Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ANONYMOUS ATACA SITIOS PÚBLICOS GUATEMALTECOS

06/10/2023

CONTENIDO

INTRODUCCIÓN

Por quinto día consecutivo el pueblo de Guatemala protesta y bloquean 58 puntos en carreteras de 19 de los 22 departamentos del país, en reclamo de la renuncia de la fiscal general, Consuelo Porras, a quién señalan de socavar la democracia en el país y de intentar evitar que el presidente electo, el progresista Bernardo Arévalo, tome posesión de su cargo en enero próximo.

ANONYMOUS ATACA SITIOS PÚBLICOS GUATEMALTECOS

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

ID de alerta:	DSOC-CERT_2023_10_06_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	06/10/2023
Es día cero (0 day):	No

RESUMEN

Por quinto día consecutivo el pueblo de Guatemala protesta y bloquean 58 puntos en carreteras de 19 de los 22 departamentos del país, en reclamo de la renuncia de la fiscal general, Consuelo Porras, a quién señalan de socavar la democracia en el país y de intentar evitar que el presidente electo, el progresista Bernardo Arévalo, tome posesión de su cargo en enero próximo.

El lunes eran 14 los puntos bloqueados, pero las manifestaciones y bloqueos se cuadruplicaron el viernes después de que la Corte de Constitucionalidad decidiera el jueves respaldar la actuación judicial al reconocer al juez penal competencia en materia electoral para suspender la personería jurídica del partido político Movimiento Semilla, el que llevó a ganar la presidencia a Arévalo.

Ante la movilización masiva, los representantes indígenas solicitaron a la Comisión Interamericana de DDHH medidas cautelares a favor de quienes protestan pacíficamente frente a algunos intentos de infiltrados en las marchas, que fueron denunciados, y frente a la posibilidad de que las manifestaciones fuesen reprimidas por la fuerza pública, algo que también ya fue descartado por el gobierno.

Las organizaciones indígenas y campesinas han mostrado su molestia y alcance al paralizar las rutas del país.

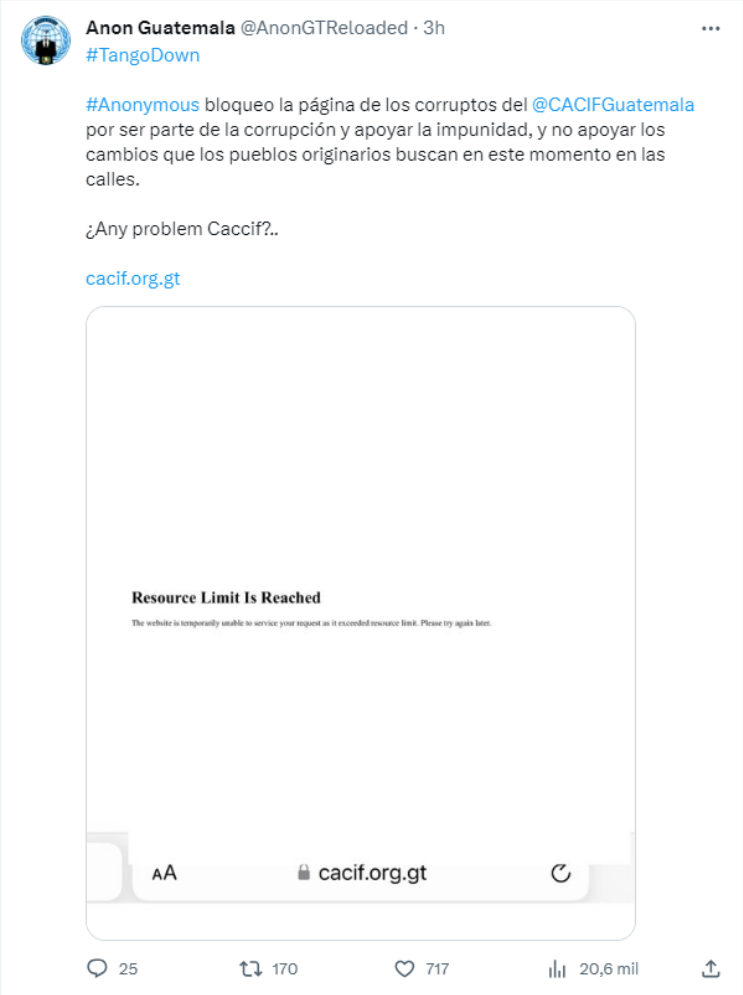
Además de la renuncia de Porras, exigen la de los fiscales Rafael Curruchiche y Cinthia Monterroso —quienes dirigieron la investigación contra Semilla—, así como la renuncia del juez Fredy Orellana que ordenó allanamientos y aprehensiones por la presunta inscripción del partido político con firmas falsas.

A este movimiento se ha sumado Anonymous Guatemala, los cuales a través de su página de X (Antes Twitter), han expresado su apoyo ante las movilizaciones, realizando ataques de Denegación de Servicio (DDoS), ha diferentes páginas de gobierno y de empresas que no apoyan la manifestación, desde el 4 de octubre hasta el día de hoy.

Algunas de las páginas afectadas han sido:

- https://dgac.gob.gt

- https://mingob.gob.gt
- https://mcdonalds.com.gt/
- https://cacif.org.gt/
- https://progreso.com/
- https://cafebarista.com.gt/



Algunas páginas siguen fuera de servicio, según Anonymous GT los ataques seguirán.

RECOMENDACIONES

Para tratar de prevenir un ataque de DDoS, se recomienda:

- **Firewalls y sistemas de filtrado de tráfico**: Implementa firewalls y sistemas de filtrado de tráfico en tu red para bloquear el tráfico no deseado antes de que llegue a tu servidor. Esto puede ayudar a mitigar algunos tipos de ataques.
- **Monitoreo constante**: Establece sistemas de monitoreo para detectar patrones de tráfico inusuales o indicadores de un ataque DDoS en curso. La detección temprana puede ayudar a tomar medidas más rápidamente.
- **Balanceo de carga**: Utiliza balanceadores de carga para distribuir el tráfico entre múltiples servidores. Esto puede ayudar a distribuir la carga de un ataque DDoS de manera más efectiva.
- **Actualizaciones de seguridad**: Mantén tus sistemas operativos y aplicaciones actualizados con los últimos parches de seguridad para proteger contra vulnerabilidades conocidas que los atacantes podrían explotar.
- **Plan de respuesta a incidentes**: Desarrolla un plan de respuesta a incidentes que detalle los pasos a seguir en caso de un ataque DDoS. Esto incluye la notificación de las partes interesadas y la coordinación con proveedores de servicios de mitigación de DDoS.
- **Implementa un Web Application Firewall (WAF)**: Utiliza un WAF para proteger tus aplicaciones web contra una variedad de amenazas, incluyendo ataques DDoS. Configura el WAF para filtrar y bloquear automáticamente el tráfico malicioso y para proteger contra ataques de capa de aplicación que puedan ser utilizados en un ataque DDoS. El WAF puede proporcionar una capa adicional de seguridad y mitigación de ataques.

NOTICIA COMPLETA

https://devel.group/blog/anonymous-gt-ataca-paginas-en-apoyo-al-pueblo-que-realiza-protestas-politicas/

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