RED AZUL INFORMA

"BAITING": MALWARE EN UNA MEMORIA USB APARENTEMENTE ABANDONADA.

- **La víctima conecta a su ordenador un USB que se ha encontrado en la calle.**
- **El USB contiene un *malware* que se autoejecuta inmediatamente una vez se conecta la memoria al ordenador de la víctima.**

Los dispositivos de memoria USB son uno de los nuevos cebos utilizados por los ciberdelincuentes para infectar los equipos de los usuarios. A este tipo de ataque se conoce como ***baiting*** y es más común de lo que parece.

Esta modalidad consiste en **dejar a la vista de la víctima la memoria USB**, la cual pensará que la misma ha sido extraviada por su dueño. De esta manera, la conectará en su dispositivo para comprobar su contenido y tratar de averiguar quién es su titular.

Los ciberdelincuentes suelen introducir en estos USB ***malwares*** para que se autoejecuten en el momento en que son conectados a un ordenador, con el objetivo de **obtener toda la información posible de sus víctimas**: contraseñas, emails, características del sistema para realizar ataques más complejos o simplemente, extender su red de dispositivos infectados.

RECOMENDACIONES:

- **Mantener el equipo actualizado**, incluyendo las *apps*, el software y el antivirus.
- **No conectar dispositivos encontrados** o de origen desconocido. Del mismo modo, se debe **tener siempre controlados nuestros propios dispositivos** para evitar que caigan en malas manos y puedan ser infectados.
- **Deshabilitar la función de autoarranque de dispositivos USB.**

Se recuerda que desde la Oficina de Seguridad del Internauta (OSI) se pone a disposición la Línea de Ayuda en Ciberseguridad, 017.