**Sujetos Intervinientes en un Delito Informático: Caso Xamalicious**

**Cibercriminales**

**Definición**: Personas o grupos que crean y distribuyen el malware.

**Ejemplo**: Los creadores de Xamalicious, que insertaron el virus en aplicaciones de la Google Play Store para robar información de los usuarios.

**Víctimas**

**Definición:** Usuarios afectados por el malware, que sufren pérdida de información o privacidad.

**Ejemplo:** Los usuarios de Android que descargaron aplicaciones infectadas y vieron comprometidos sus datos personales.

**Proveedores de Servicios**

**Definición:** Empresas que distribuyen aplicaciones y deben asegurar su seguridad.

**Ejemplo:** Google, que falló en detectar el malware en las aplicaciones disponibles en la Google Play Store.

**Desarrolladores de Seguridad**

**Definición:** Profesionales y empresas que crean herramientas para proteger contra amenazas informáticas.

**Ejemplo:** Empresas de ciberseguridad que detectaron y eliminaron las aplicaciones infectadas de la Google Play Store.

**Autoridades y Organismos Reguladores**

**Definición:** Entidades que crean y aplican leyes de ciberseguridad y investigan delitos informáticos.

**Ejemplo:** Agencias gubernamentales que podrían investigar y perseguir a los responsables de distribuir Xamalicious.

**Educadores y Concienciadores**

**Definición:** Personas y organizaciones que enseñan sobre ciberseguridad.

**Ejemplo:** Expertos que publican guías sobre cómo evitar malware y promover buenas prácticas de seguridad.

**Investigadores de Seguridad**

**Definición:** Profesionales que estudian nuevas amenazas y desarrollan métodos para prevenirlas.

**Ejemplo:** Investigadores que descubrieron cómo Xamalicious evade las medidas de seguridad y compartieron esta información para mejorar las defensas.

Esta estructura resume los roles de cada sujeto interviniente de manera clara y concisa.