POLICÍA NACIONAL · ESCALA BÁSICA

TEMA

41

Ciberdelincuencia y agentes de la amenaza

Ciberdelincuencia y agentes de la Amenaza: Botnet; Business E-mail Compromise; Cartas nigerianas; Cryptojacking; Denegación de servicio; Ingeniería social; Inyección SQL; Malware; Pharming; Phishing; Spear phishing; Ransomware; Skimming; Spoofing; Spyware, Troyano; XSS; Zero-day. Cibercriminales. Crimen as Service. Hacktivistas. Insider threat. APTs. Cyber Kill Chain.

§

NOVIEMBRE DE 2026

Material de elaboración propia a partir de las fuentes oficiales que se citan al final del tema. No es un temario oficial ni sustituye a la normativa publicada.

Índice

Presentación

1. Ciberdelincuencia y agentes de la amenaza
    - 1.1. Conceptos de partida
    - 1.2. Dos factores: la técnica y la persona
    - 1.3. Cómo se agrupan las amenazas en este tema
2. Ingeniería social y fraudes de engaño
    - 2.1. Ingeniería social
    - 2.2. Phishing
    - 2.3. Spear phishing
    - 2.4. Fraude del CEO y Business E-mail Compromise (BEC)
    - 2.5. Cartas nigerianas
    - 2.6. Spoofing
    - 2.7. Pharming
3. Malware y redes de equipos infectados
    - 3.1. Qué es el malware
    - 3.2. Troyano
    - 3.3. Spyware
    - 3.4. Ransomware
    - 3.5. Botnet
    - 3.6. Cryptojacking
4. Ataques a servicios y aplicaciones, y fraude con tarjetas
    - 4.1. Denegación de servicio (DoS) y denegación de servicio distribuida (DDoS)
    - 4.2. Inyección de código e inyección SQL
    - 4.3. XSS (Cross-site Scripting)
    - 4.4. Zero-day
    - 4.5. Skimming
5. Los agentes de la amenaza
    - 5.1. Una clasificación por motivación
    - 5.2. Cibercriminales
    - 5.3. Crimen como servicio (*Crime as a Service*)
    - 5.4. Hacktivistas
    - 5.5. Insider threat (amenaza interna)
    - 5.6. APT (Amenaza Avanzada Persistente)
6. La Cyber Kill Chain
    - 6.1. Qué es y para qué sirve
    - 6.2. Las siete fases

6.3. La cadena y los conceptos del tema

No confundas

Ideas clave

Autoevaluación

Soluciones

Fuentes