Lista IPs Ofensivas

Documentación

Un informe de Cybersecurity Ventures pronostica que el delito cibernético costará al mundo $6 billones en 2021, doblando la cifra de $3 billones en 2015. Esto incluye daños y destrucción de datos, dinero robado, pérdida de productividad, robo de propiedad intelectual, robo de datos personales y financieros, malversación de fondos, fraude, interrupción post-ataque al curso normal de negocios, investigación forense, restauración y eliminación de datos y sistemas hackeados, y daño reputacional.

Muchas empresas sufren por el pobre rendimiento de los servicios que ofrecen a través de internet. No son conscientes que el problema se debe a la lentitud y mal funcionamiento achacable, en la mayoría de las ocasiones, al aumento masivo de ataques de Fuerza Bruta que está teniendo lugar en internet en los últimos meses. Se trata de ataques polimórficos automatizados dirigidos a intentar averiguar usuarios y contraseñas de servicios ofrecidos a través de Internet para luego comercializar con los datos personales y financieros obtenidos. El mal funcionamiento aleja a los clientes. Y el posible acceso a datos personales y/o financieros pone en jaque cualquier política de cumplimiento de la GDPR.

El ciber crimen se ha convertido en una pesadilla para todas las compañías, y por tanto para sus responsables de seguridad, según más ciber criminales han añadido más y más recursos y presión en su lucha por obtener los botines que ellos creen a su alcance y el control de internet. Cientos de nuevos sistemas conectados -entre ellos los del IoT- son hackeados diariamente y añadidos a cualquiera de las redes Z (Bot).

Los procedimientos utilizados para atacar los sistemas empresariales cambian cada día. Por ello, los sistemas de protección por patrones (antivirus tradicionales) y los sistemas de protección por reputación de IPs existentes se vuelven ineficientes demasiado rápido. Ni cubren todas las posibles fuentes de ataque ni son suficientemente rápidos para responder a los cambios en los sistemas atacantes.

La única manera eficiente de proteger los sistemas conectados es aumentar la seguridad y bloquear preventivamente las IPs ofensivas, usadas por los ciber criminales para atacar al resto de Internet, en los Firewalls de nuestros sistemas, actualizando estos todas las veces posibles al día.

Para todas las empresas que se enfrentan a interminables spams de correo electrónico y ataques ransomware y de servidor, y para aquellas empresas que quieren proteger sus sitios web de las crecientes oleadas de ataques de Fuerza Bruta, así como sus servidores de correo y

sistemas críticos contra ataques DDOS o cualquier otro tipo de ataques maliciosos procedentes de sistemas pirateados detrás de las IPs ofensivas, aquí presentamos un nuevo recurso que ha sido desarrollado específicamente para mantener los sistemas empresariales a salvo y dedicados únicamente a ejecutar las tareas para las que fueron diseñados.

Después de muchos años preocupados por la seguridad cibernética y la gestión de datos, i4conAnalytics ha creado, a través de un conjunto complejo de algoritmos y sistemas, una lista de IPs infractoras única en el mundo. Tanto por el número de IPs, su dinámica de actualizaciones (96 al día – cada 15 minutos), y su bajísimo coste (ver más adelante).

La lista crece diariamente con la incorporación de centenares de nuevas IPs procedentes de los sistemas de detección. Su número actual ha crecido hasta un volumen de varios cientos de miles de IPs ofensivas, IPs que, agrupadas y usadas coordinadamente, podrían causar un gran daño en cualquier sistema bajo ataque. Esta lista, si se usa en firewalls y se actualiza cada 15 minutos, será la mejor y más fundamental herramienta para bloquear los ataques de Fuerza Bruta, DDOS, inyección de SQL Server, SMTP, spam, PHISHING, RANSOMWARE y el acceso de todo el resto del malware a sitios web, redes corporativas y sistemas críticos.

DETALLES TÉCNICOS

La lista de IPs Ofensivas de I4conAnalytics es generada por una serie de recursos abiertos a Internet que filtran todas las llamadas entrantes mediante algoritmos muy trabajados y ponen todas las IPs ofensivas detectadas en una lista común. Las IPs ofensivas son puestas en una lista común 96 veces al día.

Esta lista se ha estado preparando durante los 10 últimos años para añadir todas las posibles fuentes de ataque a los sistemas corporativos y para optimizar los algoritmos de filtrado.

Esta lista se sirve en un fichero encriptado por un servicio web Seguro que solo puede llamarse desde las IPs acordadas de aquellos clientes con contrato y únicamente el número de veces contratado.

CASOS DE USO

1. **Ataques PHISING y Ransomware**: Cualquier empleado cuya cuenta de correo electrónico haya sido añadido a la lista de aquellos hackers que atacan otros sistemas mediante redes de equipos Zombi -botnets-, recibirá diariamente, incluso a pesar de los filtros anti-spam corporativos, todo tipo de correos con mensajes atractivos para conseguir que dichos empleados pinchen en cualquier enlace o fichero adjunto y así descargarse el malware de tipo ransomware que buscará extenderse y atacar todo tipo de recursos corporativos accesibles. El coste del daño ocasionado puede ser muy elevado. Con la lista de IPs Ofensivas de i4conAnalytics bloqueando las IPs de origen de estos ataques, estos correos prácticamente desaparecerán y, cuando lleguen, sólo llegará alguno que otro antes de que sea bloqueado en la siguiente carga de la lista de IPS Ofensivas. Se acabaron los intentos repetidos desde los mismos sistemas.

2. **Ataques de Fuerza Bruta**: Estos ataques consisten en intentos repetidos de descubrimiento de usuarios y claves para acceder a Servidores y/o aplicaciones web privadas ofrecid@s a través de internet. Estos intentos son realizados por aplicaciones

polimórficas especialmente diseñadas y parametrizables para detectar los campos en los que introducir los datos de prueba y espaciar o no los intentos de ataque. Se suelen lanzar ataques simultáneos desde diferentes IPs y en oleadas de múltiples intentos por segundo. Su efecto es demoledor para el servicio atacado. No sólo pone en riesgo la seguridad del mismo y de las cuentas de sus usuarios, sino que también causa ralentización a veces extrema de los mismos al tener que responder tantas veces por segundo a los intentos de autenticación dirigidos. Son de los ataques más activos actualmente y pueden evitarse completamente con nuestra lista de IPs ofensivas.

3. **Ataques DDOS**: Muchas empresas necesitan mantener un sitio o servicio web abierto a internet para vender o mostrar sus productos al público o comunicarse con sus clientes o proveedores. Bajo un ataque DDOS, con soluciones cortafuegos anti DDOS, este sitio o servicio ofrecerá un rendimiento pésimo, cuando no una falta de servicio total, durante varias horas hasta que todas las IPs atacantes han sido detectadas y bloqueadas. El coste en términos de pérdida de confianza de los clientes o de pérdida de ventas puede ser muy alto. Con la lista de IPs Ofensivas de i4conAnalytics cargada y protegiendo el sitio o servicio web, este ataque nunca hubiera tenido lugar. Prácticamente todas las IPs atacantes hubieran estado ya bloqueadas. Nada de pérdida de confianza o de ventas.

4. **Ataques de Troyanos**: Los troyanos necesitan conectarse con los sistemas externos que los controlan para lanzar cualquier tipo de ataque interno o externo. Ningún sistema cortafuegos actual conoce las IPs de dichos sistemas de control. Si las IPs de estos sistemas estuvieran ya bloqueadas en los cortafuegos corporativos por hacer uso de la lista de IPs Ofensivas de i4conAnalytics, ningún ataque podría siquiera empezar.

5. **Ataques SQL Server Injection**: La mayoría de las empresas temen compartir un puerto SQL server en internet debido al flujo incesante de ataques al que este se vería sometido. La mayoría de estos ataques son de Fuerza Bruta, lo que implica una repetición ilimitada de intentos de acceso hasta dar con el usuario y contraseña de acceso al sistema de bases de datos. Los cortafuegos corporativos tienen que bloquear el acceso desde todas las IPs menos desde aquellas con permiso de acceso. Esto implica el coste de tener esta lista actualizada y cargada en el cortafuegos. Con la lista de IPs ofensiva de i4conAnalytics bloqueando de antemano las IPs de los sistemas ofensivos, ningún sistema atacante tendrá nunca acceso a ningún SQL server que comparta Puerto en internet. Las empresas podrán olvidarse de tener que actualizar dichos cortafuegos de forma manual cada vez que cambie una IP de un sistema cliente y los servidores SQL server podrán volver a internet y dedicarse a la tarea para la que fueron creados.

6. **SPAM**: Muchas empresas que disfrutan de sus propios servidores de correo electrónico, luchan sin descanso contra el correo electrónico no deseado que llega a los buzones de sus empleados. El Spam no incluye solo anuncios de Viagra o de sexo, sino también todo tipo de ofertas comerciales no deseadas que roban tiempo a los trabajadores. Mientras que de algunos correos uno puede deshacerse haciendo ‘click’ sobre el enlace de ‘Darse de Baja’, los empleados son muchas veces advertidos de no hacerlo ante la posibilidad de acceder a páginas no deseadas desde las que se descargaría algún tipo de malware dañino. Con la protección ofrecida por la lista de IPs ofensivas de i4conAnalytics, la mayoría del Spam dañino sería bloqueado directamente

en el cortafuegos. Los empleados no tendrían que perder su tiempo leyendo o intentando eliminar toda esa cantidad de Spam diario.

PREGUNTAS Y RESPUESTAS

1. **¿Es esta una lista para una región o es global?** Es global. Aunque algunos pocos hackers locales enfocan sus esfuerzos en compañías locales, la mayoría de los hackers son jugadores globales y crean sistemas que atacan otros sistemas alrededor del globo de forma automatizada.
2. **¿Es necesario un cortafuegos profesional para hacer uso de la lista de IPs Ofensivas de i4conAnalytics?** No. Cualquier cortafuegos donde se pueda cargar la lista de IPs Ofensivas servirá. Se puede incluso subir la lista de IPs Ofensivas en el cortafuegos -firewall- de cualquier servidor Windows/Linux. Sólo es necesario tener en cuenta que la lista consta de muchos miles de IPs Ofensivas en este momento y que dicho número aumenta diariamente en varios cientos.
3. **¿Tienen algún script que realice o facilite la descarga del fichero de IPs Ofensivas y su carga en el/los cortafuego/s corporativo/s?** Si, tenemos scripts para servidores Windows 2003-2019. Estos scripts pueden ser utilizados como referencia para el desarrollo de otros scripts para Linux, sistemas Fortinet, o cualquier otro tipo de cortafuegos que admita el uso de scripts para subir y activar listas de IPs a bloquear. Si tiene problemas creando o adaptando su propio script, puede ponerse en contacto con nosotros para un servicio de consultoría.
4. **¿Como debería ser cargada la lista de IPs ofensivas en un cortafuegos corporativo?** Todos los cortafuegos permiten la carga de una lista de IPs Ofensivas a bloquear mientras mantiene activo el bloqueo de IPs existente a resultas de una lista cargada con anterioridad. Una vez que la nueva lista ha sido cargada y configurada, en menos de un segundo, el script procederá a desactivar la antigua y activar la nueva lista de IPs Ofensivas. Sin pérdida de protección en ningún momento.
5. **¿Tienen algún tipo de soporte técnico?** Si, tenemos servicio de consultoría para poner en marcha el proceso de descarga de la lista de IPs Ofensivas y su carga inicial en el cortafuegos corporativo, así como para resolver cualquier problema que pueda surgir durante los procesos diarios de carga.
6. **¿Necesitan los cortafuegos disponer de mucha memoria ram para usar la lista de IPs Ofensivas?** En absoluto. La lista de IPs Ofensivas de i4conAnalytics ocupa unos pocos Kbytes tanto en el fichero de transmisión como en memoria una vez cargada.
7. **¿Qué tipo de software puedo usar para trabajar -descargar y subir al cortafuegos- con la lista de IPs Ofensivas?** El fichero con la lista de IPs Ofensivas de i4conAnalytics se suministra a través de un servicio web creado con Microsoft WCF y disponible en internet. Por lo tanto, cualquier software capaz de conectar con el servicio web, utilizando un nombre de usuario y su clave como parámetros de la llamada, y con capacidad de desencriptar el fichero de IPs Ofensivas descargado, puede ser utilizado para este fin.
8. **¿Qué tipo de encriptación se utiliza para el fichero de IPs Ofensivas?** El fichero de IPs Ofensivas se encripta utilizando el método de encriptación asimétrica DES. Esto significa que la clave usada para su encriptación no es la misma que la que ha de utilizarse para su desencriptado. Además, las claves empleadas son diferentes para cada cliente.
9. **¿En qué consiste la seguridad del servicio web?** Un usuario y una clave son necesarios como parámetros de la llamada al servicio web. Además de esto, nosotros

controlamos el número de veces que el fichero de IPs Ofensivas es descargado desde cada dirección IP, así como la IP desde la que se intenta acceder al servicio. Cualquier IP que de servicio a un sistema que intente obtener la lista sin estar autorizado será incluida en la lista de IPs Ofensivas.

10. **¿Cuánto tiempo lleva subir la lista de IPs ofensivas a un firewall?** La lista parcial, la que se carga cada 15, minutos tarda unos 30 segundos en estar cargada y lista en un servidor Windows 2008R2/2019, mientras que en un servidor Windows 2003/2008 tarda alrededor de 10 minutos. La lista completa tarda alrededor de 12 minutos en estar completamente cargada y lista en un servidor Windows 2008R2/2016, mientras que en un servidor Windows 2003/2008 tarda alrededor de 24 horas. Las buenas noticias son que incluso el proceso largo no perjudica el rendimiento de los servidores mientras los cortafuegos cargan las IPs y que, mientras que la lista nueva no se ha cargado y activado completamente en el cortafuegos, la antigua sigue totalmente activa protegiendo el servidor y sus servicios.

PRECIO DEL SERVICIO

El precio se establece por número de cortafuegos/firewall y con un descuento por volumen:

No. de Cortafuegos	**Precio por Cortafuegos y Mes**	**Descuento**
1-3	50€	0%
4-10	40€	20%
11-25	35€	30%
25+	30€	40%

CONTACTO

Acceder a https://www.i4con.com/que-hacemos/ipsofensivas/ para solicitar un contrato de servicio.

DESCARGO DE RESPONSABILIDAD

Esta lista ha sido creada con la única intención de proteger los sistemas informáticos del inmenso malware en Internet. Se está ofreciendo como una herramienta de ayuda y es su única responsabilidad si, al usarla, cualquiera de sus sistemas se vuelve inestable o deja de funcionar. Utilícela con cuidado y tras realizar las debidas comprobaciones. Además, cualquier usuario de esta lista debe entender que su uso no garantiza que sus sistemas se vuelvan 100% seguros. Debido a ello, i4conAnalytics no se hará en ningún caso responsable de cualquier daño ocasionado por los hackers en sus sistemas o su patrimonio.

Por otro lado, si su IP está en la lista negra, no es un 'spammer' ni un delincuente, el sistema que utilizaba dicha IP para atacar otros sistemas ha sido saneado, y quiere que esta IP sea eliminada de nuestra lista, por favor envíe un correo electrónico detallando su razonamiento y/o las acciones tomadas para limpiar la infección que dio origen a su consideración como IP ofensiva. Haremos todo lo posible para analizar cada caso y eliminar la/s IP/s de nuestra lista si así se considera.

Noviembre 2019