

LA SUPERFICIE DE ATAQUE EN LOS DISPOSITIVOS IoT



¿Qué buscan obtener los atacantes de los IoT?



Información

Los IoT contienen una gran cantidad de información que puede ser crítica, privada o sensible, dependiendo del entorno o la industria.



Movimiento Lateral

Un solo dispositivo IoT expuesto puede permitir que un ciberdelincuente obtenga acceso a la red corporativa o industrial de una empresa, lo que a su vez puede provocar otros tipos de ataques como el sabotaje.



Ganancias Monetarias

Los ataques de IoT pueden ser rentables para los cibercriminales, que pueden optar por vender los datos robados o solicitar el pago de un rescate para renunciar al control de los activos comprometidos.



Base de Ataque

Los hackers pueden utilizar los dispositivos IoT como base para ataques que pueden expandirse hacia el exterior o más profundamente en la infraestructura principal víctima. Inclusive pueden construir un nodo de canal seguro para enmascarar su tráfico malicioso para ejecutar alguna o varias amenazas como malware, APT's y ataques dirigidos.

¿Cuáles son los ataques a IoT más comunes?

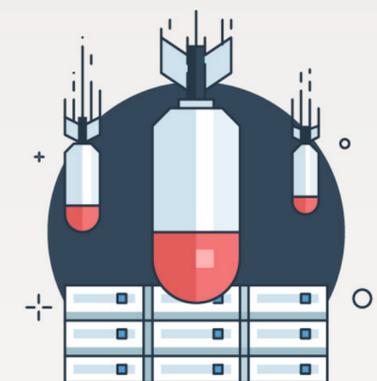
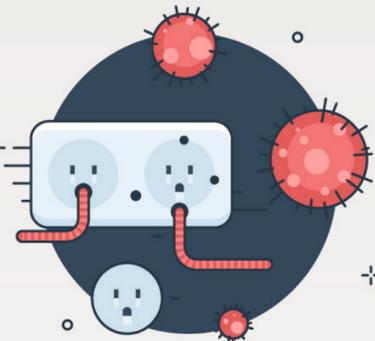


Explotación de Vulnerabilidades

La gran cantidad de componentes utilizados en los dispositivos IoT provoca que puedan tener una gran cantidad de vulnerabilidades que pueden ser explotadas por los ciberatacantes si no son parchadas a tiempo o no se cuenta con los parches de seguridad.

Malware como troyanos, backdoors y ransomware puede ser instalado a través de aplicaciones, dispositivos, firmware, protocolos y otros componentes vulnerables dentro de los sistemas IoT.

Malware



Dos & DDoS

El creciente número de dispositivos IoT y su conectividad hacen que sean susceptibles y vulnerables a los ataques de Botnets como los utilizados para la denegación de servicios distribuida (DDoS).

Ataques de Man-in-the-middle

Los protocolos y redes inseguras permiten a los atacantes posicionarse entre los canales de comunicación y robar tu información sin que te des cuenta.



Manipulación Física

El dar mantenimiento a nuestros dispositivos en sitios no autorizados ni certificados o dejarlos al alcance de personas malintencionadas puede provocar que estos sufran de alteraciones físicas que afecten su correcto funcionamiento y que puedan ser reemplazados parcial o totalmente con otros dispositivos menos seguros y apócrifos, que pueden poner en riesgo tu seguridad.

Espionaje y Robo de Información

Los ciberatacantes pueden aprovecharse de la transmisión y el almacenamiento de datos de los sistemas IoT para obtener acceso a información y eventos críticos a través de un monitoreo en tiempo real, con el objetivo de recabar estos datos con fines maliciosos.

