GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

API PÚBLICA
Servicio antibonet para empresas

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

INDICE

1 INTRODUCCIÓN Y CONTEXTO 3

2 CONDICIONES DE USO 3

3 API DEL SERVICIO 3

3.1 Servicio de chequeo de IP 4

3.1.1 GET - wscheckip/<idioma> 4

4 ANEXO – TÉRMINOS Y CONDICIONES DEL SERVICIO ANTIBONET 9

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 comprometidos o botnets, asociados a la conexión de Internet del usuario. Para ello se chequea 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 conexión y *plugins* de navegador.
- La tercera es haciendo uso directo de la API pública del servicio, descrita en este documento.

Más información del «servicio *antibotnet*» para empresas en la sección de herramientas en el 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, a través del «servicio *antibotnet*» en el portal de la Oficina de Seguridad del Internauta .

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 API del servicio

Esta API hace referencia a la versión 1.2.0 del «Servicio *antibotnet* »

3.1 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.

> *La URL de acceso al servicio es* ***https://antibotnet.osi.es/api/<metodo>***

A continuación se describen los métodos actualmente disponibles para el servicio.

3.1.1 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:

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

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

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

Petición de tipo **GET**.

PETICIÓN			
Parámetro	**Tipo**	**Valor/es**	**Descripción**
<idioma>	GET	*es* | *en*	Código de idioma en el que se quiere recibir la respuesta.
X_INTECO_WS_Request_Source	Cabecera HTTP	*api*	Cabecera que indica el origen de 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":
	{
	"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*: 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*: url con la información de desinfección. ○ *descriptionUrl*: url con la información general de la amenaza. ○ *timestamp*: *timestamp* de la última vez que se detectó que la IP está asociada a esta amenaza.

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

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*» sólo es útil si se ejecuta desde una conexión geolocalizada en España y actualmente tu dirección IP está fuera de este rango.

EJEMPLO	
Petición	https://antibotnet.osi.es/api/wscheckip/es
Cabecera HTTP	X_INTECO_WS_Request_Source = api
Ejemplo de respuesta sin amenazas	{ "ip": "11.11.11.11", "error": "", "evidences": [] }
Ejemplo de respuesta con amenazas	{ "ip": "11.11.11.11", "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" }] }
Ejemplo de respuesta con error	{ "ip": "", "error": "¡Lo sentimos! Se ha producido un error en el proceso. Por favor, inténtalo de nuevo en unos minutos.",

	"evidences": [] }

4 Anexo – Términos y Condiciones del Servicio AntiBonet

El Instituto Nacional de Ciberseguridad S.A. (en adelante INCIBE), sociedad anónima estatal adscrita a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, con CIF A-24530735 y domicilio 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.

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.

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, sólo 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. Esto significa que, aunque se hayan seguido los pasos recomendados para la desinfección, puede pasar un periodo de tiempo hasta que el servicio indique 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 anti-malware.

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

3. Gratuidad del servicio

El Servicio es gratuito para el usuario.

4. Obligaciones del usuario

4.1. 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.

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

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

4.4. 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.

5. Responsabilidad

5.1. 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.

5.2. 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.

5.3. 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.

5.4. 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.

5.5. 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.

6. Uso de la información aportada por el usuario

6.1. 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.

6.2. 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 sólo 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.

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.

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 la ley española. 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.

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 le otorga ningún derecho sobre las marcas, signos distintivos, gráficos y logotipos de INCIBE 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, será constitutivo de una infracción de los derechos de INCIBE o de terceros y podrá castigarse con sanciones civiles y penales, incluyendo el pago de indemnizaciones por daños y perjuicios derivados de dicho uso inconsentido.