Fuente:
ComputerWorld

Una compañía estadounidense ha sufrido un ataque informático por medio de este cotidiano dispositivo. Los investigadores de seguridad de Trustwave SpiderLabs se han encontrado con un ataque en el que un dongle USB fue enviado por correo a una compañía bajo la apariencia de una tarjeta de regalo de Best Buy. Esta técnica ha sido utilizada por los profesionales de la seguridad durante las pruebas de penetración física en el pasado, pero no es algo muy común.

El ataque fue analizado y divulgado por investigadores de seguridad, que se enteraron del mismo por el socio comercial de uno de los miembros de su equipo. Ziv Mador, vicepresidente de investigación de seguridad de Trustwave SpiderLabs, cuenta a CSO que una empresa estadounidense del sector de la hostelería recibió el USB a mediados de febrero.

El paquete contenía una carta de aspecto oficial con el logo de Best Buy y otros elementos de marca que informaban al destinatario de que había recibido una tarjeta de regalo de 50 dólares por ser un cliente habitual. "Puedes gastarlo en cualquier producto de la lista de artículos presentado en una memoria USB", decía la carta. Afortunadamente, el USB nunca fue insertado en ningún ordenador y fue pasado para su análisis, porque la persona que lo recibió tenía entrenamiento de seguridad.

El BadUSB
En 2014, en la conferencia de seguridad Black Hat USA, un equipo de investigadores de los Laboratorios de Investigación de Seguridad (SRLabs) con sede en Berlín, demostraron que el firmware de muchos USB puede ser reprogramado para que, cuando se inserta en un ordenador, informe que en realidad es un teclado y comience a enviar comandos que podrían ser utilizados para desplegar malware. Los investigadores llamaron a este ataque BadUSB y es diferente a poner malware en una llave USB y confiar en que el usuario la abra.

"El hecho de que también son baratos y fácilmente disponibles para cualquier persona significaba que era sólo cuestión de tiempo para ver esta técnica utilizada por los delincuentes en la naturaleza", los investigadores de Trustwave dijeron en su informe. "Dado que los dispositivos USB son usados y vistos en todas partes, algunos los consideran inocuos y seguros. Otros pueden ser muy curiosos sobre el contenido de un dispositivo USB desconocido. Si esta historia nos enseña algo, es que uno nunca debe confiar en tal dispositivo."

Disponible en:
https://cso.computerworld.es/cibercrimen/el-comun-dongle-usb-la-nueva-he... [1]

Links

[1] https://cso.computerworld.es/cibercrimen/el-comun-dongle-usb-la-nueva-herramienta-de-los-piratas-informaticos