Phishing

- Tipos
  - ~~False Positive~~
  - Vising/Smishing — vector de ataque es una llamada telefónica/vector de ataque un mensaje de texto o SMS
  - Whaling — ataque de phishing muy selectivo que se dirige a personas que ocupan puestos de dirección en una organización
  - Social Engineering — práctica de explotar a un ser humano en lugar de un sistema, utilizando métodos psicológicos para conseguir que realicen acciones que normalmente no harían
  - Spam — correos no solicitados, no deseados o inesperados, pero que no son necesariamente de naturaleza maliciosa
  - Recon — para comprobar si el buzón de destino está en uso
  - Credential Harvester — intenta recuperar credenciales válidas que pueden utilizarse para obtener acceso a servicios y cuentas como resultado de ataques de relleno de credenciales.
- Técnicas
  - Spear Phishing — se produce cuando un actor malicioso dedica tiempo antes del ataque de phishing a recopilar información sobre su objetivo específico
  - Attachments
    - Social Engineering FIles — documento no malicioso que solicita info valiosa para el atacante
    - Señuelo (Lure Documents) — documento con enlace malicioso
    - Malicious Files
  - Sender Spoofing
  - Typosquatting/Homographs — Errores tipográficos, cambiando letras o el orden para engañar/ Uso de letras en otros idiomas que simulan las correctas
  - Impersonation
  - Use legitimate services
  - Hyperlinks
  - Url-Shorteners — `Wannabrowser` ↗
  - HTML Styling
  - Business email compromise
- Análisis
  - Email Artefacts
    - Sending Email Adress
    - Subject Line
    - Recipient Email Addresses
    - Sending Server IP & Reverse DNS — `MxToolBox` ↗
    - Reply-to Adress
    - Date & Time
    - } **`PhishTool`** ↗
  - File Artefact
    - Attachment Name
    - SHA256 Hash Value

      ```
      WIndows PowerShell:
      PS C:\Users\fran\Downloads>
       Get-FileHash .\WindowsSensor.exe ; Get-FileHash -Algorithm md5 .\WindowsSensor.exe ;
      Get-FileHash -Algorithm sha1 .\WindowsSensor.exe

      Linux:
      sha256sum <file>
      sha1sum <file>
      md5sum <file>
      ```

      - `Talos` ↗
      - `VirusTotal` ↗
      - `Hybird-Analysis` ↗
  - Web Artefact
    - Full URLs
      - `Phistank` ↗
      - `URL2PNG` ↗
      - `URLhaus` ↗
      - `URLScan` ↗
    - Root Domain
- Respuesta
  - Immediate Response Process
    1. Recuperar una copia original del correo electrónico de phishing
    2. Recoger los artefactos del correo electrónico de phishing
    3. Informar a los destinatarios que recibieron el correo electrónico
    4. Investigar los artefactos maliciosos para recoger indicadores de compromiso que puedan ser bloqueados para proteger a la organización
    5. Tomar medidas defensivas
    6. Completar el informe de investigación, documentando todos los pasos anteriores
  - Blocking Email Artifacts
    - Email Sender (mailbox@domain)
    - Sender Domain (@domain)
    - Sending Server IP
    - Subject Line
  - Blocking Web Artifacts
    - Web Proxy: URL block
    - DNS Blackholing (entrada dns falsa para redirgir al usuario cuando hace click a dominio malicioso)
    - Firewall
  - Blocking File Artifacts
    - Block hash
    - Block name
  - Informing Threat Intelligence Team
- Contramedidas
  - Security Awareness Training
    - Awareness training
    - Simulated Phishing Attacks
  - Attachment Filtering
  - Attachment Sandbox
  - Spam Filter
    - Gateway Spam Filters
    - Hosted Spam Filters
    - Desktop Spam Filters
    - } **Tipos**
      - Content Filters
      - Rule-Based Filters
      - Bayesian Filters — basado en machine learning para marcar correos similares como SPAM
  - Anti-spoofing records
    - SPF — Identifica IPs o hostnames que pueden enviar correos para nuestro dominio
    - DKIM — correo electrónico cifrado
    - DMARC — protocolo establece qué hace si falla SPF y/o DKIM: none, quarantine, and reject
  - Marking External Emails

Presented with xmind