Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CONTINÚAN LOS ATAQUES HACIA SITIOS PÚBLICOS Y GUBERNAMENTALES GUATEMALTECOS

11/10/2023

CONTENIDO

INTRODUCCIÓN

La tensión se elevó en el décimo día de protestas en Guatemala por la situación que se vive actualmente.

CONTINÚAN LOS ATAQUES HACIA SITIOS PÚBLICOS Y GUBERNAMENTALES GUATEMALTECOS

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

ID de alerta:	DSOC-CERT_2023_10_11_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	11/10/2023
Es día cero (0 day):	No

RESUMEN

La tensión se elevó en el décimo día de protestas en Guatemala por la situación que se vive actualmente

Como lo habíamos comentado la semana pasada a este movimiento se ha sumado Anonymous Guatemala, los cuales a través de su página de X (Antes Twitter), realizando ataques de Denegación de Servicio (DDoS), el día de hoy Anonymous Guatemala ha publicado en su cuenta de X (Antes Twitter), el inicio de una cyber guerra, este 14 de octubre, en conjunto con diferentes grupos internacionales de hacktivistas

Anon Guatemala @AnonGTReloaded · 8h

Este 14 de Octubre #Anonymous atacara el @GuatemalaGob , pero esta vez no venimos solos, Gobierno y señora presidenta @DrGiammattei , si acepto nuestros cyber ataques, ahora tendrá que aceptar una cyber guerra en el cyber espacio de Guatemala, todo es target.

#ExpectUs

Prensa Comunitaria Km169 y 6 más

62 393 1.312 65 mil

YourAnonTl3x @YourAnonTl3x · 8h

🚨Government of Guatemala website has been Downed by @YourAnonTl3x

⚡guatemala.gob.gt | Government of Guatemala website
🎯Check-host: check-host.net/check-report/1...

Countdown 4 days to the nightmare👍. Expect Us.
#Anonymous #YourAnonTl3x #OpGuatemalan #FreeGuatemalan

10 26 103 24,3 mil

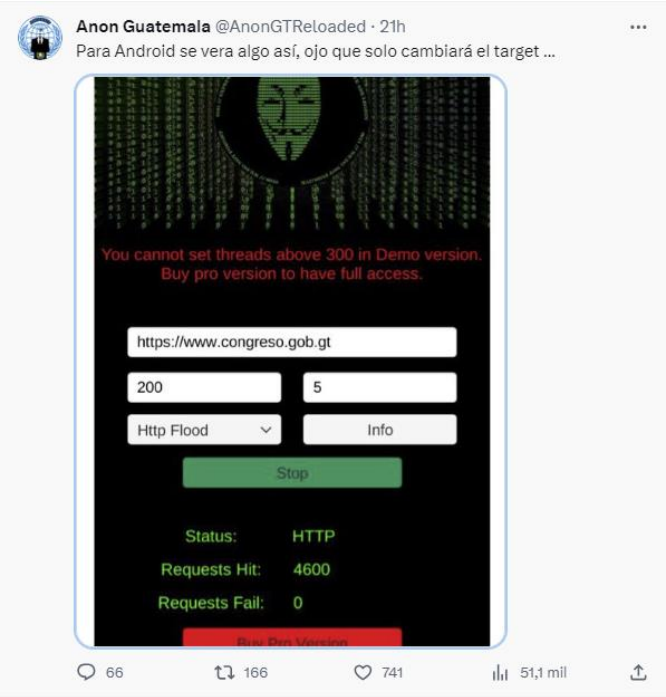
YourAnonTl3x @YourAnonTl3x · 8h

We are Anonymous. Expect Us:
@YourAnonTl3x
@YourAnonRiots
@Parrattarna
@AnonGTReloaded
@milwordgt
@YourAnonArabia
and other human rights activists....

Entre los sitios reportados como dado de baja entre esta semana, y la semana pasada se encuentra:

- https://dgac.gob.gt
- https://mingob.gob.gt
- https://mcdonalds.com.gt/
- https://cacif.org.gt/
- https://progreso.com/
- https://cafebarista.com.gt/
- https://portal.sat.gob.gt/portal/
- oj.gob.gt
- banguat.gob.gt
- https://mindef.mil.gt/index.html
- muniguate.com
- munimixco.gob.gt
- https://mingob.gob.gt
- https://ccg.com.gt
- scspr.gob.gt
- https://cang.org.gt
- mp.gob.gt
- https://cig.industriaguate.com
- https://sgp.gob.gt/web/

Y como principal la página de https://guatemala.gob.gt, la cual presento una caída momentánea que se acredito el grupo YourAnonTl3x. El grupo de Anonymous GT ha enviado por Inbox el link para descargar una aplicación para realizar pruebas de estrés hacia la paginas que los usuarios deseen, esto para utilizar los teléfonos de las personas como Bots y que pueda ayudar a realizar los ataques de DDoS hacia las páginas del gobierno.



El SOC Devel, se encuentra 24/7 al pendiente de lo que está ocurriendo, con los ataques hacia las páginas, con un constate monitoreo de las mismas.

RECOMENDACIONES

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

- 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.
- Limitar el acceso de IPs publicas hacia sus servicios publicados en la web.
- 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.
- Monitoreo constante.

NOTICIA COMPLETA

https://devel.group/blog/continuan-los-ataques-hacia-sitios-publicos-y-gubernamentales-guatemaltecos/

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