1. PERFIL DEL OBJETIVO (DATOS DE ENTRADA)
Nombre del sujeto: [redacted] [redacted] Alias principal: "DarkWatcher_99" / [redacted] Correo electrónico: j[redacted]@gmail.com Teléfono: +1 (555) [redacted]-[redacted]
Ubicación: [redacted], Estados Unidos
Alcance de la investigación: Análisis OSINT profundo que abarca puntos de datos de la web superficial, la web profunda y la web oscura. Evaluación de la huella digital, credenciales expuestas y posibles vulnerabilidades de seguridad.

2. METODOLOGÍA Y HERRAMIENTAS
La investigación se llevó a cabo utilizando Parrot Security OS en un entorno sandbox seguro y aislado. Se aplicaron los siguientes protocolos:
OSINT y SOCMINT (Inteligencia de Redes Sociales): Referencia cruzada de la disponibilidad de nombres de usuario en más de 300 plataformas mediante scripts automatizados y verificación manual.
Eliminación de Falsos Positivos: Análisis manual de cada punto de datos para descartar homónimos (personas con el mismo nombre) y coincidencias incorrectas en bases de datos.
Correlación de Filtraciones de Datos: Búsqueda realizada en bases de datos filtradas conocidas (Colecciones n.° 1-n.° 5, BreachCompilation) para identificar contraseñas comprometidas.
Rastreo de la Dark Web: Monitoreo de sitios web y mercados de venta de información personal identificable (PII) del sujeto.

3. HALLAZGOS DETALLADOS
3.1. Redes sociales y huella digital
Estado: [ALTA EXPOSICIÓN DETECTADA]
El sujeto utiliza el nombre de usuario [redacted] en múltiples plataformas. El análisis de metadatos confirmó las siguientes cuentas activas:
Twitter/X: Cuenta encontrada. El usuario interactúa frecuentemente con temas relacionados con [redacted]. El geoetiquetado estaba deshabilitado, pero el análisis de zona horaria lo ubica en UTC-05:00.
Instagram: Perfil privado detectado. Sin embargo, una referencia cruzada con una cuenta pública de Facebook reveló una conexión a través de un contacto mutuo llamado [redacted] [redacted].
LinkedIn: Perfil público encontrado. El historial laboral en [redacted] Corp es visible para quienes no tienen conexiones. Riesgo: Esto permite posibles ataques de ingeniería social contra empleadores actuales.
3.2. Análisis de geolocalización
Estado: [CONFIRMADO]
Una imagen subida a una cuenta secundaria de Flickr (alias: [redacted]_Pix) contenía metadatos EXIF que no fueron eliminados.
Coordenadas extraídas: 34.[redacted]° N, 118.[redacted]° O
Dirección física correlacionada: Calle [redacted] [redacted], Apto. 4B, [redacted], CA.
Acción: Esto confirma la residencia del sujeto con un 98 % de precisión.
3.3. Fuga de datos y violación de credenciales
Estado: [VULNERABILIDAD CRÍTICA]
Un análisis exhaustivo de las bases de datos filtradas reveló que el correo electrónico j[redacted]@gmail.com aparece en cuatro filtraciones de datos conocidas.
Origen de la filtración: Adobe (2013) y LinkedIn (2016).

Hash de contraseña identificado: 7c4a8d09ca3762af[redacted]
Contraseña en texto plano: P[redacted]123 (descifrada)
Análisis: El sujeto reutiliza este patrón de contraseña en foros no críticos.
3.4. Actividad en la Dark Web
Estado: [RASTREO ENCONTRADO]
Usando rastreadores de la red Tor, se encontró una mención del correo electrónico secundario del sujeto, [redacted]@protonmail.com, en un archivo de volcado de un foro de hackers (archivo de RaidForums).
Contenido: El correo electrónico figura en una "Lista Combinada" para ataques de robo de credenciales. No se encontró evidencia de actividad ilegal activa por parte del sujeto, pero es un objetivo.

4. VALIDACIÓN TÉCNICA (FALSO POSITIVO)
Elemento marcado: Un perfil en "Ashley Madison" con el nombre [redacted].
Verificación: El análisis de la IP y la fecha de registro indican que pertenece a otra persona residente en el Reino Unido.
Resultado: MARCADO COMO FALSO POSITIVO / DESCARTADO.

5. CONCLUSIÓN Y ESTRATEGIA DE MITIGACIÓN
El sujeto presenta una alta puntuación de riesgo digital. Su ubicación física se puede derivar fácilmente de metadatos públicos y sus credenciales circulan en la red oscura.
Recomendaciones inmediatas:
Cambiar inmediatamente las contraseñas asociadas con el patrón P[redacted].
Activar la autenticación de dos factores (2FA) en la cuenta principal de Gmail.
Solicitar la eliminación de los datos de dirección de los motores de búsqueda de personas (agentes de datos).

CERTIFICACIÓN DE AUTENTICIDAD
Este informe se generó utilizando herramientas de inteligencia de código abierto de grado forense. Todos los hallazgos han sido verificados por un analista certificado.
Firma: [redacted]. Red de analistas forenses certificados: [redacted].
(Fin del informe)