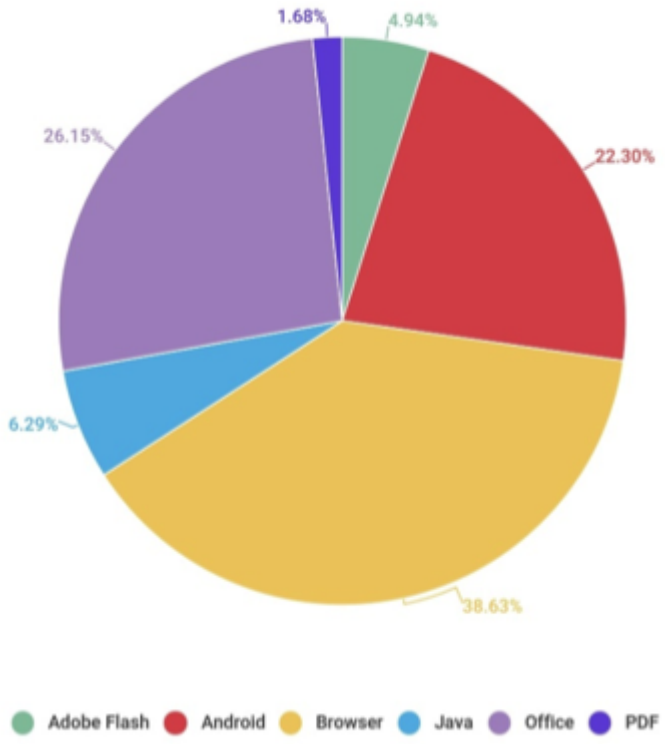
Los exploits: tendencia en las nuevas amenazas

La propagación incontrolada de paquetes de **exploits** cambió el panorama de las amenazas cibernéticas durante el segundo trimestre de 2017, de acuerdo con el último informe de Kaspersky Lab que e"l crecimiento alcanzó su punto máximo al final del trimestre, lo que indica la implacable escala de esta amenaza cibernética.

Un **exploit es un tipo de malware** que utiliza errores en el software para infectar dispositivos con código malicioso adicional como **troyanos bancarios, ransomware o malware de espionaje cibernético**.



Los ataques realizados con la ayuda de exploits están entre los más eficaces, ya que generalmente **no requieren de ninguna interacción con el usuario** y pueden distribuir su código sin que el usuario sospeche nada, dice el informe de Kaspersky Labs.

El segundo trimestre de 2017 experimentó una ola masiva de estas vulnerabilidades incontroladas debido a una serie de exploits que se filtraron en la web. Esto generó un cambio significativo en el panorama de las amenazas cibernéticas. Se **inició principalmente con la publicación del archivo "Lost In Translation"** por el grupo Shadow Brokers, que contenía una gran cantidad de exploits para diferentes versiones de Windows.

El daño causado por el malware que utilizó exploits originados en el archivo, así como el número de usuarios infectados, va más allá, y las pandemias de ExPetr y WannaCry son los ejemplos más

notables. Otro ejemplo es la vulnerabilidad CVE-2017-0199 en Microsoft Office, descubierta a principios de abril. A pesar de que fue reparada en el mismo mes, el número de usuarios atacados alcanzó un máximo de 1.5 millones.