5 PREGUNTAS SOBRE DNS IMPRESCINDIBLES

Casi todas las acciones que se realizan en Internet empiezan por una solicitud al sistema de nombres de dominio (DNS), que traduce los nombres de dominio a direcciones IP. Pese a que el DNS ayuda a ofrecer una Internet más rápida y eficiente, además de facilitar la navegación de los usuarios, es vulnerable ante los ataques debido a su carácter abierto y omnipresente. El DNS no cuenta con inteligencia en sí mismo y, como resultado, resuelve las solicitudes de dominios inofensivos, pero también de los maliciosos.

Los ciberdelincuentes aprovechan esta vulnerabilidad de la infraestructura de DNS recursivo para lanzar campañas de phishing, malware, ransomware y exfiltraciones de datos contra empresas. A medida que los usuarios, dispositivos, aplicaciones y datos se trasladan fuera del perímetro tradicional de la empresa y de la zona de control, la superficie de ataque se expande.

Por eso, ¿cómo protege su red de forma proactiva frente a estas amenazas específicas? Muchas empresas están recurriendo a una estrategia de seguridad de confianza cero ("zero trust"), basada en el principio de "verificar, pero nunca confiar", para todos los usuarios y dispositivos. Este enfoque es especialmente relevante si analizamos el riesgo inherente que plantean dichos usuarios y dispositivos en las solicitudes de DNS salientes. Estas son las cinco preguntas que debe plantearse para determinar si necesita una estrategia de seguridad de DNS.

1 ¿Cuántas solicitudes resuelve su DNS recursivo al día?

Un dispositivo realiza varios miles de consultas diarias; multiplique esto por el número de usuarios y dispositivos que se conectan a su red. Resulta difícil consultar estos datos en conjunto, dado que el volumen suele denegar el acceso al sistema de gestión de eventos e información de seguridad (SIEM). Sencillamente, hay demasiado tráfico bueno (y demasiado poco tráfico perjudicial) como para justificar la adición de registros a SIEM. Además, exportar registros y extraer datos de diversas fuentes es una tarea bastante engorrosa. Incluso en el supuesto de que superase todos estos problemas de recopilación, se acabaría encontrando frente a miles (o millones) de nombres de host sin contexto. Aunque una cantidad excesiva de datos supone un problema, contar con pocos es aún peor, puesto que hay un vacío de información.

2 ¿Cómo es el tráfico de DNS irregular?

En otras palabras, ¿dispone de una referencia para evaluar el estado y la regularidad del tráfico de DNS? Dada la cantidad y la variedad de las solicitudes de DNS de su red (procedentes de portátiles, teléfonos móviles, equipos de escritorio, tablets, impresoras y Wi-Fi de invitados, por no mencionar todos los dispositivos "inteligentes" conectados), es difícil saber cuál es la norma en el día a día. Además, habitualmente, resulta demasiado tedioso y engorroso sumergirse en los datos para identificar qué dispositivos de la red están realizando solicitudes.

Sin embargo, esta información es importante, ya que el tipo de dispositivo puede indicar que algo no va bien. Que un portátil haga miles de consultas de DNS recursivo al día no debería resultar sospechoso; pero, si es el sistema de acondicionamiento de aire de la empresa quien las hace, sin duda se debería investigar. Eso sí, siempre que pueda identificar que el sistema de acondicionamiento de aire es el origen de esas solicitudes superfluas. A medida que aumenta el número de dispositivos conectados (Internet de las cosas), que se prevé que alcance los 20 400 millones en 2020,[1] la exposición de su empresa a los ataques no hará sino crecer en paralelo.

Por mucho que asignara recursos para supervisar y examinar al milímetro los registros de DNS, o se descubriera (seguramente, demasiado tarde) que algo ha salido tremendamente mal, es muy poco probable que pueda detectar y mitigar una intrusión antes de que cause estragos. Esto se debe a que las muestras de su empresa son demasiado pequeñas como para identificar las amenazas y tendencias que se dan a lo largo y ancho de Internet. Por eso, en muchos casos, se recurre a un servicio en la nube. Cuanto más tráfico e inteligencia observe en conjunto, más fácil será detectar el tráfico de DNS irregular; debe conocer los patrones y las tendencias globales para identificar las amenazas de forma eficaz y constante.

3 ¿Sabe que el DNS recursivo se puede utilizar para extraer datos de su empresa?

Las amenazas específicas van evolucionando conforme las empresas y las personas reaccionan ante los ataques. Los ciberdelincuentes cada vez utilizan más el DNS recursivo para introducirse en los perímetros de seguridad, aprovechando las vulnerabilidades inherentes a la infraestructura. Una vez que se contagia algún dispositivo de su red, la inmensa mayoría del malware devuelve una solicitud a su servidor de mando y control (CnC) para obtener indicaciones. Estas consultas aprovechan que el tráfico de DNS debe carecer de filtros y ser abierto para pasar desapercibidas y esquivar la seguridad de la capa de red.

A través de los túneles DNS, los piratas informáticos pueden exfiltrar registros financieros, números de la seguridad social, datos de tarjetas de crédito y propiedad intelectual, entre otros tipos de información confidencial. Para no ser detectados, estos paquetes de datos se cifran, comprimen, dividen y, finalmente, transmiten mediante diversas técnicas, como el goteo, la suplantación de IP, los algoritmos de generación de dominios (DGA) y el Fast Flux. Por ello, no se enteraría en absoluto de una filtración de este tipo si dependiera únicamente de la seguridad de nivel de red.

Entender esta vulnerabilidad inherente es aún más importante si se tiene en cuenta la creciente movilidad de los empleados en la actualidad. A medida que los empleados, proveedores, partners y distribuidores salen del perímetro de red tradicional (al trabajar cada vez más desde casa, cafeterías, aeropuertos, hoteles o conferencias, por ejemplo), aumentan las probabilidades de que sus dispositivos se conecten a redes que no estén bien protegidas. Tan solo es necesario que un dispositivo afectado se vuelva a conectar a la red corporativa para desencadenar un ataque de malware que facilite la filtración de datos de la empresa.

4 ¿Puede aplicar políticas para bloquear la actividad maliciosa en cualquier punto de la empresa en cuestión de segundos?

Identificar una dirección IP o un dominio perjudiciales es difícil, pero solo es la mitad del trabajo que implica mitigar una amenaza específica. Una vez que se ha localizado el ataque o la vulnerabilidad, los equipos de TI tienen la poco envidiable tarea de implementar un plan de defensa rápidamente y en toda la empresa. Si no se cuenta con una solución en la nube, dicha tarea puede implicar numerosas actualizaciones de software e instalaciones de hardware poco prácticas. Para aplicar estas directivas, también es necesaria una comunicación eficaz y a tiempo de la sede central, además de estar supeditadas al pleno cumplimiento por parte de la totalidad de las divisiones, los empleados y los dispositivos de su red.

Eso significa que pueden tener cabida muchos errores, además de horas (si no días) de exposición. Por otro lado, una solución basada en la nube se puede configurar e implantar en cuestión de minutos, sin hardware ni software. Es posible gestionarla desde cualquier lugar, distribuirla a donde sea y aplicarla de forma unilateral casi al instante.

5 ¿Forma parte el DNS de su sistema de seguridad por capas?

No puede permitirse lo contrario. El 70 % de las organizaciones sufrió un incidente de seguridad que ha impactado negativamente en su negocio en 2016;[2] el número de filtraciones creció un 30 % en 2017;[3] la media de tiempo que se tarda en identificar una filtración es de seis meses;[4] y el coste medio es de 18 millones de dólares, que incluye el daño a la reputación de la marca.[5]

Dado que todas las solicitudes web procedentes de una empresa comienzan por el DNS, este sistema es el punto de control perfecto para proteger la visibilidad empresarial en las solicitudes web y para aplicar una política de seguridad. Y dado que esta validación tiene lugar antes de que se establezca la conexión IP, las amenazas se detienen en las primeras fases de la intrusión, lejos del perímetro empresarial. A menudo, se olvida que el DNS recursivo es un vector de ataque, pero con un malware en constante evolución y unos incentivos financieros, cada vez mayores, para los piratas informáticos, necesita reforzar esta puerta trasera tan vulnerable.

Protección proactiva ante amenazas específicas en la nube

Proteger el DNS recursivo de las amenazas específicas de forma proactiva es primordial, e incorporar una solución en la nube como Akamai Enterprise Threat Protector a la pila de seguridad es más sencillo que nunca. Se configura rápidamente, y es fácil de escalar e implementar, sin hardware, ni software, ni tiempo de inactividad. El portal en la nube ofrece una gestión central ágil y la aplicación de políticas unificadas en minutos. Por otro lado, con el panel es posible analizar en profundidad el tráfico de DNS, los eventos asociados a amenazas y las actividades que contempla la política de uso aceptable (PUA).

Enterprise Threat Protector se integra fácilmente con otros productos de seguridad y herramientas de generación de informes, de forma que las empresas puedan aprovechar al máximo sus inversiones en todas las capas de su estrategia de defensa en profundidad. Enterprise Threat Protector, que incorpora la inteligencia en tiempo real de Akamai Cloud Security Intelligence y datos clave que provienen de la gestión del 30 % del tráfico web global mediante Akamai Intelligent Platform, proporciona una protección casi instantánea para las empresas y sus empleados.

Para obtener más información sobre Enterprise Threat Protector, lea el documento "*Cómo usar el DNS para protegerse proactivamente contra el malware*" y visite la página de producto.

FUENTES

1. http://www.gartner.com/newsroom/id/3598917
2. **RSA Cybersecurity Poverty Index 2016,** https://www.rsa.com/en-us/resources/rsa-cybersecurity-poverty-index-2016
3. http://247wallst.com/technology-3/2017/06/22/2017-data-breaches-nearly-30-higher-than-2016s-record-pace
4. **Ponemon Institute: 2016 Cost of Data Breach Study,** https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN
5. **Ponemon Institute: The Economic Impact of Advanced Persistent Threats**