Informe de Reconocimiento: TomTom-Global.com

Índice

---

1. Introducción

TomTom-Global es una extensión de la reconocida empresa TomTom, conocida por sus soluciones de navegación y mapeo. Actualmente, cuenta con un programa activo de Bug Bounty que incentiva a los investigadores de seguridad a identificar y reportar vulnerabilidades dentro del alcance permitido. Este informe realiza un reconocimiento de su infraestructura pública basándose en la información disponible y respetando los límites definidos en su programa.

Scope actual del programa de Bug Bounty: Según las políticas del programa, el alcance incluye dominios y servicios específicos listados en su plataforma oficial. Este informe se limita al dominio principal `tomtom-global.com` y recursos relacionados que se encuentran dentro del scope permitido.

---

2. Objetivos, Metodología y Herramientas Utilizadas

Objetivos

- Recopilar información pública relevante sobre TomTom-Global.
- Identificar posibles puntos de entrada, tecnologías utilizadas e información sensible sin realizar pruebas activas ni intrusivas.

Metodología

1. Recolección de registros DNS, subdominios y configuraciones relacionadas.

2. Identificación de servidores, tecnologías y puertos abiertos utilizando herramientas de escaneo pasivo.
3. Análisis de información pública como registros WHOIS, archivos TXT y redes sociales.
4. Respetar los límites definidos por el programa de Bug Bounty.

Herramientas Utilizadas

- **DNSDumpster**: Para analizar registros DNS y subdominios.
- **Shodan**: Para identificar tecnologías y puertos abiertos.
- **SecurityTrails**: Para investigar configuraciones de DNS y archivos TXT.
- **WHOIS**: Para obtener información sobre el dominio.
- **Google Dorking**: Para buscar información sensible en fuentes públicas.
- **Spiderfoot**: Para obtener un informacion general
-

recon: mi propia herramienta de reconocimiento

3. Resultados Obtenidos

Registros DNS

Servidor NS:

```
dns4.p09.nsone.net
dns1.p09.nsone.net
dns2.p09.nsone.net
dns3.p09.nsone.net
```

Servidor SOA:

```
dns1.p09.nsone.net. hostmaster.nsone.net. 1648037683 7200 3600 24796800 3600
```

Subdominios

Se identificaron posibles subdominios mediante el análisis de registros DNS y herramientas como SecurityTrails: - `www.tomtom-global.com` - `support.tomtom-global.com` - `maps.tomtom-global.com`

Servidores

Rango RIPE:

```
185.5.120.0 - 185.5.123.255
```

Dirección IP:

```
185.5.122.154
```

Tecnologías Utilizadas

Mediante herramientas de reconocimiento pasivo, se identificaron las siguientes tecnologías: - **Web Servers:** Akamai, Microsoft IIS. - **Correo Electrónico:** Sin configuraciones avanzadas identificadas. - **Seguridad:** Uso de SPF con política estricta (`v=spf1 -all`).

Puertos Abiertos

Los siguientes puertos fueron identificados como abiertos mediante análisis pasivo: - Puerto 80 (HTTP) - Puerto 443 (HTTPS)

Correos Electrónicos

No se encontraron direcciones de correo específicas en los registros analizados.

Información Sensible

Archivos TXT públicos encontrados:

```
"xl8tp62s8qwz0bdjv4hhf9y1whq2mvs3"
"identrust_validate=Cgyng0jYAQMdSOKNoU9TNszVUpOZfK1LfEJetCC4r8Ep"
"v=spf1 -all"
```

Estos verifican la propiedad del dominio y reflejan configuraciones de seguridad.

Vulnerabilidades Conocidas

No se encontraron vulnerabilidades activas públicamente conocidas asociadas al dominio dentro del alcance.

---

4. Conclusión

El reconocimiento realizado para TomTom-Global muestra una infraestructura bien configurada con un enfoque en la seguridad, especialmente en el uso de políticas de SPF estrictas. Sin embargo, la exposición de subdominios y configuraciones TXT puede ser utilizada para mapear el alcance de la infraestructura.

Recomendaciones: 1. Revisar periódicamente los registros DNS y limpiar configuraciones innecesarias. 2. Monitorear subdominios expuestos y limitar la información en archivos TXT.

Este informe se limita al reconocimiento pasivo y cumple estrictamente con las directrices del programa de Bug Bounty de TomTom-Global.