Troyano

Es un tipo de malware que a menudo se disfraza de software legitimo. Se pueden utilizar para tratar de acceder a los sistemas de los usuarios. Generalmente, los usuarios son engañados por alguna forma de ingeniería social para que descarguen y ejecuten troyanos en sus dispositivos. Una vez activados pueden darle accesos al ciberdelincuente para espiar, robar información confidencial y obtener acceso de puerta trasera al sistema.

¿Cómo funciona?

El usuario debe de activarlos para que realice su trabajo. Los troyanos pueden infectar los dispositivos de diferentes maneras como pueden ser:

- **Phishing y Ingeniería Social**: Correos electrónicos maliciosos con archivos adjuntos infectados o enlaces a sitios web maliciosos son una de las principales formas de distribución de troyanos.
- **Software de Fuentes No Confiables**: Descargar software de sitios web no oficiales, redes P2P o fuentes no verificadas aumenta el riesgo de descargar troyanos disfrazados de programas legítimos.
- **Redes Wi-Fi Falsas (Evil Twin)**: Los atacantes crean puntos de acceso Wi-Fi con nombres similares a redes legítimas para engañar a los usuarios y redirigirlos a sitios web maliciosos que distribuyen troyanos a través de exploits de navegador o descargas engañosas

Tipos de troyanos

- **Puertas traseras:** Ofrece a los usuarios maliciosos control a distancia del dispositivo infectado. permitiendo a los atacantes acceder al dispositivo de forma remota sin la autorización del usuario.
- **Exploits:** Los exploits son programas que contiene datos o códigos que aprovechan una vulnerabilidad del software de aplicaciones que se ejecutan en el dispositivo.
- **Troyano Clampi:** También conocido como Ligats e llom, se mantiene a la espera de que los usuarios inicien sesión para realizar una transacción financiera, como acceder a la banca en línea o ingresos a los datos de tarjetas de crédito para una compra en línea.
- **Troyano Wacatac:** Es una amenaza troyana muy dañina que puede llevar a cabo diversas acciones maliciosas en el sistema de destino. Se clasifica como un troyano de acceso remoto (RAT) y puede realizar una amplia gama de acciones maliciosas, incluyendo robo de información, control remoto del sistema, descarga e instalación de malware adicional, y más.