baja tensión, los requisitos de seguridad de audio, compatibilidad electromagnética, y RoHS (como se mencionó anteriormente), entre otros. Además, en la mayoría de los países, los teléfonos móviles deben ser del tipo aprobado (a veces referido como homologación o certificación de producto) por el regulador de las telecomunicaciones. La certificación del producto, entre otras cosas, asegura que el teléfono móvil lleva a cabo las funciones que pretende ser capaz de realizar, prueba la interoperabilidad y la interferencia, y confirma que es seguro para el uso del consumidor. En algunos países también se certifican los accesorios tales como cargadores y baterías. Es seguro decir que mientras los productos legítimos se someten a rigurosos procesos internos de aprobación y requerimientos legales antes de que puedan ser vendidos en el país, es probable que los teléfonos móviles falsificados/subestándares no cumplan con ninguno de estos requisitos.

3: CALIDAD DE SERVICIO

Dos estudios recientes confirman lo que siempre sospechó el MMF: los teléfonos móviles falsificados/ subestándares son de baja calidad, no funcionan bien, y, de hecho, causan interferencias con la red.

A : GSMA

Un estudio realizado para la Asociación GSM por Qualcomm, supervisó el rendimiento técnico de 18 smartphones falsificados junto con 3 smartphones auténticos utilizando protocolos estándares de la industria. Toda la prueba se realizó en un laboratorio acreditado, con todos los dispositivos con conexiones rápidas HSDPA. A diferencia de los dispositivos originales, ninguno de los dispositivos falsificados parecía haber sido probado por el gobierno o los laboratorios del sector privado para el cumplimiento de las normas legales o industriales.

Los resultados indican que 15 de los 18 dispositivos falsificados no cumplirían con los requisitos TIS de la industria (sensibilidad de recepción) con la mitad de los dispositivos 10 -15dB por debajo de los teléfonos de referencia. Del mismo modo, 16 de los 18 dispositivos falsificados no cumplirían con los requisitos de rendimiento de transmisión con 11 de estos dispositivos 6 - 13db por debajo de las necesidades. Ambos indicadores claves muestran un alto nivel de deterioración de rendimiento y se traduciría en un alto porcentaje de llamada fallidas para un usuario al utilizar el dispositivo.

Además, el estudio tomó los resultados de esta primera fase e investigó el impacto que estos dispositivos podrían tener sobre la red en términos de pérdida de la capacidad de voz y de datos, las velocidades de transmisión de datos y el impacto sobre la cobertura. Los resultados destacaron que tales dispositivos no sólo degradan la experiencia de los usuarios, sino que también crean una importante carga para los operadores de red. Por ejemplo, los resultados muestran que si se están utilizando dichos dispositivos en grandes cantidades, los operadores sufrirían una pérdida de 200 % en la capacidad de voz y de 50 % en la capacidad de datos, con la máxima velocidad de datos en las redes modeladas que caería a sólo 250 kilobits por segundo (kbps). Del mismo modo, debido a los malos resultados de los dispositivos, la cobertura se redujo significativamente creando efectivos agujeros en la red, lo que exige más del 80% de aumento de estaciones de base para corregir los problemas.

Estos resultados ponen en evidencia el considerable impacto tanto para los usuarios como para los operadores de redes que resultaría de la disponibilidad a grande escala y el uso generalizado de tales dispositivos.

B: INDT STUDY

El laboratorio INDT en Brasil también llevó a cabo un estudio similar sobre la experiencia del usuario. El estudio del INDT se hizo sobre 44 teléfonos falsificados / subestándares y realizó pruebas en los teléfonos originales, así como un " grupo de control"[8]. El objetivo de este estudio era evaluar el impacto en el rendimiento del servicio de telefonía móvil, debido a la existencia de los teléfonos falsificados y subestándares en la red del operador. Los procesos de prueba se basan en protocolos de prueba 3GPP[9] con el fin de comparar el rendimiento de los productos originales frente a los teléfonos falsificados / subestándares. En concreto, las siguientes categorías fueron probadas para el funcionamiento : 1) fallas de acceso 2) llamadas fallidas 3) capacidades de transmisión 4) capacidad de transmisión de energía 5) control de potencia de transmisión y 6) el acceso a Internet.

Consistente con el estudio de Qualcomm, el estudio INDT reveló problemas significativos con la experiencia del usuario. Se encontró que la calidad global de los circuitos en los teléfonos falsificados / subestándares era significativamente menor a los teléfonos originales y por lo tanto estos teléfonos experimentaron altos números de llamadas fallidas, fallas de acceso, así como problemas de transmisión. El estudio también concluyó que los teléfonos falsificados / subestándares no sólo degradan la calidad del servicio del usuario, sino también impactan negativamente a otros usuarios también. Las representaciones gráficas de los resultados se pueden ver en el Anexo A.

[8] Los teléfonos originales probados están homologados por ANATEL (Agencia Nacional de Telecomunicaciones de Brasil).

[9] Proyecto de Asociación de la 3 ª Generación (3GPP).

Los resultados de estos dos estudios son significativos y tienen consecuencias de amplio alcance para todos. Debido a la disminución del rendimiento de los teléfonos falsificados / subestándares, la experiencia de los consumidores se ve afectada negativamente (números de llamadas fallidas, fallos de acceso y problemas de transmisión excesivamente altos). Estos productos no sólo frustran la responsabilidad de los gobiernos para proteger a los consumidores y gestionar la calidad del servicio, sino también tienen implicaciones graves para los operadores de red dadas las medidas técnicas costosas e innecesarias que se necesitan con el fin de compensar los problemas causados por los teléfonos falsificados / subestándares (es decir las instalaciones de más antenas, estaciones bases y la necesidad de más espectro).

4: TELEFONOS FALSIFICADOS/ SUBESTANDARES SE VENDEN SIN GARANTIA

Los estudios Qualcomm y INDT confirman la mala calidad de los productos falsificados / subestándares. Sin embargo, este problema se ve agravado por el hecho de que estos productos, a diferencia de marcas conocidas (que ofrecen garantías de por lo menos un año), obviamente no ofrecen ninguna garantía al consumidor de sus productos. Por lo tanto, estos consumidores no tienen ningún recurso cuando los productos falsificados / subestándares dejan de funcionar.

5: CUESTIONES DE SEGURIDAD (CIBERSEGURIDAD, ROBO DE TELEFONOS, PROTECCIÓN DE DATOS, ETC.)

Es difícil imaginar cualquier otro dispositivo que contenga información más sensible que un teléfono móvil. La mayoría de la gente ha renunciado a sus libretas de direcciones de papel, ya que son demasiadas pesadas para llevarlas a todas partes y actualizar. Ahora que almacenan toda esa información en sus teléfonos móviles, junto con las notas rápidas para sí mismos, calendario de reuniones y eventos, correos electrónicos y mensajes instantáneos. Los consumidores utilizan sus teléfonos móviles mucho más que solo para llamar a personas. Los utilizan para tomar, almacenar y compartir fotos y videos, conectarse con amigos y familiares a través de redes sociales, para publicar opiniones en blogs, navegar por Internet, descargar y escuchar música y para realizar transacciones financieras. En Kenia, por ejemplo, más del 50 % de la población hace de todas sus transacciones financieras a través de banca móvil. Como resultado, los riesgos relacionados con la seguridad que se derivan de los teléfonos móviles tienen que ser tomadas en serio.

Los ciber-delincuentes como es de esperar están cometiendo cada vez más delitos cibernéticos a través de los dispositivos móviles. Numerosos tipos de malware ya están circulando continuamente en Internet buscando dispositivos móviles susceptibles. Los ciber-delincuentes utilizan el malware para infectar teléfonos móviles (troyanos maliciosos, virus, spyware, gusanos, etc) que están diseñados para buscar números de tarjetas de crédito, números de seguridad social, información de cuentas bancarias y otros tipos de información. No hay manera de que un consumidor pueda estar seguro de que el software de estos teléfonos móviles no esté escaneando continuamente la información que el consumidor entra en el teléfono para buscar información que permita cometer un delito cibernético o simplemente invadir la privacidad de una persona. Esta información se utiliza para robar el dinero de los consumidores o su identidad. Los hackers también son conocidos por disfrazar crímenes de seguridad cibernética en los juegos corruptos que permiten a los criminales apoderarse del teléfono y hacer llamadas y / o enviar mensajes SMS.

Los hackers también son conocidos para instalar igualmente malware que dirige el teléfono para enviar mensajes de texto a números de tarificación adicional que resulta en cargos importantes en la factura del teléfono. Otro tipo de malware que se ha descubierto tiene como objetivo secuestrar los dispositivos móviles y pedir rescate. Este malware, por ejemplo, podría eliminar todos los mensajes de texto de los teléfonos específicos y amenazan con paralizar el aparato a menos que los usuarios envían dinero. Otra malware tiene la capacidad de actuar como un registrador de información incluyendo el monitoreo remoto del teléfono, el registro de mensajes SMS entrantes y salientes, y la visualización del historial de llamadas, libreta de direcciones y otros datos.

Además de las amenazas a la seguridad cibernética, los teléfonos móviles falsificados/subestándares son dispositivos potencialmente atractivos para las personas que participan en la delincuencia organizada. Los teléfonos móviles falsificados/ subestándares no son rastreados con facilidad dado el hecho de que no tienen número de IMEI o un número de IMEI inválido.

El impacto que los teléfonos falsificados/ subestándares tienen sobre el creciente problema del robo de teléfonos celulares no se puede subestimar. Este es un gran problema de la sociedad en todos los países del mundo y no es raro que el robo de teléfonos móviles represente uno de los cinco principales delitos cometidos en un país determinado. El hecho de que los teléfonos falsificados/subestándares en la mayoría de los casos no tengan número IMEI o un número de IMEI inválido (y la relativa facilidad en la que el IMEI se puede cambiar en estos dispositivos) amenaza los esfuerzos de los países para controlar el robo de teléfonos móviles mediante la creación de listas negras y otras medidas similares.

La seguridad cibernética, la protección de los intereses de privacidad de los ciudadanos, y la lucha contra la delincuencia son una piedra angular de los más importantes debates de política pública en curso en la sociedad actual. Sin embargo, el impacto de los teléfonos móviles falsificados/subestándares en estos problemas sociales no está en la mira de la mayoría de los gobiernos. Muchos todavía no reconocen que

un teléfono móvil falsificado / subestándar presenta una amenaza mucho más importante que otros productos falsificados, ya que es tal vez el dispositivo de comunicaciones más importante de nuestra época. Más de mil millones de personas en el mundo utilizan los teléfonos móviles y si se considera la estimación más conservadora de ARCchart de 148 millones de dispositivos falsificados/subestándares vendidos a nivel mundial en 2013, se puede entender el peligro a la seguridad de que los teléfonos móviles falsificados/subestándares representan. Esta es una amenaza que debe ser tomada en serio.

B: ¿CUÁL ES EL IMPACTO DE LOS DISPOSITIVOS FALSIFICADOS/ SUBESTANDARES EN LOS GOBIERNOS?

El impacto del problema de teléfonos falsificados / subestándares en los gobiernos es igualmente convincente. La base de desarrollo de nuevos negocios en cualquier país es la existencia de una protección jurídica de los derechos de los negocios legítimos y la promoción de la competencia leal. Los gobiernos han adoptado muchos requerimientos que van desde la adopción de leyes de consumo que requieren garantías, normas que exigen la certificación de los teléfonos móviles, las leyes ambientales y las leyes que protegen la propiedad intelectual, las leyes relativas a la seguridad cibernética , y otros. Los teléfonos falsificados y subestándares frustran todos los esfuerzos del gobierno, ya que, por definición, operan fuera de la ley.

Sin embargo, quizás el impacto más significativo de estos productos en los gobiernos se relaciona con la pérdida de ingresos. Estos productos generalmente no pagan derechos e impuestos de venta cuando se importan y se venden y las empresas que participan en estas operaciones, obviamente, sería absurdo (por el riesgo de la captura) no pagan impuestos sobre las ganancias. Una vez más, usando estimaciones muy conservadoras, se trata de un problema de 6 mil millones de dólares en todo el mundo, lo que resulta en la pérdida de potencialmente miles de millones en ingresos por impuestos directos e indirectos cada año.

C: IMPACTO EN LA INDUSTRIA PRIVADA: PROBLEMA DE TELEFONOS FALSIFICADOS / SUBESTÁNDARES RESULTA EN PÉRDIDAS PARA TITULARES DE DERECHOS”

Fabricantes legítimos invierten miles de millones de dólares en investigación y desarrollo y otros millones más para garantizar que sus productos cumplen con la gran cantidad de requisitos legales impuestos por determinados países. La mayoría de los principales fabricantes emplean a decenas de miles de empleados en sus operaciones. Sin embargo, se encuentran en competencia directa con los teléfonos falsificados y subestándares y sufren pérdidas directas de ventas como resultado de estos productos del mercado negro ya que estos productos tienen una importante ventaja competitiva, dado que se pueden producir con bastante facilidad y a bajo costo.

La aparición hace unos años de los fabricantes de soluciones de chip integral en China ha alterado radicalmente el panorama de la competencia en este sentido, ya que reduce significativamente las barreras de entrada al mercado para las entidades del mercado negro. Las empresas que operan bajo un nuevo modelo de negocio han surgido por lo que en lugar de limitarse a ofrecer un conjunto de chips como los otros grandes proveedores de chipset, ofrecen a los clientes soluciones de software llave en mano (chipset, interfaces de hardware y otro software). Esto permite a los fabricantes del mercado negro crear y distribuir los teléfonos falsificados mucho más fácilmente que en el pasado.

La disponibilidad de soluciones llave en mano elimina esencialmente la etapa de investigación y desarrollo en el ciclo de desarrollo de los teléfonos móviles y los fabricantes del mercado negro pueden ahora simplemente conseguir los componentes, tales como pantallas y cubiertas y no hacer mucho más que montarlos. Esto ha permitido a las entidades del mercado negro proliferar. Sin el tamaño, el gasto en I + D, los costos regulatorios de los fabricantes legítimos (fabricantes de equipos originales), los fabricantes del mercado negro fueron capaces de introducir fácilmente estos productos en el mercado y beneficiarse ampliamente de ellos. Para agravar este problema, los fabricantes del mercado negro no pagan derechos de propiedad intelectual. En esta época y momento, no se puede producir un teléfono móvil sin tener que pagar regalías a los titulares de patentes esenciales. En resumen, debido a la aparición de soluciones llave en mano, los teléfonos móviles falsificados y subestándares se pueden producir muy baratos y compiten injustamente con los productos auténticos.

5 ¿QUÉ PUEDEN HACER LOS GOBIERNOS PARA CONTROLAR ESTE PROBLEMA?

Dado el crecimiento del problema de los teléfonos falsificados/subestándares en los últimos años, es evidente que los esfuerzos de aplicación por sí solos no son suficientes para controlarlo. Por tanto, es necesario explorar formas nuevas y creativas para atacar este problema. En esta parte, el MMF discute las posibles soluciones al problema (en orden de preferencia) y proporciona ejemplos de soluciones similares que se han adoptado.

A: SOLUCIONES DE BLOQUEOS DE RED

El MMF cree que la manera más eficaz para hacer frente a este problema de teléfonos falsificados/ subestándares es bloquear estos dispositivos en las redes. Una gran ventaja que los teléfonos celulares tienen sobre otros productos falsificados es que estos productos deben ser activados en la red para poder funcionar. Esta ventaja no se debe desperdiciar.

Soluciones de bloqueo de red son, probablemente, las mejores y más eficaces formas que tienen los gobiernos para controlar este problema. La pregunta es qué tipo de solución de bloqueo de la red es el más adecuado para un determinado país.

1: SOLUCIONES DE BLOQUEO TIPO "FINGERPRINTING DE LOS TELÉFONOS FALSIFICADOS/ SUBESTÁNDARES

Como se mencionó anteriormente, los teléfonos falsificados / subestándares tienen probablemente números de IMEI no válidos. Estos productos, tienen ya sea números no válidos (todos ceros, por ejemplo), o no tienen número de IMEI, o el número de IMEI es un número válido, pero clonado a partir de un teléfono original. En consecuencia, esto presenta retos para los gobiernos que buscan bloquear estos dispositivos simplemente utilizando el número de IMEI, porque la tecnología puede no ser capaz de distinguir qué teléfono móvil es el que tiene el número de IMEI válido. Por otra parte, tener un IMEI válido ni siquiera puede considerarse como suficiente para establecer la legitimidad del dispositivo debido a que la emisión de un IMEI válido por un fabricante para un modelo en particular no garantiza que el modelo no es falsificado o subestándar. GSMA por ejemplo, no comprueba la legitimidad del dispositivo antes de emitir un número IMEI. En efecto, no sería sorprendente encontrar muchos modelos de mercado negro que tienen un IMEI válidamente emitido. Además, una solución de bloqueo basada únicamente en IMEI es inherentemente poco fiable debido a que es bastante fácil cambiar el IMEI en los teléfonos falsificados / subestándares. Afortunadamente, nuevas tecnologías se han desarrollado para hacer frente a este problema.

Una solución tecnológica (referida como "fingerprinting" o "Plataforma Identificadora de falsificación ") puede identificar y bloquear los teléfonos falsificados / subestándares mediante el bloqueo del IMSI de la tarjeta SIM cuando se utiliza en un teléfono móvil falsificado mediante una comprobación cruzada de las capacidades del terminal con las esperadas. Las capacidades de los teléfonos utilizados por esta plataforma se refieren a la información ya estandarizada por 3GPP. Esta tecnología está diseñada para funcionar de la siguiente manera:

a. El sistema comprueba la base de datos de "capacidad" para determinar si las capacidades del teléfono coinciden con las capacidades listadas. La tecnología luego, compara las capacidades del teléfono con capacidades almacenadas en la base de datos de capacidad (la creación de base de datos se basa en la información proporcionada por el fabricante legítimo del dispositivo relativa al IMEI del teléfono y las capacidades). La base de datos de capacidad también puede, por ejemplo, utilizar otros datos para bloquear teléfonos como por ejemplo si el tipo de producto está homologado o no.
b. La plataforma envía una petición al HLR (base de datos de suscrición) para bloquear el IMSI del suscritor si la verificación cruzada de capacidad falla.
c. Hasta que el usuario cambie su teléfono móvil por uno con las capacidades correctas (en la base de datos de capacidad) el teléfono permanecerá bloqueado.

La tecnología no tiene por qué bloquear los teléfonos móviles en primera instancia. Como primer paso, el operador puede notificar los usuarios de los teléfonos ilegales y solicitar la regularización (por ejemplo, dar al usuario la oportunidad de insertar su SIM en un teléfono legal). Mientras que las otras soluciones que se mencionan a continuación pueden ser eficaces en el bloqueo de los teléfonos falsificados/ subestándares, esta tecnología de "fingerprinting" representa la "segunda generación" de soluciones y es el método preferido de MMF. Varios países están considerando este enfoque.

2: SOLUCIONES DE BLOQUEO DE RED IMEI

Una opción efectiva que no puede distinguir automáticamente IMEI válido de un IMEI invalido, pero que, sin embargo, puede ser una opción viable y eficaz para los gobiernos es la solución de bloqueo de IMEI. Muchos gobiernos de todo el mundo ya cuentan con una lista negra de dispositivos robados (lista negra IMEI que en muchos casos se basa en las denuncias por parte del usuario) que se utiliza para bloquear los dispositivos que han sido supuestamente robados. Un tipo de solución similar también puede ser usado para bloquear dispositivos falsificados / subestándares.

Un país puede lograr esto de dos maneras diferentes. Se puede exigir a los operadores de red que establezcan un sistema por el cual todos los teléfonos móviles activados en la red se cotejarán con la base de datos GSMA IMEI "lista blanca". Esto permitirá al operador determinar qué teléfonos o bien no tienen el número de IMEI o un número no válido o proceder a bloquear esos teléfonos. En el caso de duplicado de IMEI, medidas adicionales pueden ser tomadas por el operador para investigar cuál de los usuarios está utilizando un número válido. La base de datos GSMA está disponible sin costo alguno para los gobiernos con este fin de comprobación cruzada. La desventaja de este método es que no permite la verificación cruzada de otros incumplimientos como la homologación de los productos del teléfono y otros requisitos legales / regulatorios similares.

El segundo método de bloqueo de red IMEI empleado por algunos países es tal vez mejor representado por el proceso establecido en Ucrania y Turquía. Las soluciones usadas en ambos países establece una lista negra y una "lista blanca" para efectos de verificación cruzada [10]. La lista negra se centra en los dispositivos robados o perdidos y la lista blanca (que es creada localmente) se centra en los dispositivos que están autorizados para ser vendidos en el país (por ejemplo, homologados o de importación legal). Los dispositivos son verificados con las dos listas para determinar si el teléfono móvil está bloqueado o no. Esta solución tiene la posibilidad de controlar

[10] Costa Rica también exige a los importadores legítimos que registren el IMEI con el regulador quien alimenta una lista blanca de dispositivos que pueden ser activados en las redes. Un enfoque similar se utiliza en Uruguay.

más dispositivos que por el simple uso de una lista negra, pero se requiere el establecimiento del registro la lista blanca y, como tal, crea obstáculos pesados y no deseables para los visitantes temporales e importadores. Además, como ya se ha explicado el control exclusivamente de validez del IMEI puede no ser eficaz teniendo en cuenta la manera en que los IMEIs se distribuyen.

3: RED DE BLOQUEO BASADO EN LA HOMOLOGACIÓN

Otra posible medida para atacar el problema de teléfonos falsificados y subestándares es exigir el bloqueo de los dispositivos que no están homologados en la red. Dado que la mayoría de los dispositivos falsificados / subestándares no están homologados por el regulador, este tipo de aplicación de bloqueo de la red puede ser un medio eficaz para el control de este problema. En efecto, la implementación podría realizarse en conjunción con las soluciones de bloqueos de red anteriormente discutidas. Esta solución se requirió recientemente por el regulador en Brasil y la implementación debe ser completada para enero de 2014.

B: SOLUCIONES DE BLOQUEO DE IMPORTACIÓN

Soluciones de tipo IMEI y de bloqueo de red basado en la homologación mencionadas anteriormente también se pueden implementar en la frontera en caso de que el bloqueo de la red no es factible. En lugar de la verificación cruzada con la base de datos IMEI de GSMA (o base de datos de móviles homologados) y el bloqueo de la red de los teléfonos con IMEI no válido, un gobierno puede optar por bloquear estos dispositivos en el momento de la importación. Ambas soluciones filtrarán los teléfonos falsificados / subestándares importados a través de canales “legales” normales, pero, obviamente, la eficacia se ve obstaculizada por el hecho de que esto no va a bloquear los teléfonos que se importan de contrabando (al margen del proceso de aduanas)[11]

C: DESARROLLO DE UN PLAN INTEGRAL

Mientras que las estrategias mencionadas anteriormente están diseñadas para lanzar una amplia red con enfoques nuevos e innovadores, las medidas más tradicionales también deben ser un foco. Como se ha explicado anteriormente, el impacto social de los dispositivos falsificados / subestándares está mal entendido y por lo tanto se le otorga generalmente muy insuficientes recursos. El desarrollo de un plan integral es necesario para hacer frente a este problema complejo y este plan integral debe incluir, entre otras cosas, la conciencia de los consumidores, mayores medidas de aplicación y las reformas correspondientes a la legislación / normas.

1: AUMENTO DE SENSIBILIZACIÓN DE LOS CONSUMIDORES

La sensibilización por parte las autoridades gubernamentales sobre los peligros de los productos falsificados / subestándares es un componente crítico de cualquier estrategia. El lado de la demanda se debe abordar también y en este sentido, los consumidores deben ser conscientes de los graves problemas que plantean estos productos, como la seguridad y amenazas para la salud, el bajo rendimiento de los productos, la falta de cobertura de garantía e igualmente importante las amenazas de seguridad en particular en el ámbito de la seguridad cibernética y privacidad. Generalmente, los consumidores no son conscientes de estos problemas.

2: AUMENTO DE APLICACIÓN DE LAS NORMAS

El aumento de la aplicación de las normas es también esencial. Si bien los nuevos enfoques mencionados anteriormente pueden ser opciones eficaces para controlar este problema, no hay balas de plata. Una política integral debe incluir un aumento de recursos en forma de recopilación de inteligencia y operativos con un enfoque particular en los grandes mercados negros que existen en todas las ciudades importantes. Las autoridades gubernamentales no suelen ser capaces de colaborar eficazmente en todas las jurisdicciones de organización. Mientras el problema de teléfonos falsificados/ subestándares tiene impactos sobre una serie de autoridades de gobierno, el establecimiento de mecanismos de coordinación entre funciones con una fuerte representación de la industria es necesario. El MMF urge los reguladores y ministerios de las TIC establecer comités nacionales de lucha contra la falsificación para garantizar el desarrollo y seguimiento de planes de acción multi-funcionales y la asignación de los mecanismos de financiación adecuados y sostenibles.

3: REFORMAS LEGISLATIVAS / REGULATORIAS

La eficacia de la legislación / reglamentación existente también debe ser revisada. Muchos países no cuentan con una legislación adecuada para hacer frente a este problema. Muchos países, por ejemplo, no cuentan con una legislación que especifica como delito la distribución de teléfonos con IMEI no válidos, ni que sea ilegal cambiar el número IMEI. Otro ejemplo se refiere a los controles ambientales. Si bien muchos países tienen leyes relativas a los residuos del medio ambiente no hay controles establecidos para asegurar que los teléfonos falsificados / subestándares cumplan con estas normas. Muchos teléfonos móviles falsificados / subestándares están fuera del alcance de las autoridades aduaneras, ya que se encuentren “en tránsito” a través de un país especifico. Esto crea un enorme vacío legal para las organizaciones criminales que distribuyen estos productos en todo el mundo como los funcionarios de aduanas no tienen poder para confiscar productos falsificados que están siendo enviados a país tercero.

[11] For example imports of counterfeit/substandard phones over the courier services which is an increasingly used mechanism for importation of these phones.

CONCLUSIÓN

Los teléfonos móviles falsificados y subestándares representan un enorme problema social, dada la naturaleza de los teléfonos móviles y su importancia en la sociedad actual. Este problema afecta muchos aspectos de la sociedad, incluyendo la salud, la seguridad, el medio ambiente, la calidad de servicio, la pérdida de ingresos fiscales, y la competencia desleal. Eso representa una industria de miles de millones para los fabricantes ilegales y que está causando miles de millones de dólares de pérdidas para los gobiernos, la economía y la industria. Una acción fuerte es necesaria por parte de los gobiernos para controlar este problema, ya que las herramientas tradicionales son cada vez menos eficaces. (Tecnológicas y legislativas) existen soluciones eficaces y países ya han comenzado a adoptarlas. La acción concertada entre la industria y el gobierno debe ocurrir a fin de adoptar la solución que mejor se adapte a un determinado país. El MMF puede ayudar a los gobiernos en la solución de este problema al proporcionar conocimientos especializados y otros recursos.

Este documento fue preparado por el Mobile Manufacturers Forum - una asociación internacional fabricantes de equipos de comunicación móvil o inalámbrica. Para obtener más información sobre este importante tema, por favor visite:

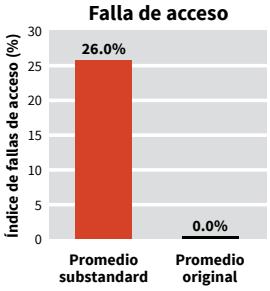
www.spotafakephone.com

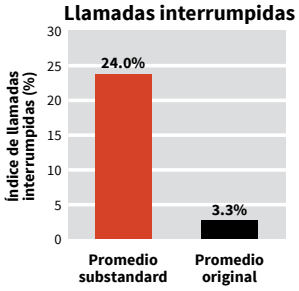
El proyecto Spot -a – Fake - Phone está diseñado para ayudar a los consumidores a conocer más acerca de los peligros asociados con los dispositivos falsificados y subestándares y para ayudar a identificar estos dispositivos antes de comprarlos.

ANEXO 1

PRUEBA DE CATEGORÍA # 1 Y # 2: Fallo de Acceso y Llamadas fallidas

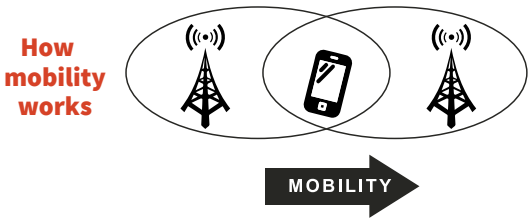
- Los operadores suelen evaluar la calidad del servicio monitoreando las fallas de acceso y llamadas fallidas.
- **Falla de acceso:** Esta categoría mide los intentos que fallan en la red.
- **Llamadas fallidas:** Esta categoría mide las llamadas en curso que son indeseablemente interrumpidas (fallidas) de la red.
- **Resultados:** En las dos categorías de pruebas, los teléfonos falsificados / subestándares tienen un desempeño significativamente inferior a los teléfonos originales con valores de fallos de acceso y llamadas fallidas de 26 % y 24 %, respectivamente.

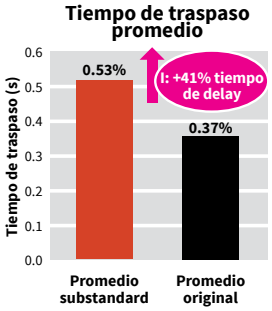


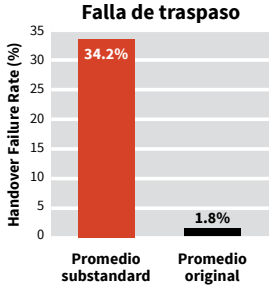


PRUEBA DE CATEGORÍA # 3: Rendimiento de Transmisión

- Una movilidad de teléfono exitosa depende del proceso de transferencia de la llamada de una cobertura de antena a otra.
- Este mecanismo se llama transmisión y debe ser lo más rápido posible. Si la transmisión se retrasa, la transmisión puede fallar y la llamada puede ser terminada (es decir, fallida).

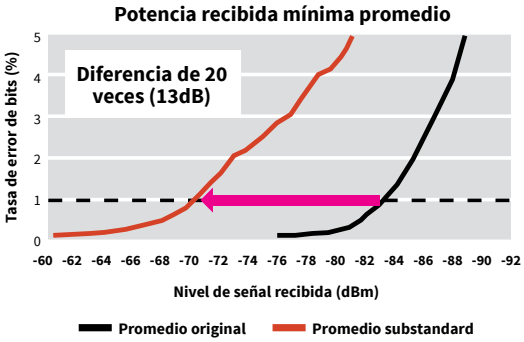


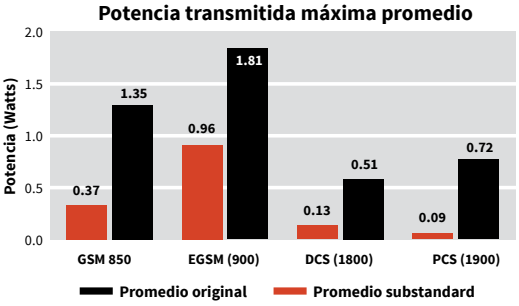




PRUEBA DE CATEGORÍA # 4:
Capacidades de potencia de transmisión:

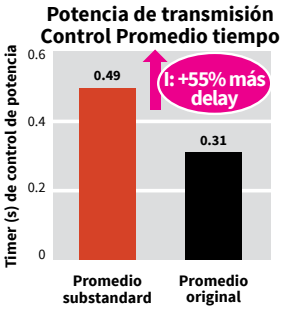
- La potencia de transmisión es muy importante porque afecta a la cobertura geográfica, así como a la calidad de la conexión a la red.
- Distancia máxima de cobertura está restringida por los teléfonos:
  - Potencia mínima recibida desde la torre de antena.
  - La potencia de transmisión máxima que se escuchaba por la antena.
- Distancia máxima de la torre de antena a teléfono disminuye de 57 % para un teléfono falsificado / subestándar para mantener la conexión (llamada de voz).

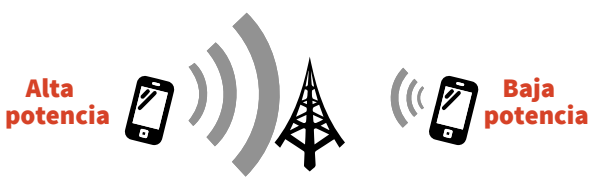




PRUEBA DE CATEGORÍA # 5:
Control de Transmisión de energía:
¿Mi teléfono debería transmitir alto o bajo?

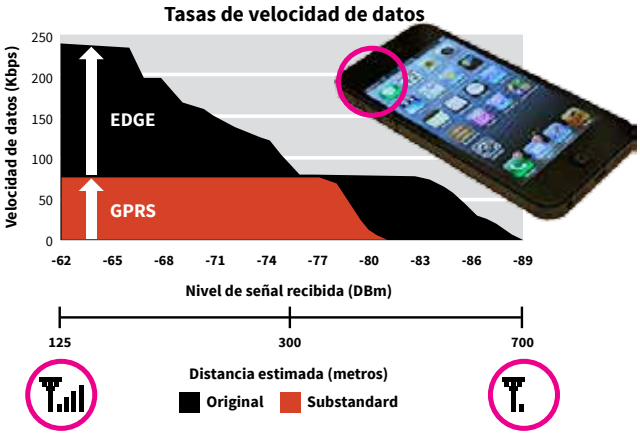
- La potencia de transmisión del teléfono tiene que ser controlada.
- Mecanismo de control con retrasos mínimos.
- Si transmite demasiada energía, el teléfono va a interferir con los otros teléfonos y si transmite muy poco, se degradará su propio servicio.





PRUEBA DE CATEGORIA #6:
¿Qué tan rápido es mi acceso a internet?

- La velocidad del acceso a Internet tiene que ver con la tecnología (GPRS y EDGE) disponible y la calidad de receptor.
- La mayoría de los teléfonos subestándares probados no son compatibles con la tecnología EDGE que nos permite transmitir alrededor de 200kbps.



MMF

Mobile Manufacturers Forum

Diamant Building
Boulevard Auguste Reyers 80
1030 Brussels Belgium
Telephone + 32 2 706 8567
Facsimile + 32 2 706 8569

15th Floor, 100 Queen's Road Central,
Central, Hong Kong
Telephone +852 3180 9375
Facsimile +852 3180 9399

Av. Paulista, 2300 – Piso Pilotis
CEP 01310-300 São Paulo/SP Brazil
Telephone +55 11 2847-4610
Facsimile +55 11 6847-4550

www.mmfai.org