Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CloudFlare sufre interrupción en sus servicios.

21/junio/2022

Contenido

Introducción

Por medio del presente boletín, queremos notificarle sobre las fallas en los servicios de CloudFlare.Han sufrido un apagón en uno de sus datacenter lo cual genero el problema.

CLOUDFLARE

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

ID de alerta:	DSOC-CERT_2022_06_21_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**WHITE**
Fecha de publicación:	06/21/2022
Es día cero (0 day):	NO

RESUMEN

Cloudflare sufrió una interrupción que afectó el tráfico en 19 de nuestros centros de datos. Desafortunadamente, estas 19 ubicaciones manejan una proporción significativa de tráfico global. Esta interrupción fue causada por un cambio que formaba parte de un proyecto de larga duración para aumentar la resiliencia en sus ubicaciones más concurridas. Un cambio en la configuración de la red en esas ubicaciones provocó una interrupción que comenzó a las 06:27 UTC. A las 06:58 UTC, el primer centro de datos volvió a estar en línea y, a las 07:42 UTC, todos los centros de datos estaban en línea y funcionando correctamente.

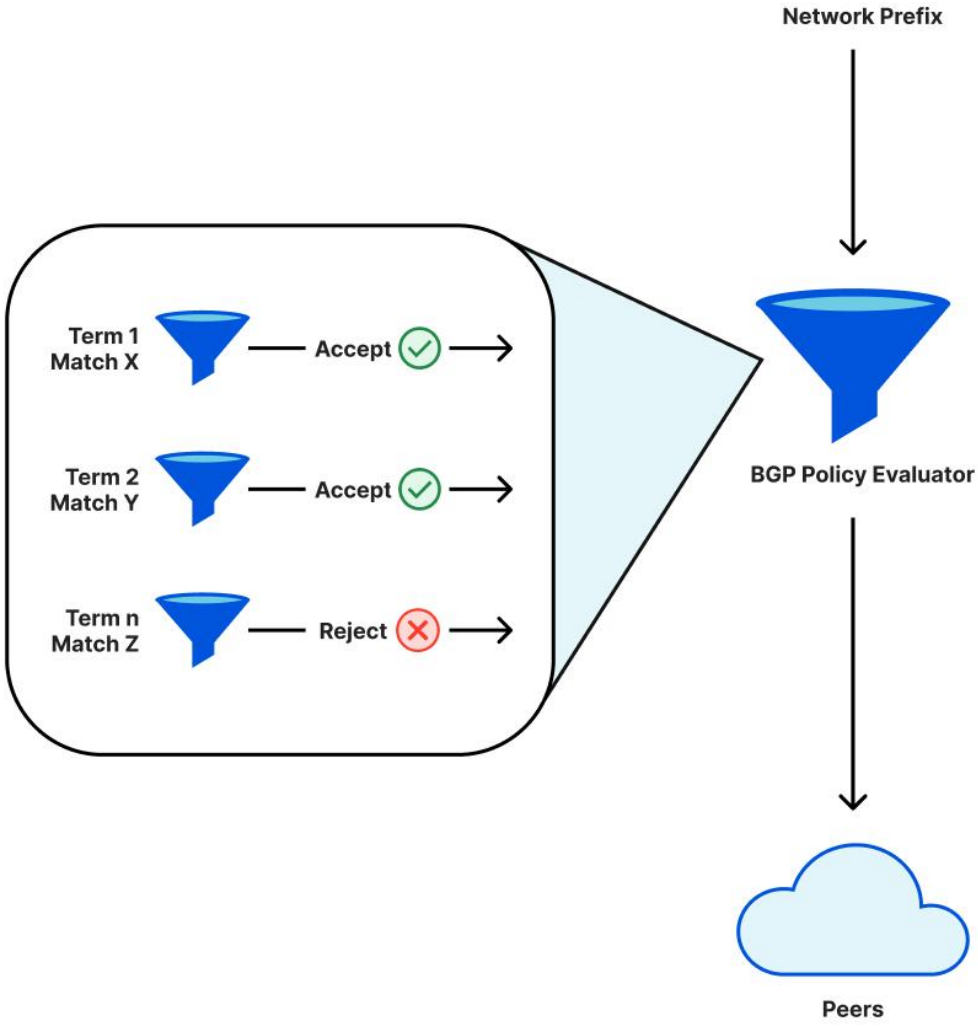
Según la ubicación de los usuarios en el mundo, es posible que no hayan podido acceder a sitios web y servicios que dependen de Cloudflare. En otros lugares, Cloudflare siguió funcionando con normalidad.

Cloudflare asegura que fue su error y no el resultado de un ataque o actividad maliciosa.

Cronología e impacto del incidente

Para ser accesible en Internet, las redes como Cloudflare utilizan un protocolo llamado BGP . Como parte de este protocolo, los operadores definen políticas que deciden qué prefijos (una colección de direcciones IP adyacentes) se anuncian a los pares (las otras redes a las que se conectan) o se aceptan de los pares.

Estas políticas tienen componentes individuales, que se evalúan secuencialmente. El resultado final es que cualquier prefijo dado se anunciará o no se anunciará. Un cambio en la política puede significar que un prefijo anunciado previamente ya no se anuncia, lo que se conoce como "retirado", y esas direcciones IP ya no estarán accesibles en Internet.



Al implementar un cambio en sus políticas de publicidad de prefijos, un reordenamiento de los términos hizo que eliminaran un subconjunto crítico de prefijos.
Debido a este retiro, los ingenieros de Cloudflare experimentaron una dificultad adicional para llegar a las ubicaciones afectadas y revertir el cambio problemático.

03:56 UTC : Se implementa el cambio en nuestra primera ubicación. Ninguna de nuestras ubicaciones se ve afectada por el cambio, ya que utilizan nuestra arquitectura anterior.

06:17 : El cambio se implementa en sus ubicaciones más concurridas, pero no en las ubicaciones con la arquitectura MCP.

06:27 : La implementación llegó a las ubicaciones habilitadas para MCP y el cambio se implementa en sus columnas vertebrales. Fue entonces cuando comenzó el incidente , ya que rápidamente desconectó estas 19 ubicaciones.

06:32 : Incidente interno de Cloudflare declarado.

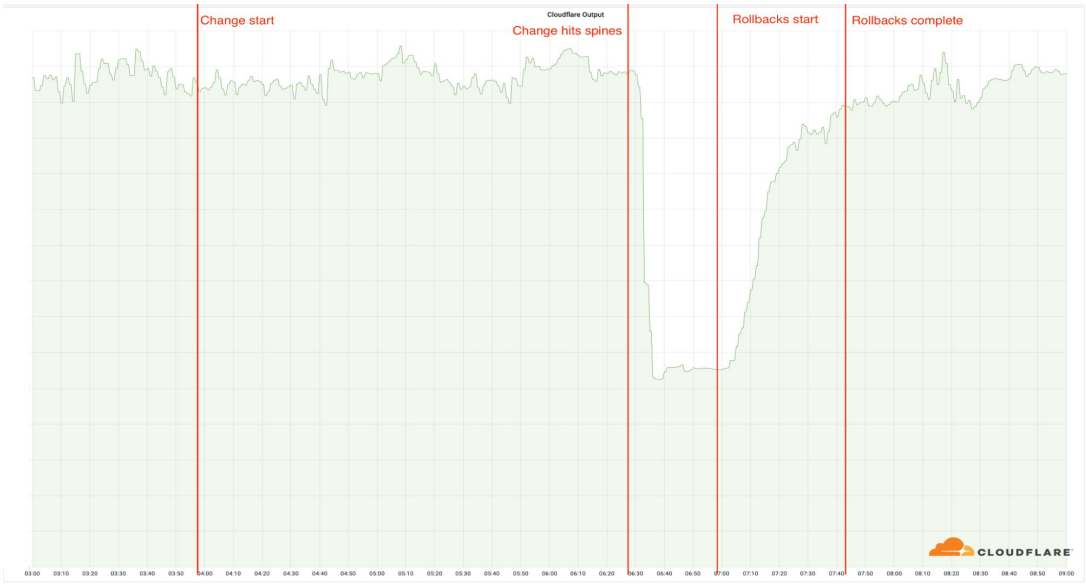
06:51 : Primer cambio realizado en un Enrutador para verificar la causa raíz.

06:58 : Causa raíz encontrada y entendida. Se empieza a trabajar para revertir el cambio problemático.

07:42: La última de las reversiones ha sido completada. Esto se retrasó porque los ingenieros de red revisaron los cambios de los demás, revirtiendo las reversiones anteriores, lo que provocó que el problema volviera a aparecer esporádicamente.

09:00 : Incidente cerrado.

La criticidad de estos centros de datos se puede ver claramente en el volumen de solicitudes HTTP exitosas que Cloudflare maneja a nivel mundial:



RECOMENDACIONES

1. Si usted utiliza los servicios de CloudFlare, valide todo se encuentre funcionando de forma adecuada, de lo contrario reportarlo a soporte.

2. Solicitar a su SOC monitoreo sobre sus plataformas, para validar si alguna se vio afectada y el tiempo de baja que la misma presento.

Noticia Completa

https://blog.cloudflare.com/cloudflare-outage-on-june-21-2022/

https://www.xataka.com/servicios/cloudflare-esta-fallando-ella-medio-internet-se-ha-venido-abajo

CONTACTOS DE SOPORTE

Correo electrónico: cert@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://www.devel.group/reporta-un-incidente