VII CIBERLIGA Modalidad Pre-Amateur
Explicación de los retos de la Fase Clasificatoria

GUARDIA CIVIL

MINISTERIO DEL INTERIOR
GUARDIA CIVIL

Contenido

1. GENERALIDADES

En los últimos años, tal y como se expone en la conferencia de concienciación (primera de las actividades formativas de la CIBERLIGA Pre-Amateur), las redes sociales representan una de las principales herramientas de comunicación para nuestros jóvenes. Es por ello, que se han convertido en el escenario ideal para la captación de menores por parte de grupos criminales especializados en cometer delitos de fraude, sextorsión y obtención ilícita de datos e imágenes privadas, los cuáles constituyen una de las principales amenazas del ciberespacio.

A través de anuncios llamativos, concursos ficticios y castings inexistentes, los delincuentes simulan oportunidades atractivas para que los jóvenes proporcionen voluntariamente información personal, fotografías, vídeos o incluso datos bancarios.

Ante este complejo y peligroso contexto, el desafío propuesto para la competición de la Fase Clasificatoria se basa en un ejercicio que pretende simular una dinámica real de actuación de ciberdelincuentes, dónde sus víctimas serán los participantes de la CIBERLIGA Pre-Amateur. Bajo esta dinámica real, la competición se desarrolla en la modalidad CTF (Capture The Flag), tratando de reproducir una campaña fraudulenta inspirada en modus operandi detectados en España durante 2024 y 2025. En esta ocasión, el desafío de la competición se basa en una campaña publicitaria viral en redes sociales: banners con rostros famosos (a menudo deepfakes generados por IA) que invitan a participar en un casting online para un evento o serie de moda.

De este modo, los retos usan la página www.miercoles.influencersymodelos.eu, una supuesta agencia relacionada con un casting para jóvenes influencers y modelos. A primera vista, el sitio web intenta aparentar profesionalidad, pero bajo la superficie, se ocultan múltiples señales de alerta: un dominio reciente, falta de historial, servidores sospechosos y formularios que solicitan datos extremadamente sensibles. Siguiendo estos patrones reales, los participantes deberán analizar la infraestructura digital que sostiene la web, el comportamiento del dominio, su antigüedad, los posibles usos previos, la presencia de ficheros sospechosos y los elementos de ingeniería social empleados para engañar a menores.

Cada uno de los retos del desafío reproduce una fase del proceso criminal, basado principalmente en técnicas variadas de ingeniería social, como puede ser el gancho inicial en redes sociales para comenzar con la captación. Y de ahí, se pasa a la redirección a la web fraudulenta y la descarga del malware tipo stealer (programa informático malicioso del tipo troyano, diseñados para robar información confidencial de dispositivos infectados), que si bien en la competición es inonfensivo, se usa habitualmente para capturar credenciales, métodos de pago, imágenes personales y otros datos que más tarde son utilizados para el chantaje o la extorsión.

De este modo, a través de los retos propuestos, los cuáles evolucionan de manera progresiva en su dificultad, los participantes aprenderán paso a paso cómo

detectar indicadores clave de fraude, identificar páginas maliciosas, examinar el historial de un dominio, encontrar fallos de desarrollo que revelan su procedencia y a analizar ejecutables peligrosos. En definitiva, aprenderán a comprender cómo una campaña aparentemente inofensiva puede escalar hacia delitos graves. Todo ello, en un entorno controlado y seguro, donde ningún dato real es recopilado y donde todos los archivos ejecutables son simulados. Aun así, reproduce con precisión los métodos actuales utilizados en campañas reales de ingeniería social dirigidas a menores en España y Europa.

2. OBJETIVOS DE LOS RETOS

Atendiendo al diseño del desafío propuesto para la competición, en función de los diferentes retos que lo componen, el objetivo general de los retos de la Fase Clasificatoria y de la competición en su conjunto, es enseñar a los participantes de la CIBERLIGA Pre-Amateur a proteger su identidad digital, sus dispositivos y su información frente a amenazas reales en Internet.

El referido objetivo general, se compone a su vez de una serie de objetivos específicos, los cuales se pretenden alcanzar de manera progresiva a través del desarrollo de los distintos retos propuestos. Conforme a ello, los objetivos específicos que permitirán la consecuación del objetivo general, son los siguientes:

- Reforzar la seguridad personal ante fraudes online, aprendiendo a detectar webs falsas o dominios sospechosos.
- Mejorar la detección temprana de malware y la comprensión del hash como herramienta de integridad.
- Sensibilizar sobre la exposición de información y malas prácticas web, como contraseñas visibles o código inseguro.
- Desarrollar la capacidad de analizar imágenes forenses y metadatos, comprendiendo riesgos de privacidad y geolocalización.
- Concienciar sobre la gestión segura de contraseñas y brechas de datos personales, promoviendo la ciberhigiene.
- Mejorar el conocimiento de técnicas básicas de rastreo digital y análisis OSINT, como ping, whois o archive.org.

3. EXPLICACIÓN Y FUNDAMENTO DE LOS RETOS

Con el fin de alcanzar los objetivos señalados en el apartado anterior, los retos que componen el desafío de la Fase Clasificatoria son los siguientes:

1º RETO: *Leer es comprender*.

- Objetivos: entender qué es una FLAG y cómo funciona un reto CTF, aprender a leer con atención y seguir instrucciones con precisión.
- Propósito: introducir la dinámica de la competición y fomentar la atención antes de actuar.
- Impacto: mejora la comprensión lectora, la paciencia y la metodología de resolución de retos digitales.
- Herramientas o recursos a utilizar: Ninguna.

- Dominios: Ninguno.

2º RETO: *Buscando a Nemo*.

- Objetivos: obtener la IP de un dominio aplicando el comando ping y entender su función.
- Propósito: aplicar una técnica básica de rastreo digital.
- Impacto: mejora el análisis técnico y la conciencia ante fraudes online.
- Herramientas o recursos a utilizar: Terminal de Windows / Terminal de Linux / ping.eu.
- Dominios:
  - ✓ https://miercoles.influencersymodelos.eu/
  - ✓ https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/ping
  - ✓ https://ping.eu/ping/

3º RETO: *Slow Mobius (Cámara Lenta).*

- Objetivos: saber usar herramientas whois y extraer la fecha/hora de creación de un dominio en el formato indicado.
- Propósito: verificar antigüedad de un dominio para evaluar su fiabilidad en una investigación digital.
- Impacto: mejora habilidades de rastreo y juicio crítico (detectar dominios fraudulentos o reutilizados) y aporta práctica en manejo de formatos temporales para evidencias.
- Herramientas o recursos a utilizar: "*whois*".
- Dominios:
  - ✓ https://miercoles.influencersymodelos.eu/
  - ✓ https://www.eurid.eu/en/
  - ✓ https://www.dondominio.com/es/whois/

4º RETO: *Metadato perdido.*

- Objetivos: extraer metadatos EXIF (GPS) de imágenes y convertir coordenadas en un lugar real.
- Propósito: enseñar análisis forense de imágenes y uso de herramientas OSINT (FotoForensics, Google Maps) para geolocalización.
- Impacto: desarrolla habilidades prácticas en privacidad y rastreo (comprender riesgos de compartir fotos), precisión en interpretación de datos y pensamiento crítico en investigaciones digitales.
- Herramientas o recursos a utilizar: Herramientas de obtención de metadatos.
- Dominios:
  - ✓ https://miercoles.influencersymodelos.eu/
  - ✓ https://fotoforensics.com/

5º RETO: *El buzón maldito.*

- Objetivos: usar *Have I Been Pwned* para comprobar si un correo ha sido filtrado y en qué brecha.

- Propósito: concienciar sobre la exposición de datos personales y el riesgo de reutilizar credenciales.
- Impacto: fomenta la ciberhigiene, la gestión segura de contraseñas y la comprensión del valor de la información personal.
- Herramientas o recursos a utilizar: "*Have I Been Pwned*".
- Dominios:
  - ✓ https://miercoles.influencersymodelos.eu/
  - ✓ https://haveibeenpwned.com/

6º RETO: *Link que veo, link con el que me infecto.*

- Objetivos: usar VirusTotal para analizar archivos sospechosos y obtener su hash SHA-256.
- Propósito: aprender a comprobar la integridad y posible maliciosidad de un fichero.
- Impacto: refuerza la capacidad de detección temprana de malware y la comprensión del hash como huella digital en ciberseguridad.
- Herramientas o recursos a utilizar: "*VirusTotal*".
- Dominios:
  - ✓ https://miercoles.influencersymodelos.eu/
  - ✓ https://www.virustotal.com/

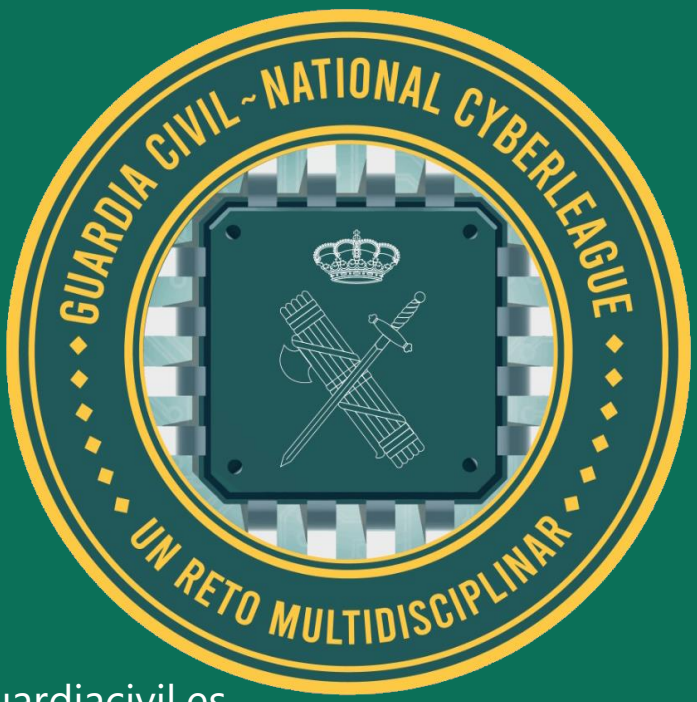
7º RETO: *Reciclar es vivir*.

- Objetivos: usar Archive.org para consultar versiones antiguas de una web y extraer información histórica (qué ofrecían).
- Propósito: enseñar preservación y análisis temporal de contenidos web para detectar cambios y fraudes repetidos.
- Impacto: mejora la capacidad de investigación histórica (ver evidencia de estafas previas), contextualiza amenazas y aporta práctica en fuentes de OSINT.
- Herramientas o recursos a utilizar: "*Archive ORG*".
- Dominios:
  - ✓ https://miercoles.influencersymodelos.eu/
  - ✓ https://archive.org

8º RETO: *Bisturí*.

- Objetivos: localizar comentarios en el código fuente de una página y extraer información sensible (contraseña en español).
- Propósito: enseñar a inspeccionar código fuente como técnica OSINT/forense para encontrar artefactos dejados por desarrolladores.
- Impacto: mejora habilidad práctica de inspección web, conciencia sobre malas prácticas (exponer contraseñas) y capacidad para extraer evidencia técnica.
- Herramientas o recursos a utilizar: Herramienta de visor de código fuente del navegador
- Dominios:
  - ✓ https://miercoles.influencersymodelos.eu/

Bases de participación VII CIBERLIGA
Modalidad Pre-Amateur



www.guardiacivil.es

MINISTERIO
DEL INTERIOR

GUARDIA CIVIL