SERVICIO ANTIBOTNET PARA EMPRESAS

API pública

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
protege tu empresa

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN Y CONTEXTO

El «Servicio Antibotnet» de INCIBE es un mecanismo que permite conocer si existen incidentes de ciberseguridad relacionados con redes de ordenadores comprometidas o *botnets,* asociados a la conexión de Internet del usuario. Para ello, se comprueba la dirección IP pública desde la que se solicita el servicio contra la base de datos del «Servicio Antibotnet».

Este servicio se ofrece de tres formas:

- La primera se lleva a cabo mediante los operadores de servicios de Internet que colaboran con INCIBE notificando a los usuarios finales de los incidentes de ciberseguridad que afectan a su conexión.
- La segunda es mediante el uso de nuestras herramientas online: chequeo de la conexión y plugins del navegador.
- La tercera es haciendo uso directo de la API pública del servicio, descrita en este documento.

2. CONDICIONES DE USO

El uso de la presente API del «Servicio Antibotnet» de INCIBE supone la aceptación de los términos y condiciones de uso reflejadas en el anexo de este documento.

3. SERVICIO DE CHEQUEO DE IP

Este Servicio **ofrece información sobre incidentes de ciberseguridad relacionados con *botnets*, asociados a la IP pública desde la cual se realiza la petición.** En concreto, el servicio chequea la IP pública desde la que se hace la petición contra la base de datos de evidencias de *botnets* de INCIBE.

3.1. API DEL SERVICIO

Esta documentación hace referencia a la versión 1.1.0 de la API (*Application Programming Interface*) del Servicio Antibotnet. A continuación, se describen los métodos de la API actualmente disponibles para el servicio algunos ejemplos de uso.

3.1.1. Método GET - wscheckip/<idioma>

Devuelve la información de las evidencias de conexiones a redes *botnet* que se hayan detectado asociadas a la IP desde la que se realice la petición:

- Durante las últimas 3 horas, si la IP es dinámica.
- Durante los últimos 4 días, si la IP es fija.

Así como información sobre la amenaza, los sistemas operativos a los que afecta y los enlaces de ayuda a la desinfección.

La base de datos de evidencias de INCIBE se actualiza cada 5 minutos.

Petición de tipo **GET.**

PETICIÓN			
Tipo	**Parámetro**	**Valor**	**Descripción**
GET	<idioma>	es / en	Código de idioma en el que se quiere recibir la respuesta
Cabeceras HTTP	X_INTECO_WS_ Request_Source	api	Cabecera que indica el origen de la petición

Tabla 1 - *Parámetros necesarios para la petición*

RESPUESTA	

Modelo	"title": "CAB JSON Schema",
	"type":"object",
	"$schema": "http://json-schema.org/draft-03/schema#",
	"required": ["ip", "error"],
	"properties":
	{
	"ip": { "type":"string" },
	"error": { "type":"string" },
	"evidences": {
	"type":"array",
	"items":
	{

Modelo	"type":"object",
	"properties":
	{
	"name": { "type":"string" },
	"threatCode": { "type":"string" },
	"operatingSystems":
	{
	"type":"array",
	"items":
	{
	"type":"object",
	"properties":
	{
	"operatingSystem": { "type":"string"},
	"disinfectUrl": { "type":"string" }
	}
	}
	},
	"descriptionUrl": { "type":"string" },
	"timestamp": { "type":"string" }
	}
	}
	}
	}

Descripción	▶ *ip*: Dirección IP desde la que se recibe la petición. ▶ *error*: cadena con el texto del error en caso de que se produzca, o cadena vacía si no hay error. ▶ *evidences*: lista de amenazas asociadas a la IP. » *name*: nombre de la amenaza. » *operatingSystems*: lista de sistemas operativos a los que afecta la amenaza. → *operatingSystem*: sistema operativo. → *disinfectUrl*: dirección url con la información de desinfección. » *descriptionUrl*: url con la información general de la amenaza. » *timestamp*: fecha y hora determinada de la última vez que se detectó que la dirección IP estaba asociada a esta amenaza.
Esquema	{ "ip": "", "error": "", "evidences": [{ "name": "", "threatCode": "", "operatingSystems": [{

Esquema	"operatingSystem": "", "disinfectUrl": "", }, ...], "descriptionUrl": "", "timestamp": "" }, ...] } *NOTA: actualmente no se ofrece más información de la evidencia, como por ejemplo, IP de destino. Si fuera necesaria más información, puede ponerse en contacto con* nuestro equipo de gestión incidentes.

Tabla 2 - *Respuesta del Servicio Antibotnet*

MENSAJES DE ERROR	
Código HTTP	**Mensaje**
200	¡Lo sentimos! Se ha producido un error en el proceso. Por favor, inténtalo de nuevo en unos minutos.
200	Lo sentimos, no podemos ofrecerte información sobre tu conexión actual. El «Servicio Antibotnet» solo es útil si se ejecuta desde una conexión geolocalizada en España y actualmente tu dirección IP está fuera de este rango.

Tabla 3 - *Mensaje de error*

3.1.1.1 Ejemplo de petición

Para realizar la petición contra la base de datos del Servicio Antibotnet se pueden utilizar distintas herramientas y lenguajes de programación. En este apartado se realizará un ejemplo de petición mediante dos herramientas utilizadas habitualmente por los administradores de redes: cURL y PowerShell.

3.1.1.1.1. cURL

cURL en una herramienta orientada a la transferencia de archivos soportando múltiples protocolos entre los que se encuentra el utilizado por la API del Servicio Antibotnet, elprotocolo HTTP. Habitualmente, se encuentra instalada en los sistemas operativos basados en Linux.

Puedes descargar la herramienta desde su página web oficial, se encuentra disponible para multitud de sistemas operativos.

- https://curl.haxx.se/

Un ejemplo de petición contra el Servicio Antibotnet sería:

- Petición:
  - https://antibotnet.osi.es/api/wscheckip/es
- Cabecera HTTP:
  - X_INTECO_WS_Request_Source = api

Los diferentes tipos de respuesta son:

```
root@root:/# curl -XGET -H "X_INTECO_WS_Request_Source: api" https://antibotnet.osi.es/api/wscheckip/es
{"ip":"[redacted]","error":"","evidences":[]}
```

Ilustración 1 - *Ejemplo de respuesta sin evidencias utilizando cCurl*

Ilustración 2 - *Ejemplo de respuesta con evidencias utilizando cCurl*

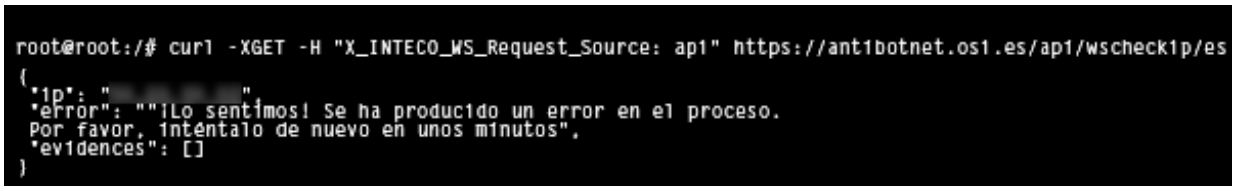

Ilustración 3 - *Ejemplo de respuesta «error en el proceso» utilizando cCurl*

3.1.1.1.2 PowerShell

Powershell es una herramienta orientada a los administradores de sistemas que permite automatizar tareas. Se encuentra presente en todos los sistemas operativos Windows con soporte actual. PowerShell también se encuentra disponible para sistemas operativos basados en Linux y macOS.

Puedes obtener más información sobre PowerShell desde su documentación oficial:

- PowerShell

Para realizar la consulta se utilizará el *cmdlet «command-let»* *Invoke-WebRequest* y los parámetros necesarios definidos en la Tabla 1 para realizar la petición correctamente.

Un ejemplo de petición contra el Servicio Antibotnet sería:

- Petición:
  - https://antibotnet.osi.es/api/wscheckip/es
- Cabecera HTTP:
  - X_INTECO_WS_Request_Source = api

```
PS C:\Users\incibe> Invoke-WebRequest -Uri https://antibotnet.osi.es/api/wscheckip/es -Method Get -Headers @{"X_
INTECO_WS_Request_Source" = "api"}
StatusCode        : 200
StatusDescription : OK
Content           : {"ip":"[redacted]","error":"","evidences":[]}
RawContent        : HTTP/1.1 200 OK
                    X-Permitted-Cross-Domain-Policies: none
                    X-XSS-Protection: 1; mode=block
                    X-Frame-Options: ALLOW-FROM https://www.osi.es/
                    Keep-Alive: timeout=5, max=100
                    Connection: Keep-Alive
                    Cont...
Forms             : {}
Headers           : {[X-Permitted-Cross-Domain-Policies, none], [X-XSS-Protection, 1; mode=block], [X-Frame-Options,
                    ALLOW-FROM https://www.osi.es/], [Keep-Alive, timeout=5, max=100]...}
Images            : {}
InputFields       : {}
Links             : {}
ParsedHtml        : mshtml.HTMLDocumentClass
RawContentLength  : 49
```

Ilustración 4 *Ejemplo de respuesta sin evidencias utilizando PowerShell*

```
PS C:\Users\incibe> Invoke-WebRequest -Uri https://antibotnet.osi.es/api/wscheckip/es -Method Get -Headers @{"X_
INTECO_WS_Request_Source" = "api"}
StatusCode        : 200
StatusDescription : OK
Content           :
{
 "ip": "[redacted]",
 "error": "",
 "evidences": [
  {
   "name": "ZeuS",
   "threatCode": "6M",
   "operatingSystems": [
    {
     "operatingSystem":"Linux",
     "disinfectUrl": http://www.limpia.es
   }
  ],
  "descriptionUrl": "http://www.info.com",
  "timestamp": "2014-10-10 02:00:19"
  }
 ]
}
]}
RawContent        : HTTP/1.1 200 OK
                    X-Permitted-Cross-Domain-Policies: none
                    X-XSS-Protection: 1; mode=block
                    X-Frame-Options: ALLOW-FROM https://www.osi.es/
                    Keep-Alive: timeout=5, max=100
                    Connection: Keep-Alive
                    Cont...
Forms             : {}
Headers           : {[X-Permitted-Cross-Domain-Policies, none], [X-XSS-Protection, 1; mode=block], [X-Frame-Options,
                    ALLOW-FROM https://www.osi.es/], [Keep-Alive, timeout=5, max=100]...}
Images            : {}
InputFields       : {}
Links             : {}
ParsedHtml        : mshtml.HTMLDocumentClass
RawContentLength  : 581
```

Ilustración 5 *Ejemplo de respuesta con evidencias utilizando PowerShell*

```
PS C:\Users\incibe> Invoke-WebRequest -Uri https://antibotnet.osi.es/api/wscheckip/es -Method Get -Headers @{"X_
INTECO_WS_Request_Source" = "api"}
StatusCode        : 200
StatusDescription : OK
Content           : {"ip":"[redacted]","error":"¡Lo sentimos! Se ha producido un error en el proceso.
Por favor, inténtalo de nuevo en unos minutos","evidences":[]}
RawContent        : HTTP/1.1 200 OK
                    X-Permitted-Cross-Domain-Policies: none
                    X-XSS-Protection: 1; mode=block
                    X-Frame-Options: ALLOW-FROM https://www.osi.es/
                    Keep-Alive: timeout=5, max=100
                    Connection: Keep-Alive
                    Cont...
Forms             : {}
Headers           : {[X-Permitted-Cross-Domain-Policies, none], [X-XSS-Protection, 1; mode=block], [X-Frame-Options,
                    ALLOW-FROM https://www.osi.es/], [Keep-Alive, timeout=5, max=100]...}
Images            : {}
InputFields       : {}
Links             : {}
ParsedHtml        : mshtml.HTMLDocumentClass
RawContentLength  : 67
```

Ilustración 6 *Ejemplo de respuesta error utilizando PowerShell*

ANEXO – TÉRMINOS Y CONDICIONES DEL SERVICIO ANTIBOTNET

El Instituto Nacional de Ciberseguridad S.A. (en adelante INCIBE) es una sociedad anónima estatal adscrita a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, con CIF A-24530735 y domicilio social en Avenida José Aguado, 41 24005- León.

La misión de INCIBE es reforzar la ciberseguridad, la confianza y la protección de la información y privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanos, empresas, Administración, red académica y de investigación española, sector de las tecnologías de la información y las comunicaciones y sectores estratégicos en general.

INCIBE está comprometido, por tanto, con la promoción de servicios de la Sociedad de la Información seguros y confiables; que permitan un aprovechamiento de sus ventajas garantizando la protección de la confidencialidad e integridad de la información relacionada con ellos, y previniendo y reaccionando ante posibles ataques que pudiesen poner en riesgo su prestación.

Mediante el presente servicio se ofrece de manera gratuita a los usuarios, la posibilidad de conocer si desde su actual conexión a Internet se han identificado amenazas de seguridad relacionadas con redes de ordenadores comprometidos o *botnets*. Para ello, se utiliza la dirección IP pública (*Internet Protocol*) que está utilizando en Internet y se comprueba en la base de datos del «Servicio Antibotnet», tal y cómo se describe en el apartado 2 de las presentes condiciones.

4.1. OBJETO

Los presentes Términos y Condiciones de Uso y Privacidad (en adelante, "TCGUyP") tienen por objeto regular las condiciones de uso de la API del «Servicio Antibotnet», consistente en el chequeo de la conexión mediante la dirección IP pública utilizada por el usuario (en adelante, "el Servicio").

El uso del Servicio está regulado por las presentes CGUyP, que el usuario acepta de forma implícita en el momento de hacer uso del servicio.

4.2. FUNCIONAMIENTO DEL SERVICIO ANTIBOTNET

El «Servicio Antibotnet» informa de amenazas o incidentes de ciberseguridad relacionados con redes de ordenadores comprometidos o *botnets*, que se puedan estar produciendo desde la conexión a Internet desde la cual se utilice el Servicio. Para ello se comprueba la dirección IP pública en uso en ese momento en la base de datos del «Servicio Antibotnet».

El Servicio no identifica dispositivos de usuario infectados, solo contrasta la dirección IP pública en la base de datos, siempre en el marco de la legalidad vigente. En caso de que el Servicio arroje un resultado positivo, se ofrece información relacionada con la amenaza que puede estar afectando a alguno de los dispositivos, para ayudar a identificarlo (como puede ser el *timestamp* de la evidencia y el sistema operativo al que afecta); y enlaces a herramientas de limpieza, para ayudar en la desinfección.

Se debe tener en cuenta que el Servicio mantiene los registros de infecciones durante 3 horas, lo que significa que, aunque se hayan seguido los pasos recomendados para la desinfección, el servicio podrá tardar un rato en indicar que ya no hay incidentes relacionados con la conexión o dirección IP.

La información del servicio se transmite de forma segura cifrada mediante el uso del protocolo SSL.

Este servicio es un mecanismo de detección puntual y no sustituye en ningún caso a los sistemas antivirus o antimalware.

La información detallada sobre el funcionamiento del servicio está disponible en el siguiente enlace.

4.3. GRATUIDAD DEL SERVICIO

El Servicio es gratuito para el usuario.

4.4. OBLIGACIONES DEL USUARIO

1. El usuario manifiesta conocer que el Servicio es de exclusiva propiedad de INCIBE, y se obliga a respetar los derechos de propiedad intelectual o industrial del autor, no pudiendo alterar, modificar en modo alguno o transformar su formato original, ni explotar el mismo con fines comerciales. Con carácter general el usuario se compromete a la correcta utilización del Servicio, a tenor de lo establecido en la legislación vigente que le fuera aplicable y a lo contenido en las presentes condiciones, absteniéndose de utilizar el Servicio para realizar actividades ilícitas o constitutivas de delito y/o que infrinjan cualquier tipo de disposición legal o intereses de terceros.

2. El usuario solo puede hacer un uso personal de la información obtenida como resultado del Servicio, no pudiendo usarla con fines comerciales ni cederla a terceros.

3. El usuario exonera a INCIBE de cualquier responsabilidad derivada de la inexactitud de los datos aportados o del funcionamiento del Servicio.

4. Si eres menor de edad no emancipado y no has cumplido aún los 18 años, debes leer el presente contrato con tu padre, madre o tutor para garantizar que comprendéis su contenido y por tanto los derechos y obligaciones que adquieres al usar este Servicio.

4.5. RESPONSABILIDAD

1. El usuario acepta que la información del Servicio puede contener errores o falsos positivos debido principalmente a que las direcciones IP públicas que se asignan a los puntos de conexión a Internet pueden cambiar. En consecuencia INCIBE no será responsable de la exactitud, fiabilidad, corrección de los elementos e informaciones del Servicio. Para hacer uso de la API, el usuario deberá previamente descargar y conocer los presentes Términos y Condiciones no pudiendo distribuir la API a terceros.

2. INCIBE puede dejar de prestar o alterar el Servicio sin previo aviso, no generándose responsabilidad alguna para INCIBE con el usuario o con terceras partes por tal motivo.

3. INCIBE declina cualquier responsabilidad respecto del Servicio, ni será responsable por los daños y perjuicios de toda naturaleza derivados de la falta de disponibilidad, mal funcionamiento o de continuidad del funcionamiento del Servicio por incidencias técnicas en los sistemas o cualquier otra causa propia o de terceros.

4. INCIBE no se responsabiliza de las consecuencias derivadas del incumplimiento por parte del usuario de las Condiciones de uso del Servicio y en consecuencia INCIBE no será responsable de los daños o perjuicios causados a otros usuarios del Servicio y/o terceros como consecuencia del comportamiento y uso de la información obtenida por los usuarios del Servicio..

5. Respecto a las citas de productos y servicios de terceros, INCIBE reconoce a favor de sus titulares los correspondientes derechos de propiedad industrial e intelectual, no implicando su sola mención o aparición en la web la existencia de derechos ni de responsabilidad alguna sobre los mismos, como tampoco respaldo, patrocinio o recomendación.

4.6. USO DE LA INFORMACIÓN APORTADA POR EL USUARIO

1. El Servicio usa la dirección IP pública, siempre con el consentimiento explícito del usuario obtenido al aceptar las presentes CGUyP del Servicio, para contrastarla en la base de datos en tiempo real y poder ofrecer el resultado del mismo.

2. Como consecuencia del acceso al Servicio se producirá el tratamiento de la dirección IP por parte de INCIBE, única y exclusivamente, con la única finalidad de comprobar que aquélla no forma parte de una red de botnets que pueda poner en peligro la seguridad de los sistemas del usuario. En este sentido, el usuario consiente que su dirección IP pública sea tratada en los términos de las presentes CGUyP. La dirección IP pública no se asocia a ningún usuario concreto y solo se almacena información a fines estadísticos sobre los resultados del Servicio.

Se informa que INCIBE dispone de un fichero para la gestión de los servicios de seguridad de la información, que ha sido comunicado a la Agencia Española de Protección de Datos y tiene por finalidad "la prestación de servicios en materia de ciberseguridad, confianza y protección de la privacidad en los servicios de la Sociedad de la Información para ciudadanos, empresas, administración, red académica y de investigación sector TIC y sectores estratégicos; y gestión de respuesta y coordinación ante incidentes de seguridad".

Los usuarios podrán ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la normativa sobre protección de datos de carácter personal, dirigiendo su solicitud, en la forma legalmente prevista, a la dirección indicada al comienzo de este documento.

4.7. DERECHO DE EXCLUSIÓN, MODIFICACIÓN Y SUSPENSIÓN DE INCIBE

INCIBE puede libremente suspender o excluir el Servicio o su uso en función de la dirección IP de origen desde la cual se solicita, en cualquier momento y sin previo aviso, o en el caso de que la utilización del Servicio pueda considerarse, a juicio de INCIBE, contraria a las presentes condiciones.

4.8. LEGISLACIÓN APLICABLE Y JURISDICCIÓN COMPETENTE

Las presentes condiciones del Servicio en lo no previsto se rigen por lo dispuesto en el aviso legal y las leyes españolas. INCIBE y el usuario, con renuncia expresa a cualquier otro fuero, se someten al de los Juzgados y Tribunales de la ciudad de León para cualquier controversia que pudiera derivarse de la interpretación, aplicación y utilización del Servicio.

4.9. OTROS

INCIBE hace reserva expresa de cualesquiera derechos pudieran corresponderle sobre el Servicio y los elementos que forman parte del mismo, sin perjuicio de los derechos que sobre ciertos materiales pudieran corresponderle a terceros y/o de las disposiciones de carácter particular que INCIBE haga de sus productos, debidamente autorizadas.

INCIBE no otorga ningún derecho sobre las marcas, signos distintivos, gráficos y logotipos utilizados en relación con el Servicio.

El uso de cualquier parte del Servicio de forma distinta a la permitida por estas TCGUyP queda estrictamente prohibido y será constitutivo de una infracción de los derechos de INCIBE o de terceros, pudiendo castigarse con sanciones civiles y penales, incluyendo el pago de indemnizaciones por daños y perjuicios derivados de dicho uso inconsentido.

5. REFERENCIAS

Más información del «Servicio Antibotnet» para empresas en la sección de herramientas del portal web de INCIBE.

Para cualquier duda sobre el uso de la API puede ponerse en contacto con nosotros a través de nuestro formulario web.

También se ofrece este servicio para un entorno doméstico, desde el «Servicio Antibotnet» de la Oficina de Seguridad del Internauta.

SERVICIO ANTIBOTNET PARA EMPRESAS

API pública

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
protege tu empresa