¿**Un equipo aislado de Internet y teniendo el WIFI y el Bluetooth desactivado es seguro**?

Una vez más, la seguridad informática parece una **quimera**, si nos ceñimos a la definición del diccionario, tenemos que es "*un sueño o creación imaginaria que se toma como real, siendo ilusoria, vana y* ***casi imposible de conseguir****"*, la que mejor define, la seguridad informática, en este caso, es el último apartado de la definición.

Aunque parezca poco creíble, una máquina aislada de la red –sin estar conectada a una red local o Wan- denominado como "air gapped", puede ser atacada y revelar su contenido.

Como conseguirlo, una vez más los artífices del desarrollo son Israelí y son investigadores, expertos en seguridad, cuyo ataque conocido como "air gap attacks" siendo su denominación **USBee.**

Este ataque, se lanza desde una memoria USB, compatible con el estándar USB 2.0, evidentemente, para que esto tenga éxito, el dispositivo, debe de conectarse a la máquina víctima del ataque, para conseguir infectar el objetivo con el malware específico.

Parece algo complicado, que si la máquina se encuentra aislada, como se podrá conectar el dispositivo USB infectado, fácil, un estudio Universitario, revela que todos los usuarios tienen la necesidad de abrir los dispositivos que encuentren, para ver su contenido.

¿Cómo se realiza la comunicación del dispositivo USB con el entorno? No hay que olvidar que este tipo de ataque, a sistemas aislados, se reduce a situaciones concretas, pero en resumen, una vez que la máquina objetivo ha sido infectada y, detecta que existe un dispositivo USB, que puede utilizar, comienza a enviar una secuencia numérica de '0', provocando que emita en la banda de VHF y UHF, con un rango de frecuencias de entre 240 y 480 MHz.

Estas frecuencias, pueden ser captadas por un receptor cercano, estando limitada la distancia, **entre 3 y 8 metros**, dependiendo de si este dispositivo utiliza una antena, como puede ser un prolongador de USB (al igual que los móviles que utilizan el cable de los auriculares como antena para el receptor de radio). Podemos tener en cuenta, que para clasificar las ondas de radio se toman como medida los múltiplos de diez en la longitud de onda. Por lo tanto la ondas de VHF tienen una longitud de onda entre **1 Metro** y 10 Metros mientras que las de UHF tienen una longitud de entre **10 Centímetros** y un **Metro**. Como la relación es que la frecuencia es igual a la velocidad de la luz (misma velocidad que la de propagación de las ondas electromagnéticas, aproximadamente 300.000 Km. /h) dividida por la longitud de onda, entonces tenemos que la banda de VHF va desde los 30 MHz a los 300 MHz y la de UHF va de los 300 MHz a los 3 GHz. Esto hace que las frecuencias utilizadas sean ideales para este tipo de objetivos, ya que el típico prolongador de USB (1m a 1,5 m), lo hace ideal para una transmisión en el rango de estas frecuencias.

En este caso, los datos se transmiten a través de una onda portadora, una onda simple cuyo único objetivo es transportar datos modificando una de sus características (amplitud, frecuencia o fase). Por este motivo, la transmisión analógica es generalmente denominada **transmisión de modulación de la onda portadora**. Se definen tres tipos de transmisión analógica, según cuál sea el parámetro de la onda portadora que varía:

- Transmisión por modulación de la amplitud de la onda portadora
- Transmisión a través de la modulación de frecuencia de la onda portadora
- Transmisión por modulación de la fase de la onda portadora

Hay que tener en cuenta, que, como la transmisión es analógica, en el momento de la transmisión, debe convertir los datos digitales (una secuencia de 0 y 1) en señales analógicas (variación continua de un fenómeno físico). Este proceso se denomina **modulación**.

Cuando recibe la transmisión, debe convertir la señal analógica en datos digitales. Este proceso se denomina **demodulación**.

Aunque la distancia limitada te parezca corta, no debes de olvidar que las ondas de radio tienen un tamaño desde centímetros hasta kilómetros. Son tan grandes que la materia simplemente no les molesta pues no llegan a interaccionar con ella (tampoco tienen energía suficiente); así, siempre que la materia no sea lo bastante densa, pueden atravesarla. Por lo tanto, tendrías cobertura suficiente, para, que sin estar en la misma habitación donde se encuentre la máquina objetivo, puedas capturar las emisiones.

Aunque la tasa de transferencia es muy baja, frente a lo que habitualmente estamos acostumbrado, de **unos 80 b/s**, sin embargo es suficiente para apropiarse de una clave de **cifrado de 4096 bits en apenas 10 segundos**. No podemos obviar, que en este tipo de transmisiones, no podemos utilizar el ancho de banda completo para transmitir datos, ya que debemos tener en cuenta, los errores que se producen en la transmisión, siendo la consecuencia inmediata del empleo de la paridad, con la expansión del alfabeto, teniendo que usar más ancho de banda, al transmitir más bits por símbolo de los estrictamente necesarios.

Los datos que son transmitidos, en una portadora hasta un receptor que utilizaría **GNU-radio**, para **desmodular la señal**.

Uno de los accesorios posibles que se pueden utilizar como receptor

Este software, permite obtener información del sistema objetivo a través del puerto USB, aun cuando este, se encuentre totalmente aislado de Internet, no disponga de altavoces, y los sistemas de transmisión como el WIFI o como el Bluetooth estén desactivados.

Y la pregunta final sería, ¿Se puede evitar este tipo de ataque?, la respuesta es sí, como, aislar el equipo o la habitación, en una **caja de Faraday** (*se conoce como el efecto por el cual el campo electromagnético en el interior de un conductor en equilibrio es nulo, anulando el efecto de los campos externos*).

Fuente: http://www.scoop.it/t/cyber-security-by-devid-thomas/p/4068164103/2016/08/30/meet-usbee-the-malware-that-uses-usb-drives-to-covertly-jump-airgaps

Autor: Ricardo R. Jorge Rodríguez, es Ingeniero Técnico en informática de Sistemas, Máster Universitario en Software libre, Perito Forense. Pertenece a la ALI, Colegiado en el COITICV, vocal del CONCITI y actualmente Decano del COITICV.