Ciberdelincuencia y agentes de la Amenaza

- **DotNet:** Plataforma de desarrollo de software desarrollada por Microsoft que incluye un gran conjunto de bibliotecas y herramientas.
- **Business E-mail Compromise (BEC):** Táctica de estafa en la que un atacante compromete correos electrónicos empresariales para realizar transferencias financieras fraudulentas.
- **Cartas nigerianas:** Esquema de estafa en línea que involucra solicitudes de ayuda o transacciones financieras fraudulentas.
- **Cryptojacking:** Uso no autorizado de dispositivos informáticos para minar criptomonedas sin el consentimiento del propietario.
- **Denegación de servicio (DoS):** Ataque que busca hacer que un recurso sea inaccesible para sus usuarios previstos.
- **Ingeniería social:** Técnica que manipula a las personas para obtener información confidencial o acceder a sistemas.
- **Inyección SQL:** Vulnerabilidad en aplicaciones web que permite a un atacante ejecutar comandos SQL no autorizados.
- **Malware:** Software malicioso diseñado para dañar, acceder sin autorización o recopilar información de sistemas.
- **Pharming:** Redireccionamiento fraudulento de tráfico de internet a un sitio web falso.
- **Phishing:** Intento de obtener información confidencial haciéndose pasar por una entidad de confianza.
- **Spear phishing:** Forma de phishing dirigida a un individuo o entidad específica con información personalizada.
- **Ransomware:** Tipo de malware que cifra archivos o

sistemas y exige un rescate para restaurar el acceso.

- **Skimming:** Técnica para robar información de tarjetas de crédito/débito a través de dispositivos ilegítimos.
- **Spoofing:** Falsificación de datos de identificación para parecerse a algo legítimo.
- **Spyware:** Software que recopila información sin el conocimiento o consentimiento del usuario.
- **Troyano:** Programa malicioso que parece legítimo pero realiza acciones no autorizadas en segundo plano.
- **XSS (Cross-Site Scripting):** Vulnerabilidad web que permite a un atacante inyectar scripts maliciosos en páginas web vistas por otros usuarios.
- **Zero-day:** Vulnerabilidad de seguridad que se explota antes de que se conozca su existencia, dejando poco o ningún tiempo para una solución.
- **Cibercriminales:** Individuos que llevan a cabo actividades ilegales o maliciosas en línea.
- **Crime as Service:** Modelo de negocio cibercriminal en el que se venden servicios, herramientas o infraestructura para llevar a cabo actividades delictivas en línea.
- **Hacktivistas:** Individuos que realizan acciones de hackeo o ciberataques para promover causas políticas o sociales.
- **Insider threat:** Riesgo de amenazas internas a la seguridad, ya sea intencional o no intencional, por parte de empleados o personas internas.
- **APTs (Advanced Persistent Threats):** Amenazas cibernéticas altamente sofisticadas y dirigidas que persisten durante largos períodos de tiempo.
- **Cyber Kill Chain:** Modelo que describe las etapas de un ciberataque, desde la identificación del objetivo hasta el compromiso y el daño.