Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

INCIDENTE EN LA RED GLOBAL: PREFIJO DE CLOUDFLARE “SECUESTRADO” TEMPORALMENTE POR TATA COMMUNICATIONS

15/ 07 / 2025

CONTENIDO

INTRODUCCIÓN 3
RESUMEN 5
NOTICIA COMPLETA 6
CONTACTOS DE SOPORTE 7

INTRODUCCIÓN

El día de ayer 14 de julio de 2025 se dio a conocer que la empresa india TATA Communications anunció incorrectamente un bloque de direcciones IP pertenecientes a Cloudflare, esto incluye su popular servicio DNS 1.1.1.1 .

INCIDENTE EN LA RED GLOBAL: PREFIJO DE CLOUDFLARE “SECUESTRADO” TEMPORALMENTE POR TATA COMMUNICATIONS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_07_15_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	15/07/2025
Es día cero (0 day):	No

RESUMEN

El día de ayer 14 de julio de 2025 se dio a conocer que la empresa india TATA Communications anunció incorrectamente un bloque de direcciones IP pertenecientes a Cloudflare, esto incluye su popular servicio DNS 1.1.1.1 .

¿Por qué secuestro?

El incidente en cuestión tiene que ver con el protocolo llamado BGP (Border Gateway Protocol) Si lo quisiéramos explicar de forma sencilla este protocolo se encarga de ser el mapa de carreteras de internet, esto permite que distintas redes AS (Sistemas Autónomos) puedan decirse mutuamente que bloques de direcciones IP controlan y como llegar a ellas.

Ahora un secuestro de BGP sucede cuando una red anuncia erróneamente que es la dueña de un bloque de direcciones IP que, en realidad pertenecen a otra entidad. Si lo queremos simplificar es como si un supuesto dueño de una carreta principal anunciase que es de él, cuando no es así, esto podría desviar a las personas hacia un camino diferente o generar un callejón sin salida.

¿Qué sucedió?

Recientemente TATA Communications anunció el prefijo 1.1.1.0/24, siendo este un segmento del rango de direcciones IP que Cloudflare utiliza para servicios cruciales, aquí está incluido el conocido DNS público 1.1.1.1. Este incidente no se tomó como un ataque intencional, generalmente este tipo de errores se suelen dar por una mala configuración en la compleja red de rutas de internet.

Cabe recalcar que el incidente tuvo una corta duración de tiempo y fue rápidamente mitigado.

¿Cuáles pueden ser las consecuencias?

Esto pueden causar un impacto significativo en el servicio, puede llegar a desviar el tráfico legítimo, causando interrupciones en el servicio. Una alta latencia y problemas de conectividad para los usuarios finales.

Aunque esta vez no parece ser con una mala intención un secuestro de BGP puede ser utilizado para realizar ataque de denegación de servicio (DDoS) o dirigir a los usuarios a sitios web falsos.

RECOMENDACIONES

- Diversificación y Redundancia: Las organizaciones con una fuerte dependencia de servicios en línea deberían considerar estrategias de diversificación, utilizando múltiples proveedores para servicios críticos como DNS, CDN (Redes de Distribución de Contenidos) y conectividad a Internet.

- Adoptar Estándares de Seguridad BGP (RPKI y MANRS): Es fundamental que los operadores de red adopten e implementen activamente estándares como RPKI (Resource Public Key Infrastructure) para validar la autenticidad de los anuncios de rutas. Iniciativas como MANRS (Mutually Agreed Norms for Routing Security) también son cruciales para mejorar la seguridad del enrutamiento global a través de la colaboración y las mejores prácticas.

- Monitoreo Activo: Implementar sistemas de monitoreo avanzados para detectar anomalías en el enrutamiento y el tráfico de red es vital para una respuesta rápida ante cualquier incidente.

NOTICIA COMPLETA

https://devel.group/blog/incidente-en-la-red-global-prefijo-de-cloudflare-secuestrado-temporalmente-por-tata-communications/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group