

CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

CAMPAÑA CONTRA ENTIDADES DE GOBIERNO

24/ Julio/2023

CONTENIDO

INTRODUCCIÓN	3
ANONYMOUS GUATEMALA.....	4
CONTEXTO.....	5
INTITUCIONES BAJO ATAQUE.....	7
RECOMENDACIONES	13
CONTACTOS DE SOPORTE	14

INTRODUCCIÓN

Recientemente el grupo “Hacktivista” AnonymousGT han iniciado una campaña de denegación de servicios (DoS) a múltiples Instituciones Gubernamentales. Entre las instituciones objetivo de dicha campaña se pueden resaltar: El Ministerio de Trabajo, El Ministerio de Defensa, El Ministerio de Relaciones Exteriores y organizaciones como el CACIF y otras empresas guatemaltecas.

La campaña llevada a cabo el grupo de actores maliciosos, busca ser una protesta contra el gobierno respaldándose en acusaciones contra dichas entidades, de ser coaptadas por personal corrupto o en su defecto, apoyar acciones fraudulentas conducidas por el gobierno. Ninguna de las organizaciones antes mencionadas ha emitido algún comunicado oficial al respecto.

ANONYMOUS GUATEMALA

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

ID de alerta:	DSOC-CERT_2023_07_24_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	CLEAR
Fecha de publicación:	24/07/2023
Es día cero (0 day):	No

CONTEXTO

El día de hoy 24 de Julio de 2023, el grupo de actores AnonymousGT ha iniciado una campaña de denegación de servicios DoS, hacia entidades de gobierno, alegando ser una campaña que apunta a aquellas entidades que se han dejado corromper y que, según estos, han sido coaptadas por la corrupción.

Los ataques se registran desde las 7:00 de la mañana de este lunes 24, según lo observado en la cuenta oficial de Twitter de @NonGTReloades (AnomynousGT) siendo la primera entidad en ser atacada, no una de gobierno si no, el sitio web de Diario de Centroamérica. 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.



Imagen 1. Cuenta de Twitter de AnonymousGt.



Imagen 2. Sitio web de Diario de Centroamérica con complicaciones para acceder.

The screenshot shows a website availability checker tool. At the top, there's a search bar with the URL 'oticias-guatemala-diario-centro-america/' and buttons for 'Info', 'Ping', 'HTTP', 'TCP port', 'UDP port', and 'DNS'. Below the search bar, a message reads: 'Check website https://dca.gob.gt/noticias-guatemala-diario-centro-america'. A banner for 'aeza.net' is visible. Below the banner, there's a table showing the results of the check from various locations.

Location	Result	Time	Code	IP address
Austria, Vienna	Connection timed out			172.67.209.71
Brazil, Sao Paulo	Connection timed out			104.21.85.189
Bulgaria, Sofia	Connection timed out			172.67.209.71
Czechia, C.Budejovice	Connection timed out			172.67.209.71
Finland, Helsinki	Connection timed out			172.67.209.71
France, Paris	Connection timed out			172.67.209.71
Germany, Frankfurt	OK	23.786 s	200 (OK)	172.67.209.71
Germany, Nuremberg	Connection timed out			104.21.85.189
Hong Kong, Hong Kong	Connection timed out			104.21.85.189
Iceland, Reykjavik	Connection timed out			104.21.85.189

Imagen 3. Indisponibilidad del sitio web.

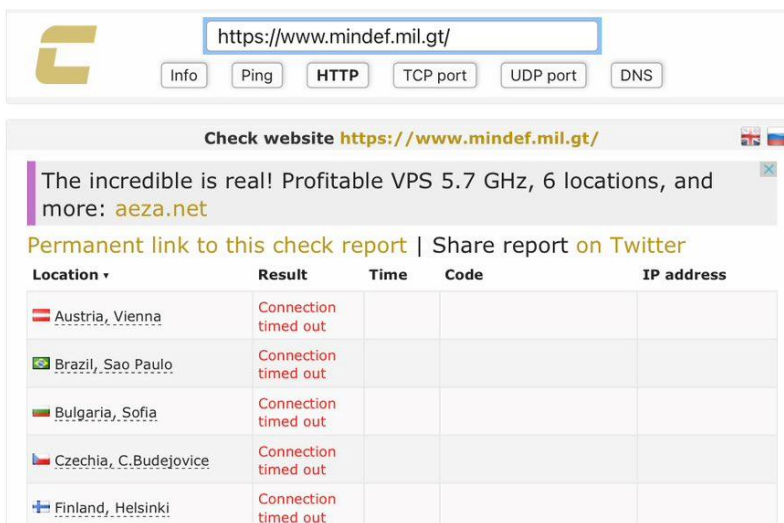
INTITUCIONES BAJO ATAQUE

Esta campaña apunta a atacar varias instituciones gubernamentales y ya se tiene confirmación de ataques hacia varias entidades. Esta campaña de Denegación de Servicios (DoS) ha sido atribuida a AnonymousGT quienes alegan una supuesta represalia hacia instrucciones que estos consideran se han visto envueltas en acciones turbulentas de gobierno. El a través de su cuenta en Twitter, han adjuntado pruebas del ataque a las instituciones antes mencionadas.

Entre las instituciones que se pueden observar como objetivo de esta campaña, se encuentra:

- Página web Tribunal Supremo Electoral (TSE)
- El Ministerio de la Defensa Nacional
- Ministerio de Relaciones Exteriores
- Ministerio de Trabajo
- Ministerio de Ambiente y Recursos Naturales
- Policía Nacional Civil
- Secretaría de Obras Sociales
- La Diaco
- El Comité Coordinador de Asociaciones Agrícolas, Comerciales, Industriales y Financieras (CACIF)
- Cámara de la Industria de Guatemala, entre otras empresas guatemaltecas.


Con cada tweet expuesto por el grupo, se adjunta algún mensaje que busca justificar dichos ataques, entre los mensajes se pueden observar múltiples alusiones a casos de corrupción o ser parte de dicho acto. Mensajes como “apoyo a la corrupción e impunidad”, “apoyo a gobiernos corruptos”, “por estar bajo servicio de las mafias”, entre muchos otras de la misma índole.



The screenshot shows a web application interface for checking website availability. At the top, there is a search bar with the URL `https://www.mindef.mil.gt/` entered. Below the search bar are buttons for 'Info', 'Ping', 'HTTP', 'TCP port', 'UDP port', and 'DNS'. The main section is titled 'Check website `https://www.mindef.mil.gt/`'. Below this, there is a message: 'The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: [aeza.net](#)'. Below the message is a link: 'Permanent link to this check report | Share report on Twitter'. Below the link is a table with the following columns: 'Location', 'Result', 'Time', 'Code', and 'IP address'. The table contains five rows of data, all showing 'Connection timed out' as the result.

Location	Result	Time	Code	IP address
Austria, Vienna	Connection timed out			
Brazil, Sao Paulo	Connection timed out			
Bulgaria, Sofia	Connection timed out			
Czechia, C.Budejovice	Connection timed out			
Finland, Helsinki	Connection timed out			

Imagen 4. disponibilidad sitio web del Ministerio de defensa.



Info Ping **HTTP** TCP port UDP port DNS


Check website <https://alejandrogiammattei.presidencia.gob.gt/>

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: aeza.net

[Permanent link to this check report](#) | [Share report on Twitter](#)

Location ▼	Result	Time	Code	IP address
Austria, Vienna	Connection timed out			104.26.3.138
Brazil, Sao Paulo	Server error	11.226 s	525 (Date: Mon, 24 Jul 2023 13:20:42 GMT)	172.67.69.152
Bulgaria, Sofia	Connection timed out			104.26.2.138
Czechia, C.Budejovice	Connection timed out			104.26.2.138
Finland, Helsinki	Connection timed out			188.114.98.224
France, Paris	Connection timed out			172.67.69.152
Germany, Frankfurt	Connection timed out			104.26.3.138
Germany, Nuremberg	Connection timed out			104.26.3.138

Imagen 5. Disponibilidad sitio web presidencia.



Info Ping **HTTP** TCP port UDP port DNS

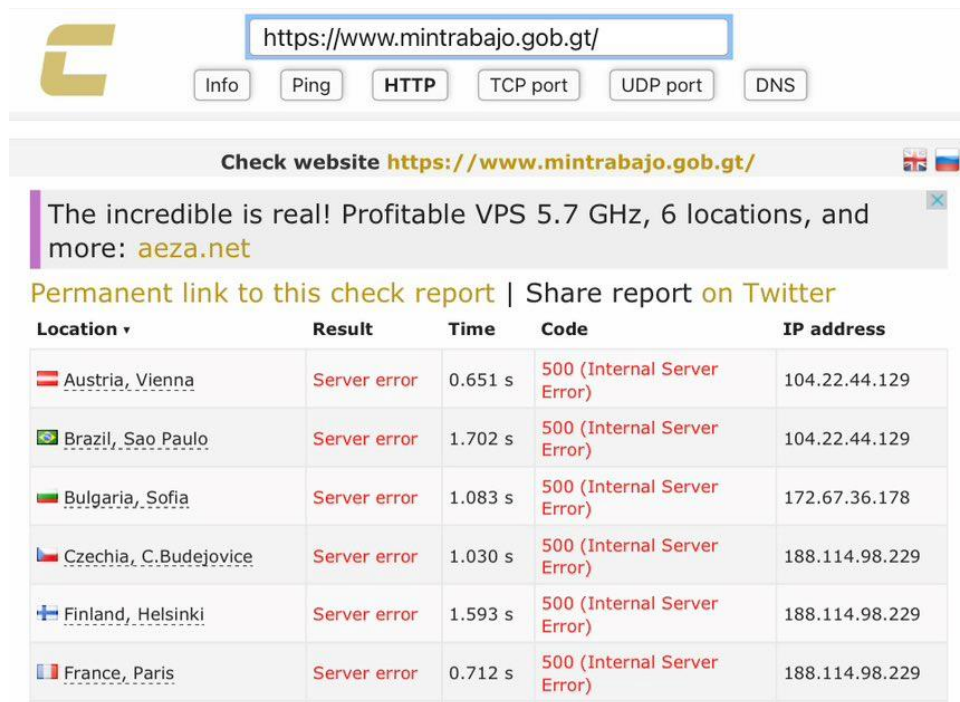
Check website <https://www.minex.gob.gt/>

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: aeza.net

[Permanent link to this check report](#) | [Share report on Twitter](#)

Location ▼	Result	Time	Code	IP address
Austria, Vienna	Server error	0.048 s	403 (Forbidden)	172.67.1.69
Brazil, Sao Paulo	Server error	0.020 s	403 (Forbidden)	104.20.162.52
Bulgaria, Sofia	Server error	0.109 s	403 (Forbidden)	172.67.1.69
Czechia, C.Budejovice	Server error	0.235 s	403 (Forbidden)	104.20.163.52
Finland, Helsinki	Server error	0.054 s	403 (Forbidden)	172.67.1.69
France, Paris	Server error	0.031 s	403 (Forbidden)	172.67.1.69
Germany, Frankfurt	Server error	0.034 s	403 (Forbidden)	172.67.1.69
Germany, Nuremberg	Server error	0.027 s	403 (Forbidden)	104.20.162.52
Hong Kong, Hong Kong	Server error	0.023 s	403 (Forbidden)	104.20.163.52
Iceland, Reykjavik	Server error	0.029 s	403 (Forbidden)	104.20.162.52
Iran, Shiraz	Server error	0.622 s	403 (Forbidden)	104.20.163.52
Iran, Tabriz	Server error	0.311 s	403 (Forbidden)	104.20.162.52

Imagen 6. Disponibilidad sitio web Ministerio de Relaciones Exteriores.



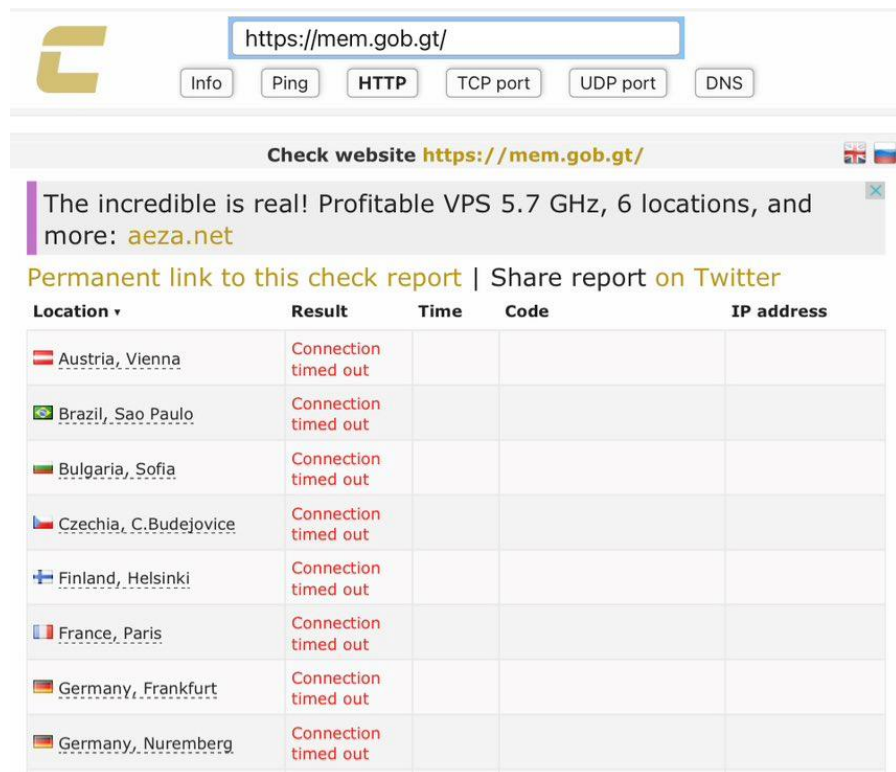
Check website <https://www.mintrabajo.gob.gt/>

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: aeza.net

[Permanent link to this check report](#) | [Share report on Twitter](#)

Location ▼	Result	Time	Code	IP address
Austria, Vienna	Server error	0.651 s	500 (Internal Server Error)	104.22.44.129
Brazil, Sao Paulo	Server error	1.702 s	500 (Internal Server Error)	104.22.44.129
Bulgaria, Sofia	Server error	1.083 s	500 (Internal Server Error)	172.67.36.178
Czechia, C.Budejovice	Server error	1.030 s	500 (Internal Server Error)	188.114.98.229
Finland, Helsinki	Server error	1.593 s	500 (Internal Server Error)	188.114.98.229
France, Paris	Server error	0.712 s	500 (Internal Server Error)	188.114.98.229

Imagen 7. Disponibilidad sitio web del Ministerio de trabajo.



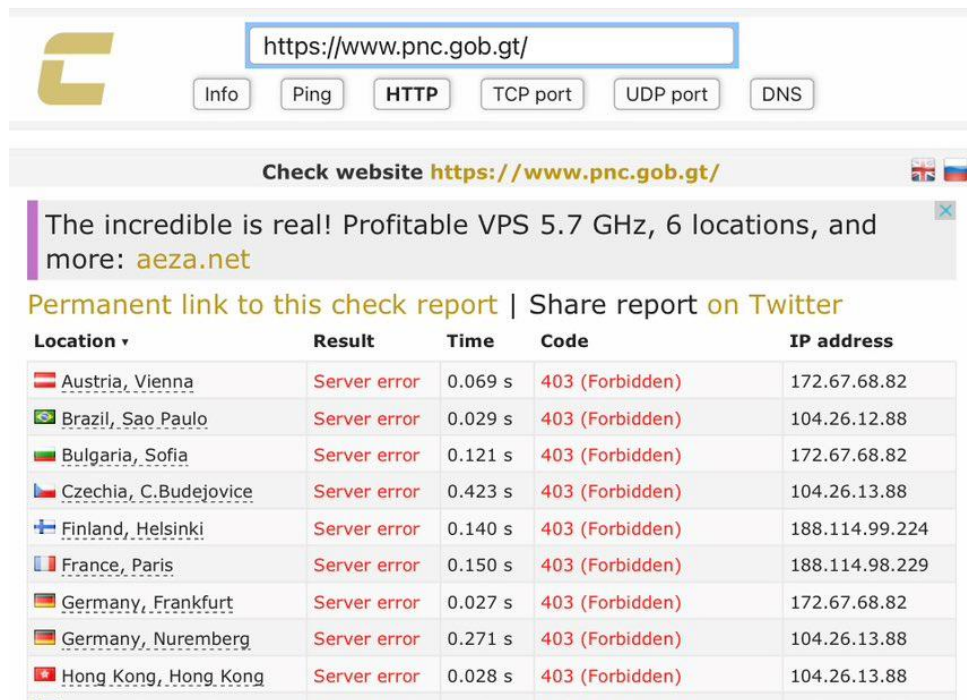
Check website <https://mem.gob.gt/>

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: aeza.net

[Permanent link to this check report](#) | [Share report on Twitter](#)

Location ▼	Result	Time	Code	IP address
Austria, Vienna	Connection timed out			
Brazil, Sao Paulo	Connection timed out			
Bulgaria, Sofia	Connection timed out			
Czechia, C.Budejovice	Connection timed out			
Finland, Helsinki	Connection timed out			
France, Paris	Connection timed out			
Germany, Frankfurt	Connection timed out			
Germany, Nuremberg	Connection timed out			

Imagen 8. Disponibilidad sitio web Ministerio de Ambiente y Recursos Naturales.



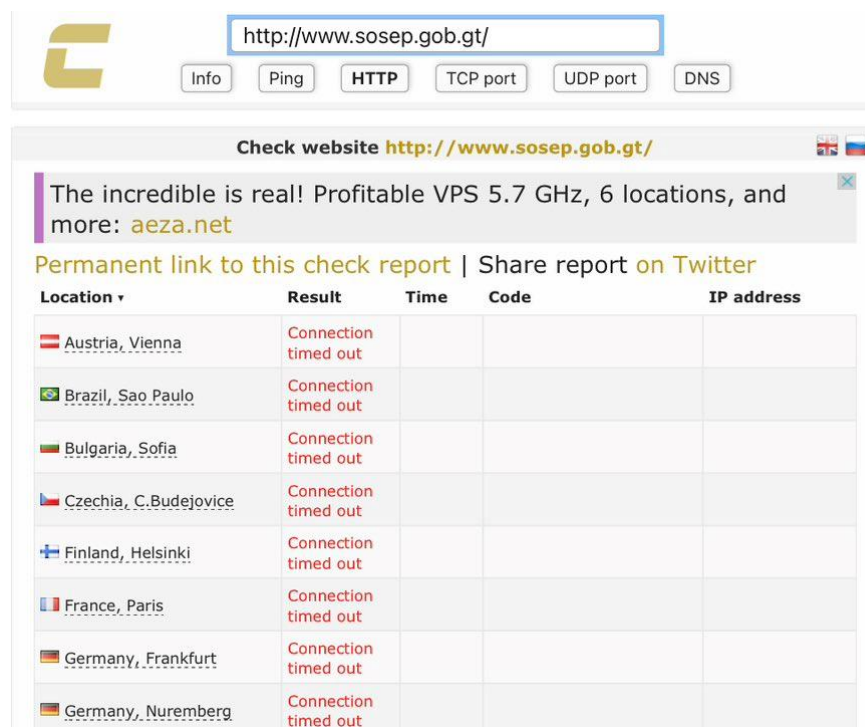
Check website <https://www.pnc.gob.gt/>

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: aeza.net

[Permanent link to this check report](#) | [Share report on Twitter](#)

Location ▼	Result	Time	Code	IP address
Austria, Vienna	Server error	0.069 s	403 (Forbidden)	172.67.68.82
Brazil, Sao Paulo	Server error	0.029 s	403 (Forbidden)	104.26.12.88
Bulgaria, Sofia	Server error	0.121 s	403 (Forbidden)	172.67.68.82
Czechia, C.Budejovice	Server error	0.423 s	403 (Forbidden)	104.26.13.88
Finland, Helsinki	Server error	0.140 s	403 (Forbidden)	188.114.99.224
France, Paris	Server error	0.150 s	403 (Forbidden)	188.114.98.229
Germany, Frankfurt	Server error	0.027 s	403 (Forbidden)	172.67.68.82
Germany, Nuremberg	Server error	0.271 s	403 (Forbidden)	104.26.13.88
Hong Kong, Hong Kong	Server error	0.028 s	403 (Forbidden)	104.26.13.88

Imagen 9. Disponibilidad sitio web Policía Nacional Civil.



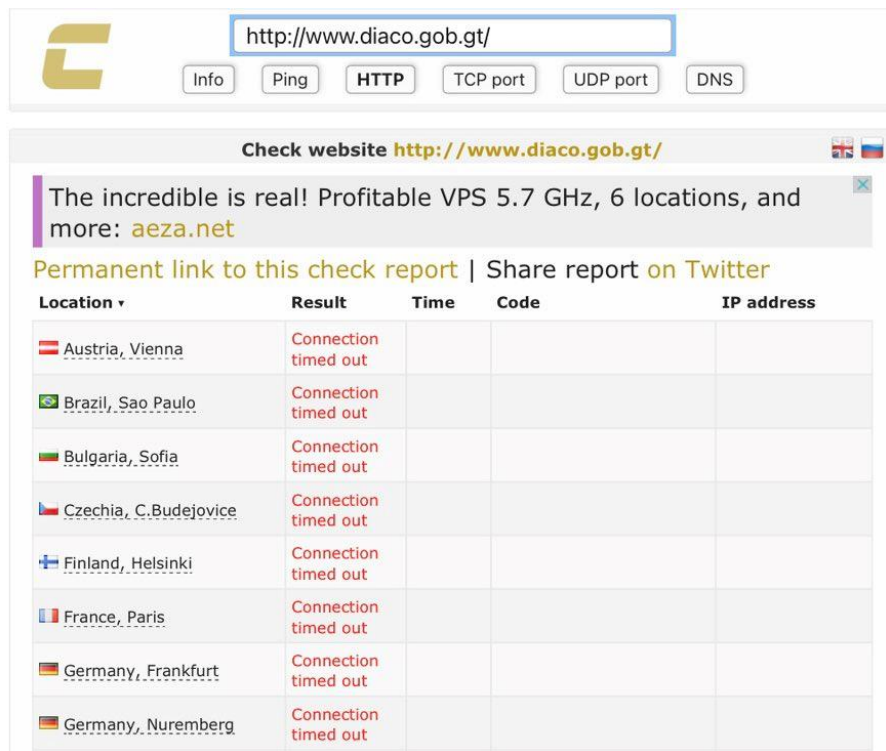
Check website <http://www.sosep.gob.gt/>

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: aeza.net

[Permanent link to this check report](#) | [Share report on Twitter](#)

Location ▼	Result	Time	Code	IP address
Austria, Vienna	Connection timed out			
Brazil, Sao Paulo	Connection timed out			
Bulgaria, Sofia	Connection timed out			
Czechia, C.Budejovice	Connection timed out			
Finland, Helsinki	Connection timed out			
France, Paris	Connection timed out			
Germany, Frankfurt	Connection timed out			
Germany, Nuremberg	Connection timed out			

Imagen 10. Disponibilidad sitio web secretaria de Obras Sociales.



http://www.diaco.gob.gt/

Info Ping HTTP TCP port UDP port DNS

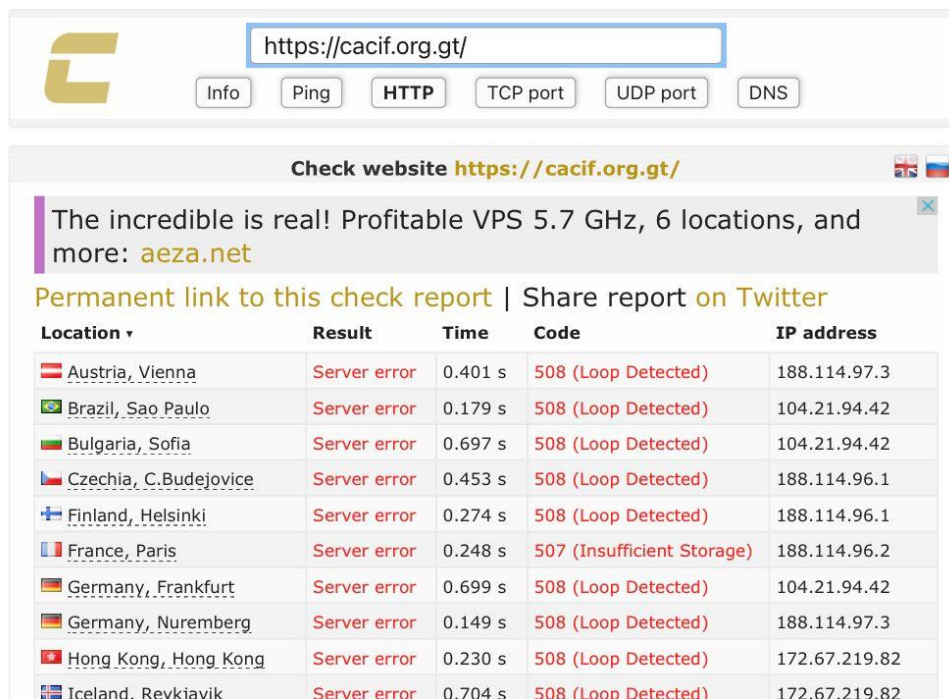
Check website <http://www.diaco.gob.gt/>

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: aeza.net

Permanent link to this check report | Share report on Twitter

Location ▼	Result	Time	Code	IP address
Austria, Vienna	Connection timed out			
Brazil, Sao Paulo	Connection timed out			
Bulgaria, Sofia	Connection timed out			
Czechia, C.Budejovice	Connection timed out			
Finland, Helsinki	Connection timed out			
France, Paris	Connection timed out			
Germany, Frankfurt	Connection timed out			
Germany, Nuremberg	Connection timed out			

Imagen 11. Disponibilidad sitio web DIACO.



https://cacif.org.gt/

Info Ping HTTP TCP port UDP port DNS

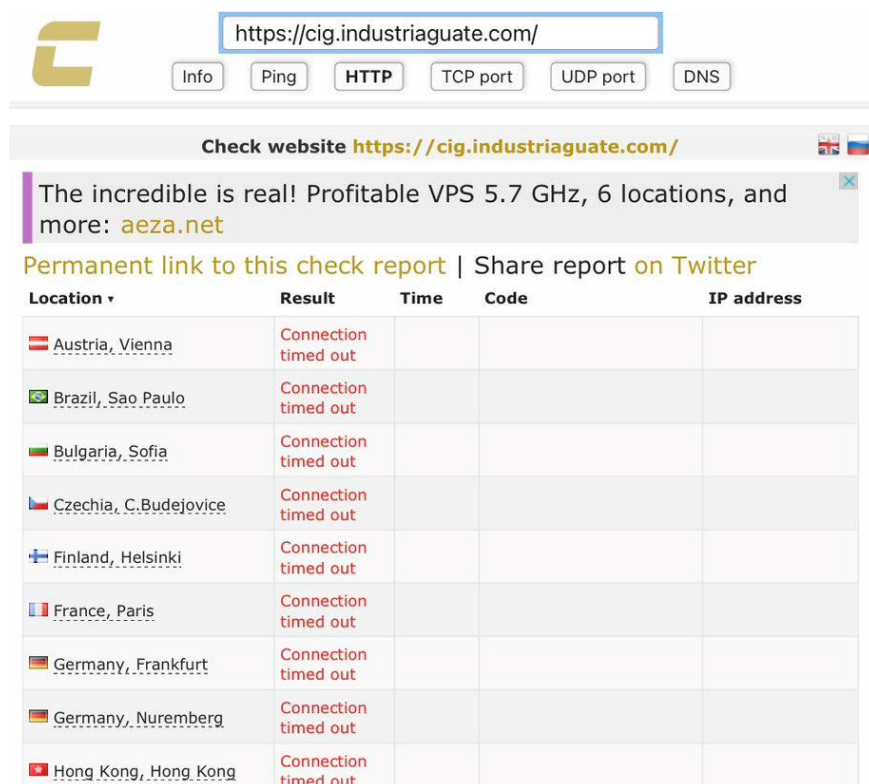
Check website <https://cacif.org.gt/>

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: aeza.net

Permanent link to this check report | Share report on Twitter

Location ▼	Result	Time	Code	IP address
Austria, Vienna	Server error	0.401 s	508 (Loop Detected)	188.114.97.3
Brazil, Sao Paulo	Server error	0.179 s	508 (Loop Detected)	104.21.94.42
Bulgaria, Sofia	Server error	0.697 s	508 (Loop Detected)	104.21.94.42
Czechia, C.Budejovice	Server error	0.453 s	508 (Loop Detected)	188.114.96.1
Finland, Helsinki	Server error	0.274 s	508 (Loop Detected)	188.114.96.1
France, Paris	Server error	0.248 s	507 (Insufficient Storage)	188.114.96.2
Germany, Frankfurt	Server error	0.699 s	508 (Loop Detected)	104.21.94.42
Germany, Nuremberg	Server error	0.149 s	508 (Loop Detected)	188.114.97.3
Hong Kong, Hong Kong	Server error	0.230 s	508 (Loop Detected)	172.67.219.82
Iceland, Reykjavik	Server error	0.704 s	508 (Loop Detected)	172.67.219.82

Imagen 12. Disponibilidad sitio web CACIF.



The screenshot shows a web application interface for checking website availability. At the top, there is a search bar containing the URL `https://cig.industriaguatemala.com/`. Below the search bar are buttons for 'Info', 'Ping', 'HTTP', 'TCP port', 'UDP port', and 'DNS'. The main section displays the checked website `https://cig.industriaguatemala.com/` and a message: 'The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: [aeza.net](#)'. Below this, there is a link to the check report and a 'Share report on Twitter' button. A table follows, showing the results of the check from various locations. All locations show a 'Connection timed out' result.

Location	Result	Time	Code	IP address
Austria, Vienna	Connection timed out			
Brazil, Sao Paulo	Connection timed out			
Bulgaria, Sofia	Connection timed out			
Czechia, C.Budejovice	Connection timed out			
Finland, Helsinki	Connection timed out			
France, Paris	Connection timed out			
Germany, Frankfurt	Connection timed out			
Germany, Nuremberg	Connection timed out			
Hong Kong, Hong Kong	Connection timed out			

Imagen 15. Disponibilidad sitio web Cámara de la industria de Guatemala.

Hasta ahora no se han obtenido declaraciones oficiales de las instituciones listadas anteriormente, sin embargo, se sabe que el tiempo estimado de los ataques de denegación de servicios llevándose a cabo a dichas instituciones tendrán una duración mínima de 3 horas en los servicios.

RECOMENDACIONES

- Conozca los patrones de tráfico de su red y monitorícelos para detectar cualquier anomalía.
- Cree un plan de respuesta a la denegación de servicio basado en una evaluación de seguridad exhaustiva.
- Asegure su infraestructura de red con protección multinivel y cortafuegos.
- Practique una buena ciberhigiene y actualice su software y hardware con regularidad.
- Amplíe su ancho de banda y utilice la redundancia de servidores para distribuir la carga.
- Aproveche las soluciones de hardware y software anti-DDoS.
- Trasládese a la nube o utilice una red de distribución de contenidos para mitigar el ataque.
- Conozca los síntomas de un ataque y actúe con rapidez para detenerlo.
- 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.

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>