Ciber Guardián de IPs Ofensivas

Documentación

Un informe de Cybersecurity Ventures ha estimado que el delito cibernético costó 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 paulatino de ataques de Fuerza Bruta que está teniendo lugar en internet. 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 perimetral 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, Exabai ha creado, a través de un conjunto complejo de algoritmos y sistemas, un Ciber Guardián que gestiona 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 o miles 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. Si el Ciber Guardián que gestiona esta lista se usa en firewalls y se actualiza cada 15 minutos, tendrá la mejor y más fundamental herramienta de defensa perimetral 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 Exabai es generada por una serie de recursos dispersos abiertos a Internet que filtran todas las llamadas entrantes mediante algoritmos muy trabajados y ponen todas las IPs ofensivas detectadas en una lista común 96 veces al día.

Esta lista se ha estado preparando durante los 14 últimos años para añadir todas las posibles fuentes de ataque a los sistemas corporativos y para optimizar los algoritmos de filtrado.

La lista se sirve desde un API REST seguro que solo puede llamarse desde el Ciber Guardian ubicado en los sistemas con 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 hagan ‘clic’ en cualquier enlace o descarguen un fichero adjunto y así inyectar un malware de tipo troyano o ransomware que buscará extenderse y encriptar todo tipo de recursos corporativos accesibles. El coste del daño ocasionado puede ser muy elevado. Con el Ciber Guardián y la lista de IPs Ofensivas de Exabai bloqueando las IPs de origen de estos ataques, estos correos disminuirán enormemente en número y, cuando lleguen, sólo llegará alguno que otro antes de que su IP de origen sea bloqueada 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 error 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 nuestro Ciber Guardián y su 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, incluso 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 el Ciber Guardián y su lista de IPs Ofensivas de Exabai cargado y protegiendo la seguridad perimetral del sitio o servicio web, este ataque nunca hubiera tenido lugar. Prácticamente todas las IPs de los sistemas atacantes hubieran estado ya bloqueadas sin merma de rendimiento. 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 del Ciber Guardián con su lista de IPs Ofensivas de Exabai, 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. Para enfrentar este desafío, 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 el Ciber Guardián y su lista de IPs ofensiva de Exabai bloqueando regularmente las IPs de los sistemas ofensivos, ningún sistema atacante tendrá nunca el acceso necesario 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 el Ciber Guardián y la lista de IPs Ofensivas de Exabai bloqueando las IPs de origen de estos ataques, estos correos disminuirán enormemente en número y, cuando lleguen, sólo llegará alguno que otro antes de que su IP de origen sea bloqueada en la siguiente carga de la lista de IPS Ofensivas. Se acabaron los intentos repetidos desde los mismos sistemas. 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 del Ciber Guardián y su lista de IPs Ofensivas de Exabai?** No. Cualquier cortafuegos donde se pueda cargar la lista de IPs Ofensivas y tenga un servidor cercano donde instalar el cliente del Ciber Guardián 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 o miles más. Los recursos necesarios para un servidor Windows 2019 son actualmente de 1.5Gb de memoria.
3. **¿Tienen algún cliente que realice o facilite la descarga del fichero de IPs Ofensivas y su carga en el/los cortafuego/s corporativo/s?** Si, tenemos clientes del Ciber Guardián para servidores Windows 2003-2019 y Linux. Estos clientes pueden ser utilizados como referencia para el desarrollo de otros clientes para sistemas Fortinet o cualquier otro tipo de cortafuegos que admita el uso de scripts para subir y activar listas de IPs a bloquear. Exabai ofrece un servicio de consultoría para adaptaciones o creación de nuevos clientes de su Ciber Guardián.
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 mantienen 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 cliente 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 instalación del cliente del Ciber Guardián y su lista de IPs Ofensivas, así como de su carga inicial en el cortafuegos corporativo. También podemos ayudarle a resolver cualquier problema que pueda surgir durante los procesos diarios de carga de sus firewalls.
6. **¿Necesitan los cortafuegos disponer de mucha memoria ram para usar la lista de IPs Ofensivas?** Los firewalls suelen disponer las listas de IPs a bloquear de forma que su consulta sea muy eficiente en términos de carga y tiempo de procesamiento. Por ello la lista de IPs Ofensivas de Exabai, una vez cargada y activada en el cortafuegos, ocupa actualmente 1.5Gb.

7. **¿Puedo usar otro tipo de software para trabajar -descargar y subir al cortafuegos- la lista de IPs Ofensivas?** El Ciber Guardian trabaja con la lista de IPs Ofensivas de Exabai a través de un API REST web disponible en internet. Este API REST sólo permite accesos desde determinado software y determinas IPs que han sido dadas de alta una vez cerrado el acuerdo con nuestros clientes. Es por ello que Exabai ofrece consultoría para crear cualquier nuevo cliente del Ciber Guardián o cualquier modificación que se considere necesaria al objeto de cubrir el espectro de usuarios más amplio posible. No es posible utilizar ningún otro tipo de cliente que no sea el Ciber Guardián.
8. **¿Qué tipo de encriptación se utiliza para el fichero de IPs Ofensivas?** El Ciber Guardián encripta sus comunicaciones con el API REST que sirve las IPs Ofensivas 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 la lista de IPs Ofensivas es descargada 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 180 minutos en estar completamente cargada y lista en un servidor Windows 2008R2/2019, 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.exabai.com/que-hacemos/ciber-guardian/ para solicitar más información o un contrato de servicio.

DESCARGO DE RESPONSABILIDAD

Nuestro Ciber Guardián y su lista de IPs Ofensivas han sido creadas con la única intención de proteger los sistemas informáticos del inmenso malware en Internet. Se están 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, tal y como se ha detallado en este documento, cualquier usuario de esta herramienta debe entender que su uso no garantiza que sus sistemas se vuelvan 100% seguros. Debido a ello, Exabai 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 sus datos, 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.

Septiembre 2024