Informe de Reconocimiento: TomTomGroup.com

Índice

---

1. Introducción

TomTomGroup es una organización reconocida por sus soluciones tecnológicas avanzadas y su enfoque en la innovación. 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 `tomtomgroup.com` y recursos relacionados que se encuentran dentro del scope permitido.

---

2. Objetivos, Metodología y Herramientas Utilizadas

Objetivos

- Recopilar información pública relevante sobre TomTomGroup.
- 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:

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

Servidor SOA:

```
dns1.p09.nsone.net. hostmaster.nsone.net. 1648553029 7200 3600 24796800 3600
```

Subdominios

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

Servidores

Rango RIPE:

```
96.125.160.0 - 98.96.159.255
```

Dirección IP:

```
98.64.11.144
```

Tecnologías Utilizadas

Mediante herramientas de reconocimiento pasivo, se identificaron las siguientes tecnologías: - **Web Servers:** Akamai, Microsoft IIS. - **Correo Electrónico:**

Microsoft Outlook (protección a través de `tomtomgroup-com.mail.protection.outlook.com`).
- **Seguridad:** Uso de SPF y DMARC para la protección del correo.

Puertos Abiertos

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

Correos Electrónicos

Dirección de contacto DMARC: - `dmarc@smtpeter.com`

Información Sensible

Archivos TXT públicos encontrados:

```
"v=spf1 include:sharepointonline.com include:_spf.axxerion.com ip4:20.76.56.69 ip4:185.5.121
"MS=ms84333051"
"Z1ezHqg+M0d9WR1ADAHlEh6Wue1dlsXxTwYCoL4TFPT6gcjFtqlaKg3U/p5zXnNYh9k1DH4z/RbBXtI5oQ9kYw=="
"identrust_validate=6QXAdFg9nMWd7KyNr8+ivNdlS0L1r+ioDJcmyKM8sUir"
```

Estos verifican la propiedad del dominio en diversas plataformas.

Vulnerabilidades Conocidas

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

---

4. Conclusión

El reconocimiento realizado para TomTomGroup revela una infraestructura robusta con buenas prácticas de seguridad, como el uso de DMARC y SPF. Sin embargo, la exposición de múltiples subdominios y verificaciones en archivos TXT puede ser utilizada por actores maliciosos para mapear el alcance de su 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 TomTomGroup.