Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ATAQUES DE DENEGACION DE SERVICIO A INSTITUCIONES DE GOBIERNO

14 / Abril / 2023

CONTENIDO

INTRODUCCIÓN 3

ATAQUES DE DENEGACION DE SERVICIOS 4

RESUMEN 4

OTRAS ENTIDADES GUBERNAMENTALES 5

RECOMENDACIÓN 6

NOTICIA COMPLETA 6

CONTACTOS DE SOPORTE 7

INTRODUCCIÓN

Instituciones Gubernamentales sufren campaña de Denegación de Servicios (DoS). Se reportan actualmente dos instituciones afectadas siendo estas el Organismo Judicial, Tribunal Supremo Electoral (TSE) así como la Municipalidad de Mixco.

ATAQUES DE DENEGACION DE SERVICIOS

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

ID de alerta:	DSOC-CERT_2023_04_14_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	14/04/2023
Es día cero (0 day):	No

RESUMEN

Desde el 12 de abril del año en curso Instituciones gubernamentales Guatemaltecas reportan ser víctimas por parte de campaña de Denegación de Servicios. Los ataques se registran desde el pasado miércoles 12 de abril, siendo la primera entidad en ser atacada, el Organismo Judicial. El ataque de Denegación de Servicios DoS utilizan el protocolo HTTP (80/TCP), TCP/IP lo que resulta en una limitante en los servicios que la página proporciona.

Según comunicado oficial, El ataque iniciaría a la 10:00 horas hacia la página web del Organismo Judicial, provocando una interrupción temporal a los servicios en línea que esta institución presta siendo controlado a las 21:00 horas del mismo día.

OTRAS ENTIDADES GUBERNAMENTALES

Esta campaña apunta a atacar varias instituciones gubernamentales y ya se tiene confirmación de ataques hacia la página web Tribunal Supremo Electoral (TSE), así como la Municipalidad de Mixco quienes aún no han hecho comunicado oficial del acontecimiento. Esta campaña de Denegación de Servicios (DoS) ha sido atribuida a AnonymousGT quienes alegan una supuesta represalia hacia instrucciones que estos consideran corruptas y quienes, a través de su cuenta en Twitter, han adjuntado pruebas del ataque a las instituciones antes mencionadas.

RECOMENDACIÓN

- Asegurarse de tener buena seguridad de red y que este implementada correctamente.
- Asegurar redundancia a nivel de servicios.
- Mantener monitoreo proactivo sobre los servicios críticos públicos.
- Utilizar una estrategia de protección basada en nube.
- Tener un plan de respuesta con playbook definido y certificado para estar listo ante ataques de este tipo.

NOTICIA COMPLETA

https://devel.group/blog/ataques-de-denegacion-de-servicio-a-instituciones-de-gobierno/

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