Akamai

INFORME SOBRE LAS SOLUCIONES DE AKAMAI

PROTECCIÓN ANTE AMENAZAS ESPECÍFICAS EN LA NUBE

PROTEJA A SU EMPRESA DE MANERA PROACTIVA FRENTE A LAS AMENAZAS ESPECÍFICAS

La mayoría de los profesionales del sector de la seguridad coinciden en que no es cuestión de si su empresa va a ser presa de un ataque específico con malware, ransomware o phishing, sino de cuándo va a ocurrir eso. De hecho, un 70 % de las organizaciones habría sufrido un incidente de seguridad que impactó negativamente en su negocio el año pasado[1], una cifra que concuerda con la realidad de los más de 390 000 programas maliciosos que se registran a diario.[2] Dado el creciente número de dispositivos conectados y los mayores incentivos financieros para los ciberdelincuentes, la presencia, el volumen y la sofisticación de las amenazas específicas van en constante aumento.

El mayor riesgo de sufrir ataques y la reacción de las empresas ante los mismos han hecho evolucionar al panorama de amenazas. Los actores maliciosos evolucionan las amenazas específicas y localizan vulnerabilidades en las defensas de seguridad de las empresas. Una de las áreas que capta cada vez más la atención de los ciberdelincuentes es el sistema de nombres de dominio (DNS). El DNS en general, y el DNS recursivo en particular, es el objetivo perfecto para un ciberataque, porque está en todas partes, es abierto y no suele estar protegido. El número de amenazas específicas que aprovechan este vector va en aumento.

¿POR QUÉ SE EXPLOTA EL DNS?

Casi todas las acciones que se realizan en Internet comienzan con una solicitud de DNS que asigna nombres de dominio a direcciones IP. Si bien el DNS dota de agilidad, eficiencia y capacidad de navegación a Internet, dada su naturaleza abierta y omnipresente, es también el objetivo perfecto para su explotación. 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 para lanzar ataques específicos como los ataques de phishing, las campañas de malware y ransomware o la exfiltración de datos de las empresas.

¿POR QUÉ ES ESTE UN PROBLEMA URGENTE?

Si el DNS recursivo no se supervisa, es cuestión de tiempo que una de las cientos de miles de solicitudes diarias de Internet realizadas desde su red produzca una descarga maliciosa. Esto puede ocurrir de diferentes maneras: Un empleado hace clic en un enlace de un correo electrónico de phising, seleccionar un anuncio infectado por malware, abre una URL afectada en una red social, navega a sitios que utilizan la táctica de typosquatting, accede a un dominio homográfico, comparte contenido multimedia infectado almacenado en el equipo o sucumbe ante una táctica de ingeniería social.

Un dispositivo afectado se convierte rápidamente en una puerta de enlace para las infecciones de toda la empresa que pueden ralentizar o bloquear su red, espiar las actividades empresariales, robar información, eliminar datos y archivos, convertir los dispositivos en "ordenadores zombi" que alojan contenido ilegal o involucrarla en ataques DDoS, por citar solo algunas.

Además, una vez que accede a su red, la gran mayoría del malware enviará una solicitud a su servidor de mando y control (CnC) para recibir instrucciones adicionales. Puesto que el tráfico de DNS debe ser abierto y sin filtros, estas comunicaciones maliciosas se realizarán sin ser detectadas, eludiendo todos los niveles de seguridad de la red. A través de estos túneles DNS, los actores maliciosos pueden extraer registros financieros, números de la seguridad social, información de las tarjetas de crédito, de la propiedad intelectual y otros datos confidenciales. Estos paquetes de datos se cifran, se comprimen, se trocean y, a continuación, se transmiten fuera de la red.

¿QUÉ CONSECUENCIAS HAY PARA LA EMPRESA?

El impacto empresarial potencial de estas amenazas específicas es amplio. Según el Ponemon Institute, el coste asociado a la protección y corrección de un ataque se puede desglosar en cuatro centros de costes: asistencia técnica, pérdida de la productividad, pérdida de ingresos y perjuicio de la marca. En total, todos estos perjuicios pueden suponer más de 18 millones de dólares por ataque.[3] Llama la atención que el coste asociado al daño a la marca y a la reputación de la empresa ascienda a prácticamente 9,5 millones de dólares, el triple que los asociados al resto de categorías.[4] Si su empresa sufre una filtración de datos como resultado de un ataque específico, Ponemon estima que se tendrían que invertir otros 4 millones de dólares para mitigar los daños.[5] Entre los distintos gastos incurridos en dicho total se incluyen los relativos a la gestión de la crisis y de los clientes, la respuesta ante los incidentes, gastos de investigación y auditoría de seguridad, costes de renovación de los empleados y diversificación de talentos para contratar un nuevo director de seguridad de la información y personal de seguridad, impuestos e indemnizaciones legales y multas regulatorias.

Se calcula que la ciberdelincuencia supone actualmente un coste a la economía a nivel mundial de 450 000 millones de dólares, con un aumento previsto hasta los 600 000 millones para 2021.[6] En vista de esto, resulta mucho más imperativo que las empresas instalen defensas, soluciones en capas, productos y herramientas en sus actuales pilas de seguridad con objeto de reforzar las vulnerabilidades de red y los vectores de ataque conocidos, como el DNS recursivo.

DESAFÍO: PROTEGER ESTE VECTOR DE ATAQUE NO ES TAREA FÁCIL

Las soluciones de seguridad existentes suelen ser poco efectivas e inconsistentes a la hora de proteger la infraestructura de DNS recursivo. Las medidas de seguridad a nivel de red no son capaces de detectar la entrada de amenazas ni el filtrado de datos a través del DNS recursivo, ya que tienen su origen fuera del perímetro de la empresa. Productos como los firewalls, las puertas de enlace web segura, los antivirus y los servicios de inteligencia ante amenazas confían en gran medida en las listas negras, las actualizaciones manuales, los ajustes reactivos y la conformidad total por parte del usuario; y su eficacia va normalmente en consonancia con las bases de datos de proveedores.

Además, la mayoría de los servicios de seguridad solo inspeccionan los protocolos HTTP y HTTPS de los puertos 80 y 443. Los actores maliciosos son conscientes de ello y utilizan puertos y protocolos alternativos. Dada la tasa de evolución del malware y las medidas evasivas que utilizan los actores maliciosos para evitar ser detectados (el goteo constante, la suplantación de IP, los algoritmos de generación de dominios o el flat flux, por citar algunos), la mayoría de los mecanismos de defensa carecen de agilidad para adaptarse a esta gran variedad de amenazas quedando rápidamente obsoletos.

Quizás lo más complejo es el hecho de que las decisiones de seguridad de DNS se toman sin contexto. Dado el número y la variedad de solicitudes de DNS en su red (provenientes de portátiles, teléfonos móviles, equipos de escritorio, tabletas, impresoras, proyectores o Wi-Fi de invitados, por no mencionar todos los dispositivos "inteligentes" conectados), resulta complicado saber qué es lo habitual, incluso si se tienen recursos asignados para la supervisión y disección continuas de los registros de DNS. Esto se debe a que el tamaño de la muestra de su empresa es demasiado pequeño para detectar tráfico irregular de DNS de manera efectiva. Para identificar las amenazas de forma eficiente y constante, deberá conocer los patrones globales.

AKAMAI PROTEGE DE MANERA PROACTIVA A LA EMPRESA CON UN ENFOQUE DE SEGURIDAD BASADA EN LA NUBE SENCILLO, RÁPIDO Y CÓMODO

La nueva aplicación Akamai Enterprise Threat Protector protege proactivamente a su empresa frente a las amenazas específicas mediante la modificación de la configuración de DNS recursivo existente. Ya 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.

Enterprise Threat Protector es una solución en la nube rápida de configurar y fácil de implementar y de ampliar que no requiere hardware ni software adicional, y con tiempo de inactividad cero. Las reglas de las políticas de uso aceptable (PUA) y normativas de seguridad y actualizaciones se aplican unilateralmente en todas las sucursales, empleados y dispositivos en solo unos minutos. El portal en la nube agiliza la gestión que se realiza de forma centralizada. El panel de control proporciona información detallada del tráfico de DNS, los eventos asociados a amenazas y las actividades de PUA. Enterprise Threat Protector también integra otros productos de seguridad y herramientas de generación de informes, lo que permite a su empresa aprovechar al máximo las inversiones en todas las capas de su estrategia de "defensa en profundidad".

Y lo más importante, Enterprise Threat Protector se incluye en Akamai Intelligent Platform, avalada por la inteligencia en tiempo real de Akamai Cloud Security Intelligence (CSI). Nuestros amplios conocimientos sobre DNS, la total disponibilidad del acuerdo de nivel de servicio (SLA) y el avalado servicio AnswerX, junto a los datos obtenidos de gestionar el 30 % del tráfico web mundial y los más de 150 000 millones de solicitudes de DNS diarias se traducen en una visibilidad inigualable de las amenazas y del tráfico mundial y de poder ofrecer una protección sin precedentes para su empresa y los empleados.

¿Desea obtener más información sobre Enterprise Threat Protector? Puede consultar la información sobre el producto y una demostración del mismo en akamai.com/etp.

FUENTES

1. RSA Cybersecurity Poverty Index 2016, https://www.rsa.com/en-us/resources/rsa-cybersecurity-poverty-index-2016
2. https://www.av-test.org/en/statistics/malware/
3. Ponemon Institute: The Economic Impact of Advanced Persistent Threats, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03060USEN
4. Ibid
5. Ponemon Institute: 2016 Cost of a Data Breach Study, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN
6. Cybersecurity Ventures: 2016 Cybercrime Report, http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/