Informe de Reconocimiento de Infraestructura

Índice

Introducción

Este informe detalla el reconocimiento realizado sobre la infraestructura pública de la organización "Wickr", dentro de los límites establecidos por su programa de Bug Bounty. El objetivo principal fue identificar elementos clave como dominios, registros DNS, servidores, tecnologías utilizadas y otros datos relevantes.

Alcance del Programa de Bug Bounty

El programa de Bug Bounty de Wickr fomenta la investigación de seguridad responsable, centrada en la evaluación técnica de su software. Este programa respalda a investigadores en el descubrimiento de vulnerabilidades de seguridad, respetando estrictamente las siguientes directrices:

- Limitar las pruebas a vulnerabilidades técnicas dentro del software de Wickr.
- Prohibir la ingeniería social (phishing, vishing, smishing).
- Garantizar que las pruebas no interrumpan servicios, afecten la disponibilidad ni comprometan datos que no sean del investigador.
- Respetar las leyes aplicables y los Términos de Servicio de Wickr.

Estas políticas buscan garantizar un equilibrio entre la seguridad de la plataforma y la protección de la información y los servicios.

Objetivos, Metodología y Herramientas Utilizadas

Objetivos

El objetivo principal del reconocimiento fue recopilar información pública sobre la infraestructura de Wickr, con énfasis en identificar configuraciones, tecnologías y posibles puntos de entrada, siempre respetando el alcance del programa de Bug Bounty.

Metodología

La metodología se basó en técnicas de OSINT (Open Source Intelligence), utilizando herramientas especializadas para la recolección de datos. Se realizaron consultas DNS, identificación de subdominios, análisis de servidores y tecnologías empleadas, sin realizar pruebas invasivas ni penetración.

Herramientas Utilizadas

- **Dig**: Consultas DNS.
- **Whois**: Información sobre dominios y registros.
- **Curl**: Peticiones HTTP/S para análisis de servidores.
- **Katana**: Exploración de subdominios y recursos.
- **Ctfr**: Enumeración de registros DNS.
- **Httpx**: Análisis de configuraciones HTTP/S.
- **Nmap**: Detección de puertos abiertos.

Resultados Obtenidos

Registros en los DNS

Dominio Principal

- **Dominio**: `wickr.com`

Registros AAAA

- `d3sm679bvfdp92.cloudfront.net`

Registros CNAME

- `d3sm679bvfdp92.cloudfront.net`

Servidor HTTP (HEADER_SERVER)

- `AmazonS3`

Direcciones IP Asociadas

- `18.154.48.61`
- `18.154.48.7`
- `18.154.48.3`
- `18.154.48.5`

Registros MX

- `d3sm679bvfdp92.cloudfront.net`

Servidores de Nombres (NS)

- d3sm679bvfdp92.cloudfront.net
- ns-2046.awsdns-63.co.uk
- ns-966.awsdns-56.net
- ns-1032.awsdns-01.org
- ns-93.awsdns-11.com

Rangos de IP

- 14.102.240.0 - 23.19.47.255

Servidores Autoritativos (SOA)

- **Servidor**: d3sm679bvfdp92.cloudfront.net
- **Información adicional**: ns-2046.awsdns-63.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

Registros SRV

- d3sm679bvfdp92.cloudfront.net

Subdominios

- d3sm679bvfdp92.cloudfront.net

Servidores

- **Servidor Principal**: Amazon Web Services (AWS)

Tecnologías Utilizadas

- **Servicios Cloud**: Amazon S3, Amazon CloudFront

Puertos Abiertos

- **IP**: 18.154.48.61
  Puertos: 443 (HTTPS), 80 (HTTP)
- **IP**: 18.154.48.7
  Puertos: 443 (HTTPS), 80 (HTTP)
- **IP**: 18.154.48.3
  Puertos: 443 (HTTPS), 80 (HTTP)
- **IP**: 18.154.48.5
  Puertos: 443 (HTTPS), 80 (HTTP)

Correos Electrónicos

- aws-pr@amazon.com
- wickr-sales@amazon.com

Información en Redes Sociales

- **Instagram**: wickr_app
- **Facebook**: mywickr
- **YouTube**: WickrInc
- **X**: myWickr
- **LinkedIn**: Wickr
- **Medium**: Wickr

Conclusión

El análisis realizado demuestra que la infraestructura de Wickr depende principalmente de los servicios proporcionados por Amazon Web Services (AWS), como Amazon S3 y CloudFront. Los registros DNS y los rangos de IP confirman una configuración distribuida y robusta. Además, no se identificaron vulnerabilidades conocidas ni información sensible durante el reconocimiento.

Este informe cumple con los lineamientos del programa de Bug Bounty, proporcionando un panorama detallado de la configuración pública de Wickr sin comprometer su seguridad ni exceder los límites establecidos.