Cuando hablamos de seguridad cibernética y hacking, es común encontrarse con el término exploit, que tiene como significado explotar o aprovechar, generalmente utilizado para realizar acciones maliciosas en contra de un sistema aprovechando una o más vulnerabilidades.

Entre las acciones que se pueden realizar con un exploit, se encuentran el acceso no autorizado a sistemas, tomar el control de un equipo de cómputo o cualquier otro dispositivo, escalada de privilegios, ejecución de ataques de denegación de servicio, entre otros.

Existen distintos tipos de exploits, dependiendo del sistema o software vulnerable, pueden clasificarse como:

- Exploit remoto: Se utiliza en una red de comunicaciones para acceder al sistema víctima.
- Exploit local: Se necesita tener acceso al sistema vulnerable.
- Exploit en cliente: Se aprovechan las vulnerabilidades de aplicaciones que por lo general están instaladas en gran parte de las estaciones de trabajo de las empresas.

Por otro lado, existen exploits desarrollados para compañías o software de los que no se tiene conocimiento de vulnerabilidades sin parchear, por los que los hackers buscan o compran vulnerabilidades de día cero.

De este tipo, los más comunes son para hackear empresas financieras o de Internet, como redes sociales. Entre los exploits más buscados para este fin, se encuentran los que se puedan utilizar contra Facebook, WhatsApp o Twitter, e incluso existen empresas que pueden otorgar dichos exploits, como hackear facebook xploitz que provee este tipo de software para aprovechar vulnerabilidades.

En el caso de las vulnerabilidades de día cero, también conocidas como 0-day, se aprovecha un fallo en el sistema o software víctima de reciente descubrimiento, por el que dependiendo de la organización víctima, podría venderse hasta por millones de dólares.

Esto debido a que como no se tiene conocimiento suficiente sobre la brecha de seguridad, podría explotarse y causar un impacto enorme a la empresa u organización, ocasionando pérdidas tanto financieras como de información.

Es por esto que compañías como Google o Apple pagan buenas recompensas a hackers por informar sobre vulnerabilidades en sus sistemas. De este modo, las empresas que obtienen la información de los hackers éticos, podrán lanzar mitigaciones en lo que encuentran una solución que pueda lanzarse en modo de parche.

Algunos exploits se desarrollan con el fin de proporcionar acceso de administrador o superusuario a un sistema objetivo, adoptando la forma de varios tipos de malware, como gusanos, troyanos o spyware.