Un ataque de Día Cero, Zero Day ó 0Day, es un tipo de ataque contra un sistema o aplicación, que como objetivo tiene la ejecución de código malicioso, mediante vulnerabilidades que son desconocidas por la gente y por el fabricante o desarrollador.

Cuando se encuentra una vulnerabilidad de este tipo, generalmente es explotada por potenciales atacantes, hasta que se publica en foros de Internet.

Los ataques de día cero son considerados como los más peligrosos cuando se habla de una guerra informática.
La gente que se dedica al malware pueden aprovecharse de tales vulnerabilidades con diferentes vías de ataque, como códigos en páginas web, que revelan vulnerabilidades en navegadores.

También es posible descubrir las vulnerabilidades utilizando aplicaciones para lograr abrir ciertos documentos que revelan los fallos en seguridad.

Es posible que los piratas informáticos utilicen dichos ataques para conseguir información confidencial, como contraseñas bancarias, por lo que se convierte en un gran negocio, ya que cuando un pirata logra encontrar una vulnerabilidad de este tipo, puede aprovecharla para obtener grandes ingresos, o en su caso, venderla al mejor postor.

Un 0Day de páginas importantes puede venderse en más de 8,000 dólares. Existe la llamada “Protección día-cero”, que es la habilidad para proporcionar protección contra ataques, como limitar los ataques referentes a vulnerabilidades en memoria, donde se utilizan técnicas como buffer overflow.

Existen empresas especializadas en este tipo de protección, como Gama-Sec en Israel y DataClone Labs en Reno, Nevada.

Hablando éticamente, las empresas de seguridad informática investigan estos ataques para

poder entender el funcionamiento de las vulnerabilidades, así como empresas que compran dichas vulnerabilidades con el objetivo de seguir investigando, como ocurre con la Iniciativa Zero Day.

Cabe mencionar que la compra y venta de esta información es legal en muchas partes del mundo, sin embargo, existe mucha controversia sobre la revelación de la información, ya que aunque buscar, encontrar y vender la información necesaria pueda resultar legal, por lo general el comprador la utilizará para fines ilegales.

Por esta razón, muchas empresas que manejan información delicada, contratan hackers para buscar y reparar
estas vulnerabilidades.