ESTUDIO DE CASO 3

Divulgación de Ubicación Basada en Navegador: Simulación Controlada con Enlace de Seeker

Por: Joseph Gonzalez

ZERODAY TECH LABS

Alcance	Simulación controlada usando un teléfono del investigador actuando como dispositivo víctima; fines educativos y analíticos únicamente
Entorno	Kali Linux, Seeker, túnel ngrok, navegador móvil, teléfono Android del investigador y artefactos de URL/IP/ubicación redactados
Evidencia principal	Captura de lanzamiento de Seeker, túnel ngrok, listener de solicitudes, permiso de ubicación en móvil y terminal redactada con campos de dispositivo/ubicación
Vector de ataque principal	Divulgación basada en permisos mediante un enlace público con tema de ubicación que persuade al usuario a aprobar acceso de ubicación del navegador

Uso educativo y analítico únicamente. La URL pública, IP, dispositivo y detalles de ubicación mostrados en las figuras fueron redactados.

Introducción

Los navegadores móviles solicitan permisos sensibles durante actividad web ordinaria, especialmente cuando un sitio afirma que necesita ubicación para personalizar la experiencia. Esto crea una exposición distinta al phishing de credenciales o al sideloading de aplicaciones: el usuario no necesita instalar software ni escribir una contraseña. El riesgo aparece en la solicitud de permiso.

Este estudio de caso examina una simulación controlada con Seeker usando un túnel público temporal y un teléfono del investigador actuando como dispositivo víctima. El objetivo es documentar cómo se veía la página, cómo el navegador presentó la solicitud de ubicación, qué datos aparecieron después de conceder el permiso y por qué esto importa para usuarios individuales fuera del laboratorio.

Metodología

Se realizó una simulación de ciberseguridad en un laboratorio aislado usando Kali Linux, Seeker, un túnel ngrok y un navegador móvil en un teléfono Android del investigador. El alcance se limitó a infraestructura controlada por el investigador, un enlace temporal de prueba e interacción consentida por el propio investigador. No hubo víctimas reales, dispositivos de terceros, cuentas de producción ni rastreo no autorizado.

1. Resumen

Este escenario muestra cómo una página web puede solicitar acceso a la ubicación y registrar detalles de dispositivo y red proporcionados por el navegador una vez que el usuario concede el permiso. La pregunta analítica fue si una página creíble con tema de ubicación, entregada mediante un túnel público temporal, podía producir datos observables de ubicación y dispositivo desde un teléfono que aceptó voluntariamente el aviso del navegador.

2. Análisis de Amenaza: Vector, Técnica y Factor Humano

Vector de ataque usado	Enlace público hacia una página web con tema de ubicación que solicita acceso de ubicación del navegador y registra campos de dispositivo, red y ubicación después de la aprobación.
Técnicas de ingeniería social	Phishing de permisos, pretexto, engaño contextual, señuelo basado en enlace y poca atención al origen del sitio.
Factor humano explotado	Fatiga ante avisos móviles, fijación en la tarea, confianza en el tema de la página, atención a botones grandes de aprobación y menor revisión de dominios temporales o desconocidos.
Relevancia defensiva	Las solicitudes de ubicación deben tratarse como decisiones de seguridad. Los usuarios deben denegar solicitudes desconocidas, verificar el origen del sitio, revisar permisos guardados y revocar acceso de inmediato tras una aprobación sospechosa.

Idea clave para el lector: esto no es un compromiso silencioso del sistema operativo. El navegador sí preguntó. La exposición ocurrió porque la página hizo que la solicitud pareciera lo suficientemente normal para aprobarla.

3. Preparación del Laboratorio y Entrega del Enlace Público

El host de laboratorio se usó para iniciar el entorno de Seeker y seleccionar una plantilla con tema de ubicación. La Figura 1 muestra el entorno de lanzamiento. La Figura 2 muestra el túnel temporal usado para hacer que la página local de prueba fuera alcanzable desde el teléfono. La transición importante es de una página local a un enlace público que un navegador móvil podía abrir.

Figura 1. Entorno de lanzamiento de Seeker en el host de laboratorio, mostrando la etapa de selección de plantilla usada en la simulación controlada.

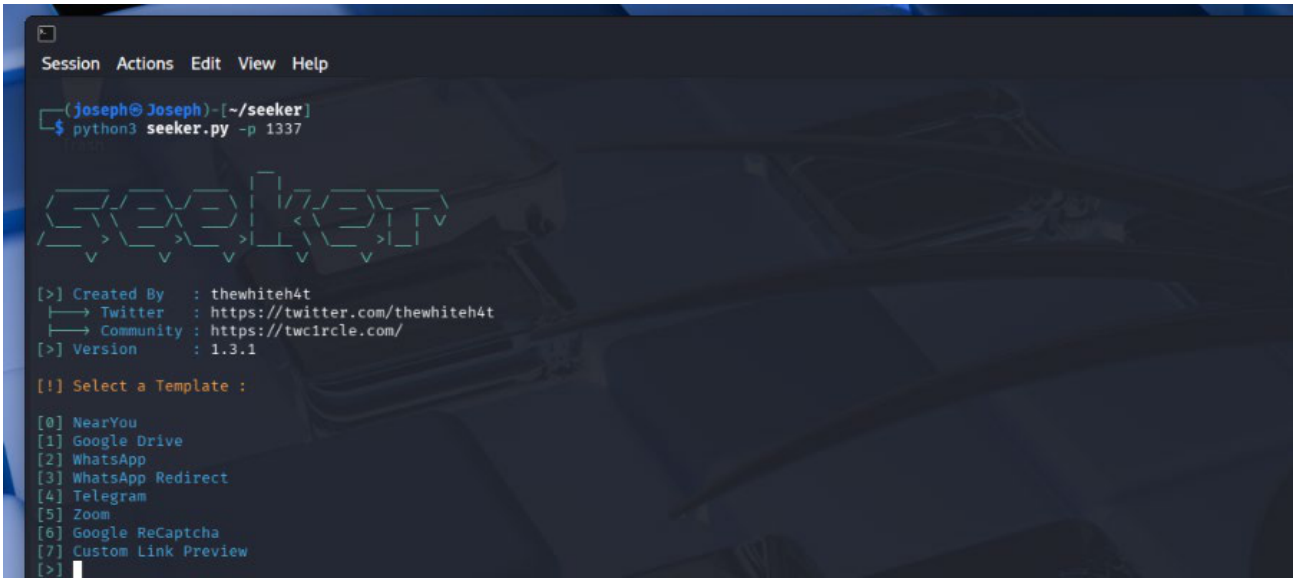

Figura 2. Sesión de túnel temporal usada para exponer la página local de prueba mediante una ruta pública de reenvío, con URL y detalles de cuenta redactados.

4. Solicitud de Permiso y Evidencia Recopilada

Después de preparar el enlace público de prueba, el teléfono abrió la página con tema de ubicación como dispositivo víctima simulado. La Figura 3 muestra actividad de solicitudes en la sesión de túnel tras visitar la página. La Figura 4 muestra el navegador móvil presentando una solicitud de permiso de ubicación para el sitio. Este es el punto de decisión clave: la exposición depende de que el usuario conceda acceso, no de un bypass invisible del modelo de permisos del navegador.

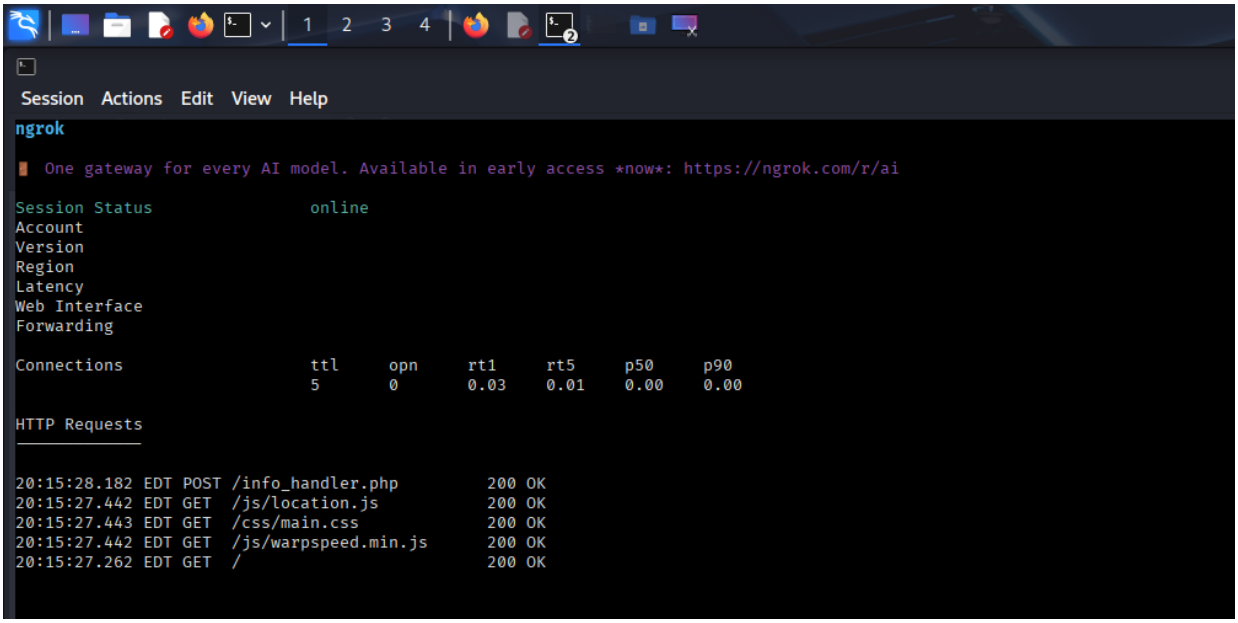

Figura 3. Vista del listener del túnel mostrando solicitudes web desde el teléfono después de abrir el enlace público de prueba, con detalles de reenvío redactados.

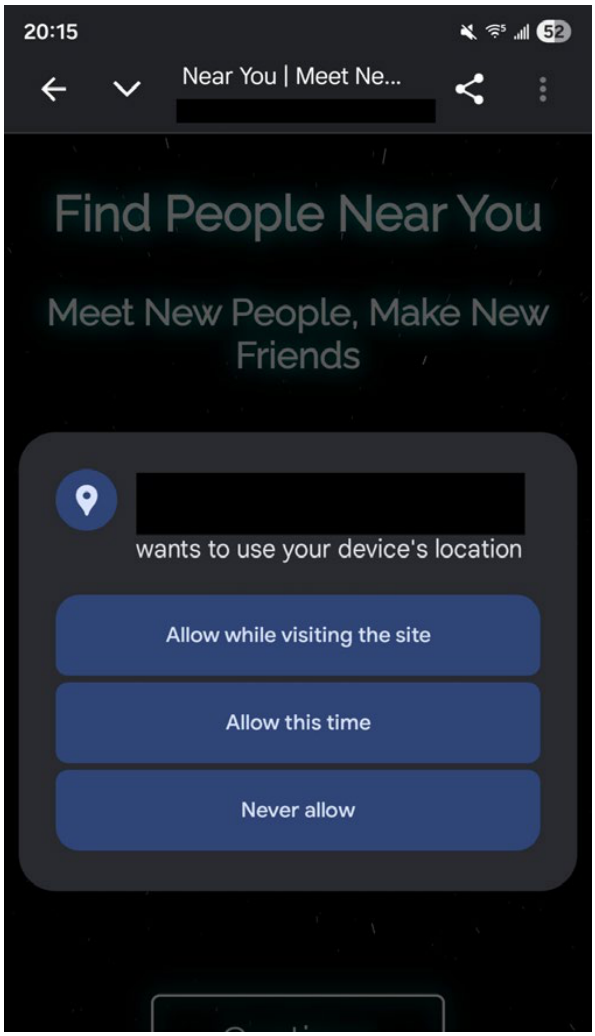

Figura 4. Teléfono del investigador actuando como dispositivo víctima, abriendo el enlace y recibiendo una solicitud de permiso de ubicación con la URL pública redactada.

El siguiente artefacto registra campos de dispositivo, red y ubicación proporcionados por el navegador después de permitir el acceso de ubicación. Las redacciones preservan el valor forense mientras eliminan IP, URL y datos de ubicación privados.

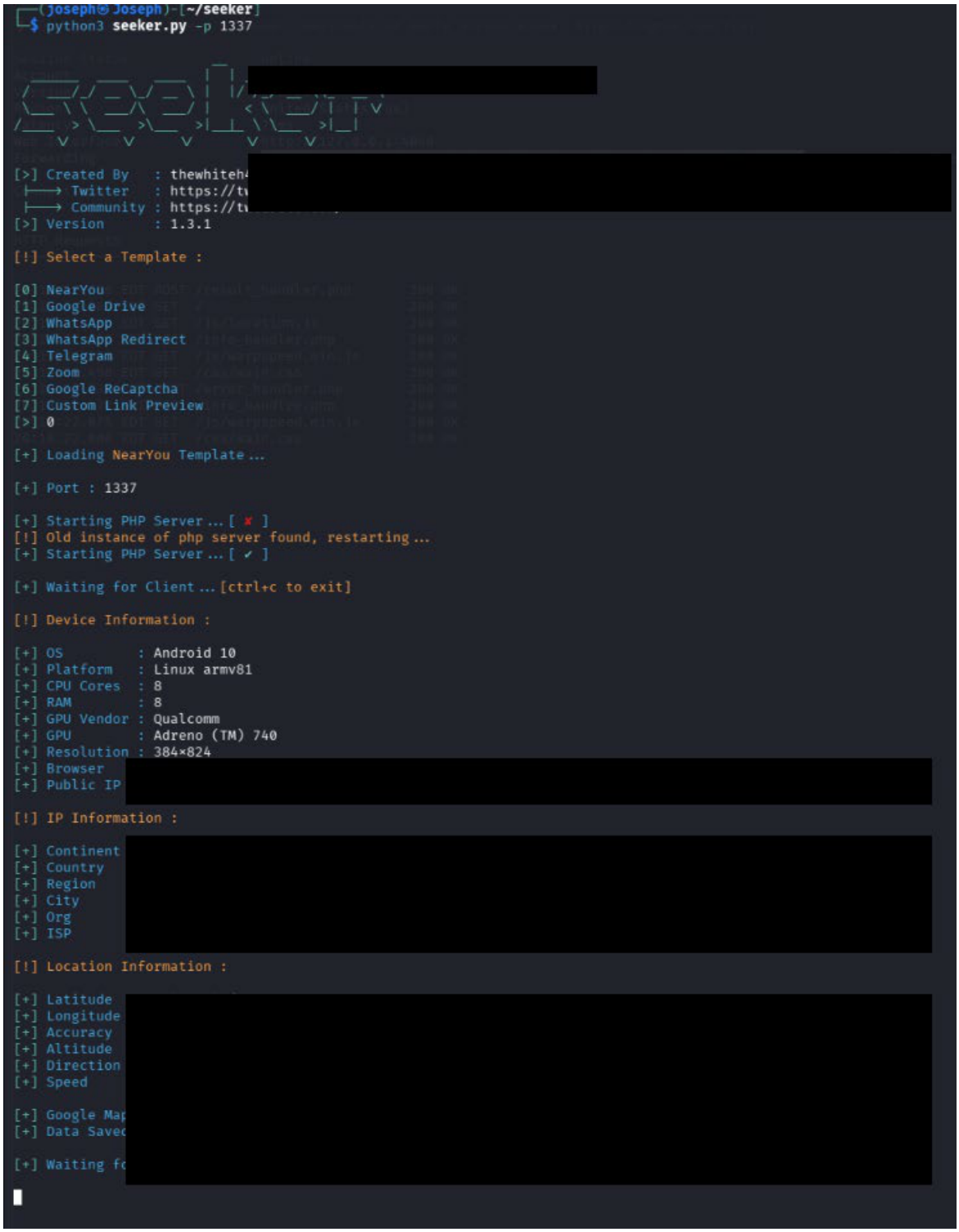

Figura 5. Captura redactada de terminal de Seeker mostrando campos de dispositivo, red y ubicación proporcionados por el navegador después de conceder permiso durante la prueba controlada.

5. Por Qué Ocurrió la Divulgación

La divulgación ocurrió porque el sitio solicitó un permiso que los navegadores están diseñados para soportar, y el usuario lo concedió. El tema de personas cerca hizo que la solicitud pareciera apropiada al contexto: una página que afirma mostrar personas cercanas naturalmente aparenta necesitar ubicación.

El navegador mostró el origen del sitio, pero los usuarios suelen enfocarse en el lenguaje de la tarea y en los botones grandes de aprobación en vez de verificar el dominio temporal. El túnel también fue importante porque convirtió un servicio local en una página pública alcanzable, permitiendo que el teléfono interactuara con contenido alojado en el laboratorio fuera del contexto de localhost.

6. Impacto Real para el Individuo

Para un usuario individual, conceder ubicación a una página engañosa puede exponer más que un solo punto de datos. La ubicación puede revelar dónde una persona vive, trabaja, estudia, adora o pasa tiempo con su familia. Combinada con IP pública, tipo de dispositivo, versión del navegador y proveedor de red, puede apoyar phishing dirigido, hostigamiento, doxxing, stalking o señuelos posteriores muy personales.

El riesgo es serio en teléfonos porque las personas tratan los avisos de permisos móviles como algo rutinario. Un usuario puede aprobar ubicación mientras está distraído y luego olvidar que el sitio preguntó. Incluso sin malware, los datos recopilados pueden ayudar a construir un perfil, programar mensajes futuros o crear un seguimiento más creíble.

7. Mitigación, Fortalecimiento y Prevención

La solución práctica es reducir permisos de ubicación innecesarios y tratar las solicitudes de permisos como decisiones de seguridad. Los usuarios deben denegar solicitudes de ubicación desde enlaces desconocidos, evitar abrir enlaces con tema de ubicación desde mensajes o redes sociales, y revisar la barra de direcciones antes de aprobar acceso.

Si se aprobó una solicitud de ubicación sospechosa, el usuario debe revocar el permiso del sitio, limpiar los datos del sitio, cerrar la pestaña y evitar interactuar nuevamente con la página. La prevención a largo plazo incluye actualizar el navegador y el sistema operativo, preferir aplicaciones oficiales y dominios conocidos, y desactivar ubicación precisa cuando no sea necesaria.

8. Lista de Preparación para el Lector

Antes de aprobar ubicación	Verificar el dominio, preguntar por qué el sitio necesita ubicación exacta y denegar por defecto solicitudes provenientes de enlaces desconocidos.
Después de una aprobación sospechosa	Revocar el permiso del sitio, limpiar los datos del sitio, cerrar la pestaña y evitar usar la página nuevamente.
Hábito a largo plazo	Revisar permisos del navegador regularmente, reducir el uso de ubicación precisa y enseñar a la familia que Permitir esta vez todavía libera datos sensibles.

9. Consideración Ética

Este estudio de caso se realizó estrictamente con fines educativos y analíticos. El sitio, el túnel, la sesión de terminal y la interacción con el teléfono fueron operados por el investigador en un escenario de prueba delimitado. El teléfono en las capturas actuó intencionalmente como dispositivo víctima, y las URLs sensibles, detalles de IP y valores de ubicación fueron redactados antes de preparar el informe.

La lección defensiva es directa: los avisos de permiso del navegador no son pop-ups inofensivos. Son decisiones de confianza. Cuando un sitio pide ubicación, el hábito más seguro es pausar, verificar el origen y denegar la solicitud salvo que la necesidad sea legítima y esperada.