Cuidado con el impacto de la ciberseguridad en SEO

Tenga cuidado con el impacto de la ciberseguridad en SEO. Como experto SEO no podía quedarme callado al respecto, un servidor web inseguro es garantía de fracaso para nuestro sitios web. No solo se pierden visitas potenciales de los motores de búsqueda sino que se mina la confianza al aparecer advertencias, etc etc.

La mayoría de las medidas de seguridad de los sitios web pueden afectar el rastreo de Google para obtener referencias naturales de las páginas y campañas pagas. Ataque DOS, inyección SQL, Malware , Ciberataque, Hacking, anti-intrusión, Scrapping, Pen test… Una serie de términos ha aumentado en la vida diaria de los referentes de SEO y SEA con sus sitios, a raíz de los ataques al gobierno sitios, robo de datos o rescate de sitios de comercio electrónico.

Sin embargo, la mayoría de las medidas de seguridad del sitio pueden afectar el rastreo de Google para referencias naturales de páginas web y campañas SEA pagas. El ciberdelito se está aprovechando de la pandemia (+ 400% desde Covid-19 según Alert MSSP) para aprovechar las fallas no corregidas con la caída de la vigilancia vinculada al período. Sin embargo, la mayoría de las medidas de seguridad del sitio pueden afectar el rastreo de Google para la referencia natural de sus sitios y sus campañas SEA pagas.

Aquí hay algunos puntos de atención sobre los pasos que planea tomar para evitar clasificar a los motores de búsqueda como atacantes cibernéticos. Asegurar un sitio no solo pasa por la compra de un certificado SSL para obtener un protocolo https.

Este Protocolo seguro también es inútil contra todos los ataques que discutiremos en este artículo.

Hay muchas consecuencias durante un ataque o un intento: el sitio se vuelve inaccesible en caso de un ataque DDoS o representa un riesgo para sus usuarios si estamos hablando de una inyección SQL. En el primer caso, el sitio experimenta una sobrecarga de solicitudes que provoca una lentitud extrema o una accesibilidad completa. En definitiva, una situación que muchas veces resulta estresante para los responsables, obligándolos a tomar medidas radicales para evitar un nuevo cierre temporal lo antes posible. La pérdida de ganancias derivada de este tipo de ataques no es solo financiera, sino que también afecta la imagen de la empresa.

Asegure su sitio para evitar matar el SEO de su sitio

Google, en su objetivo diario de presentar las mejores respuestas a cada búsqueda de los internautas, también tiene en cuenta la seguridad del sitio. Obviamente, su objetivo es no hacer que sus usuarios se arriesguen y, por tanto, ¡presentar sitios 100% seguros! Además, Google, en caso de que haya abierto una consola de búsqueda , al menos puede advertirle de un aumento de errores inusuales cuando su sitio está infectado con malware. En caso de contaminación, Google habrá identificado su sitio como infectado con malware y su clasificación bajará para dejar de estar resaltada para los usuarios de Internet.

Para terminar con la ayuda que te brinda Google en la lucha contra la ciberseguridad, la primera medida que se suele citar se refiere a la actualización de tu CMS . Google puede enviarle una notificación cuando su CMS sea una versión antigua con fallas conocidas.

¡Bloquea todo a toda costa!

El departamento de seguridad informática de una empresa buscará, para evitar ataques, reducir los espacios de intrusión. Se protege, como medida preventiva, de limitar el acceso a sitios con orígenes dudosos, frecuencias de tráfico intenso o sorprendentemente automatizados. Su objetivo es concentrar los pasos en un solo carril extremadamente supervisado para limitar los riesgos tanto como sea posible. Desafortunadamente, las acciones tomadas pueden convertirse claramente en un freno o incluso en un bloqueo para el paso de los motores de búsqueda, que siguen siendo herramientas automatizadas (rastreadores) con una huella comparable al malware.

¿Qué medidas amigables con SEO para proteger contra ataques cibernéticos?

Hoy en día, la mayoría de los sitios han comprado su certificado seguro para obtener un protocolo https. Una de las principales motivaciones fue mejorar su SEO (que aún está por demostrar). El principio de tener un certificado SSL le permite cifrar los datos que pasan por su sitio. Sin este certificado, corre el riesgo de comprometer la seguridad de sus visitantes en las etapas de pago, por ejemplo.

No, Google no realiza un ataque DDoS

Los ataques DDoS (Distributed Denial of Service) consisten en saturar un sitio que llama a su sitio para mostrar 1 o más páginas con múltiples solicitudes. En general, los servidores no admiten este tipo de sondeo masivo y, en caso de que no estén equipados con protección, se ralentizan y se bloquean.

El sitio se vuelve inaccesible por un corto tiempo y se cae si el ataque continúa. Se suele culpar a Google de ser la causa de que un sitio se ralentice o incluso de que no esté disponible.

Antes de decir esto, debe asegurarse de que Mountain View esté detrás del agente de usuario de Googlebot. Si Google es realmente el motor que hace toser a su servidor, entonces debe hacerse preguntas sobre su infraestructura: ¿está realmente bien dimensionada?

Varios servicios como Akamai o Cloudflare ofrecen soluciones de bloqueo de ataques DooS, lo que permite identificar las fuentes de estos ataques por diferentes capas. Esto implica identificar al agente de usuario con un bloque en todos los identificadores que contienen * bot *. La medición de detección también se puede realizar sobre la frecuencia de los interrogatorios. Ningún humano llamaría a las páginas de un sitio con una frecuencia regular de 5 páginas por segundo, por ejemplo.

Finalmente, algunos sistemas también detectan la IP de la entidad que solicita acceso a la página en sentido ascendente y pueden bloquearse si se considera que es una fuente de ataque regular. Sin embargo, Google rastrea desde una IP estadounidense, con un agente de usuario de GoogleBOT y con una frecuencia bastante automatizada que podría llevar a creer en una botnet maliciosa.

¿Cómo evitar que Google sea bloqueado?

Cuando una empresa es atacada, el departamento de seguridad de la empresa a menudo tiene carta blanca para evitar que vuelva a suceder. En general, las medidas son tan restrictivas que los motores de búsqueda a menudo quedan atrapados en las grietas, lo que hace que su sitio sea eliminado de la lista. Sin embargo, incluso si parece obvio que bloquear los motores de búsqueda es una herejía para el SEO de un sitio, no siempre es fácil sugerir que debe existir una lista blanca para ellos.

En primer lugar, si queremos permitir que Google eluda las medidas de seguridad, no basta con autorizar a los agentes de usuario que utilizan Googlebot para allanar el camino para su rastreador. De hecho, es bastante sencillo utilizar este agente de usuario para iniciar rastreos en sitios y pretender ser el último. La solución de resolución de DNS para detectar Google Google no comunica más rango de IP para detectar si realmente son los servidores de San Francisco los que están en acción.

De hecho, Google puede rastrear o probar sitios desde direcciones IP en cualquier parte del mundo para verificar,

por ejemplo, que el sitio sigue siendo el mismo. Google ofrece una solución a implementar para verificar que el rastreador de Googlebot es el de Google: resolución DNS. Cuando una persona / entidad visita su sitio demasiado, ¡obtendrá su dirección IP en sus registros! Al realizar una resolución DNS en esta IP, podrá obtener el dominio detrás de ella: en el caso de una IP de Google, obtendrá google.com o Googlebot.com.

Para evitar la latencia del sitio, la solución es probar las direcciones IP de solicitud demasiado frecuentes con un agente de usuario de Googlebot para clasificar las visitas legítimas de las que no lo son. No lo hagas de forma sistemática para evitar cargar tus servidores y correr el riesgo de ser la causa de la lentitud o incluso el fallo de tu infraestructura.

Leer también: Multicloud: cómo reducir la superficie de exposición a los riesgos de ciberseguridad; Ciberseguridad y protección de la privacidad: ¿quién es el responsable?; Mitigación de ataque DDos