NO PERMITA QUE LOS ATACANTES UTILICEN DNS EN SU CONTRA

El sistema de nombres de dominio (DNS, por sus siglas en inglés) es imprescindible para la marcha de cualquier negocio moderno. Estén donde estén, sean grandes o pequeñas, vendan los productos que vendan y pertenezcan al sector al que pertenezcan, las organizaciones de hoy en día utilizan el protocolo DNS para convertir nombres de dominio inteligibles para las personas (p. ej., www.paloaltonetworks.com) en direcciones IP que pueda usar una máquina (en este caso, 199.167.52.137). Sin DNS, tendríamos que memorizar cadenas numéricas aleatorias, algo nada fácil para el cerebro humano. De un lado a otro del mundo, toda empresa moderna depende del tráfico DNS, por lo que los operadores de red no pueden bloquearlo y los cortafuegos tienen que dejarlo pasar. Sin DNS, las redes no funcionarían como es debido.

Muchos profesionales de la seguridad no saben lo fácil que resulta usar el sistema de nombres de dominio para llevar a cabo un ataque, ni lo común que es este fenómeno. De hecho, es frecuente que los equipos de seguridad no inspeccionen el tráfico DNS en busca de amenazas, ya que dan por supuesto que las consultas enviadas a través del protocolo DNS y el puerto 53 son benignas. Otras organizaciones no hacen inspecciones porque, al haber tantísimo tráfico DNS, buscar indicios de actividades sospechosas es como tratar de encontrar una aguja en un pajar. Habría que dedicar un tiempo y unos recursos que muchos consideran excesivos, sobre todo quienes piensan que el protocolo DNS no supone una gran amenaza.

La peligrosidad del protocolo DNS tiende a subestimarse, pero lo cierto es que ofrece una superficie de ataque enorme y puede utilizarse para la distribución de malware, las actividades de comando y control (C2) o la exfiltración de datos. Al estar en todas partes, puede utilizarse en distintas fases de un ataque. Según el equipo de investigación de amenazas de Palo Alto Networks, Unit 42, casi el 80 % del malware utiliza DNS para iniciar procedimientos de comando y control (C2). Los atacantes lo usan para crear canales de comando difíciles de desmantelar o detectar, pues resulta sumamente eficaz para mantener la conexión con los servidores DNS. Además, los ataques automáticos son cada vez más habituales, lo que hace prácticamente imposible descubrir o detener las amenazas.

A todo esto se suma que muchos equipos de seguridad no tienen controlado el tráfico DNS y desconocen que el protocolo DNS puede servir para controlar dispositivos infectados. El trabajo de estos equipos no es fácil. Por un lado, trabajan contra reloj para aplicar mecanismos de protección coherentes que sirvan de barrera frente a millones de dominios maliciosos nuevos; por otro, deben mantenerse al tanto de tácticas avanzadas como la tunelización de DNS. Todo el mundo usa el protocolo DNS, pero la facilidad para usarlo como vector de ataque lo hace muy peligroso. Hoy en día, el número de dominios maliciosos se multiplica a gran velocidad, y las firmas estáticas tardan demasiado en crearse. Si un sistema es víctima de una infección, los equipos responsables de la red y la seguridad tendrán dificultades para identificar y resolver el problema con rapidez. Para cuando lo hagan, es posible que el malware ya se haya propagado o que se haya producido un robo de datos.

80 %

Porcentaje del malware que utiliza DNS para iniciar procedimientos de comando y control (C2) con el fin de robar datos y propagar malware.

Figura 1: Investigaciones de Unit 42 sobre el tráfico DNS

Los tres tipos de ataques principales que utilizan DNS

Comprender las técnicas que pueden convertir DNS en un arma peligrosa es el primer paso para detener los ataques dirigidos a la red y reducir los riesgos de ciberseguridad. Los ciberdelincuentes usan principalmente tres métodos, mediante los cuales ocultan su actividad de comando y control con el fin de robar datos o distribuir malware.

Malware que utiliza DNS para realizar actividades de comando y control

Se trata de uno de los métodos de ataque DNS más habituales. Los ciberdelincuentes utilizan los protocolos de red más comunes, incluido el DNS, para propagar código malicioso. El vehículo elegido puede ser un anuncio en Internet o una URL maliciosa enviada por correo electrónico, aunque existen también otros medios. Una vez que el ordenador de un usuario está infectado, el sistema devuelve una solicitud DNS al servidor de control del atacante. Así, el ordenador infectado se convierte en un bot que el atacante puede controlar. A partir de ese momento, el malware ya puede robar datos personales o financieros, así como emitir instrucciones para analizar la red u otros ordenadores y propagarse con rapidez.

Hace poco, el grupo de hackers WINDSHIFT utilizó DNS para realizar un ciberataque de comando y control dirigido a organismos oficiales e infraestructuras importantes de Oriente Medio. Si desea obtener más información sobre los ataques de WINDSHIFT, Unit 42 ha publicado una investigación con todos los detalles técnicos y la secuencia de acontecimientos.

Los ataques que utilizan DNS son muy eficaces y su uso es cada vez más frecuente. El malware que utiliza algoritmos de generación de dominios (DGA) crece a un ritmo del

124 % anual.

Figura 2: Investigaciones de Unit 42 sobre los algoritmos de generación de dominios

Malware que utiliza algoritmos de generación de dominios

Los algoritmos de generación de dominios (DGA, por sus siglas en inglés) crean de forma aleatoria grandes cantidades de nombres de dominio ligeramente distintos. Son muy eficaces y su uso es cada vez más frecuente. Por poner un ejemplo, un algoritmo de este tipo podría crear miles de dominios al día similares a www.sujetospeligrosos.com. Los DGA surgieron precisamente para que el malware sea capaz de generar todos esos dominios, que luego se usan para actividades de comando y control. Unit 42 ha observado que el 18 % del malware utiliza esta técnica para crear automáticamente miles de dominios al día imposibles de bloquear, de los cuales quizá los atacantes solo lleguen a usar uno. Los dominios controlados por los atacantes permiten mover rápidamente los canales C2 de punto a punto, ya que son inmunes a medidas de seguridad tradicionales como las listas negras o los filtros de reputación web. Los ordenadores infectados, por su parte, se ponen en contacto con algunos de estos nuevos nombres de dominio para recibir comandos y actualizaciones. Algo que distingue a los DGA es que, aunque pueden generar miles de dominios en muy poco tiempo, no todos ellos tienen por qué estar registrados.

Esto oculta la ubicación de los centros de comando y control, lo que permite a los atacantes utilizarlos para el fraude financiero, el robo de identidades y otras actividades maliciosas. Si desea obtener más información sobre los algoritmos de generación de dominios, consulte el resumen sobre amenazas de Unit 42 dedicado a ellos.

Tunelización de DNS

Se trata de una técnica cada vez más habitual entre quienes usan amenazas avanzadas persistentes (APT, por sus siglas en inglés). Gracias a ella, los atacantes codifican sus cargas en una pequeña parte de las solicitudes DNS, lo que les permite eludir los controles de seguridad. Los más avezados recurren a la tunelización de DNS para ocultar el robo de datos o las actividades de comando y control en el tráfico DNS estándar. Una vez infectado, el dispositivo de la víctima envía una solicitud dentro del tráfico DNS. El servidor DNS recibe la orden de conectarse al servidor del ciberdelincuente, lo que crea un canal dedicado al robo y la transmisión de datos. Con la tunelización de DNS, las solicitudes DNS pasan a través del servidor DNS habitual, tanto dentro como fuera del cortafuegos de una empresa. Sin embargo, los datos tunelizados ocultos en las solicitudes DNS pasan inadvertidos. En los últimos años, varios grupos de ciberdelincuentes —entre ellos, OilRig— han utilizado la tunelización de DNS en innumerables ocasiones.

Investigación de Unit 42 sobre el grupo OilRig

OilRig es un grupo de ciberdelincuencia organizado descubierto por primera vez por Unit 42. Sigue en activo en la actualidad y actúa principalmente en Oriente Medio, donde elige cuidadosamente a las víctimas que mejor se ajustan a sus objetivos en la zona, se ha cebado en diversos sectores y ha llevado a cabo ataques a cadenas de suministro. Sus integrantes usan técnicas avanzadas de tunelización de DNS para robar datos y realizar actividades de comando y control, como las siguientes:

- El troyano ALMA Communicator, que se sirve de la tunelización de DNS para recibir comandos de los atacantes y exfiltrar datos. Ayudándose de determinados subdominios —creados para facilitar este tipo de ataque—, el malware envía datos al servidor de comando y control, así como a algunas direcciones IPv4. Del servidor C2, los datos se transmiten al troyano por medio de solicitudes DNS.
- El troyano Helminth, basado en PowerShell, repite una serie de consultas DNS en formato TXT cada 50 milésimas de segundo para obtener archivos de un servidor de comando y control. Así, va enviando malware a los sistemas de las víctimas mediante el protocolo DNS, en incrementos difíciles de detectar.

OilRig usa la tunelización de DNS para crear canales de comando y control fiables que le ayuden a sortear los mecanismos de defensa existentes para llevar sus ataques lo más lejos posible. Si desea obtener más información al respecto, consulte el Playbook Viewer —un visor interactivo de las campañas— o lea la serie de entradas del blog que ha publicado Unit 42 sobre OilRig.

Por qué los métodos de seguridad actuales ya no sirven

Las técnicas actuales para bloquear ataques de malware que utilizan DNS resultan inadecuadas por varios motivos. En primer lugar, existen muchas maneras de atacar a una organización por medio del protocolo DNS y es difícil abarcarlas todas. Muchas organizaciones se limitan a proteger su infraestructura DNS. En realidad es lógico, ya que si falla el sistema de nombres de dominio, se quedarán sin acceso a Internet. Sin embargo, olvidan algo no tan obvio: que el protocolo DNS también puede ser el arma elegida por los ciberdelincuentes para robar datos o propagar malware. Algunas no hacen nada al respecto y dejan vía libre a los atacantes. Muchas carecen de un sistema de supervisión DNS y bloquean únicamente los dominios maliciosos, ignorando el peligro que supone el malware basado en DNS.

Otros equipos de seguridad consultan fuentes de información sobre amenazas relativamente estáticas y crean listas negras para bloquear los ataques provenientes de dominios maliciosos conocidos. No obstante, esta técnica ya no da tan buenos resultados ahora que el malware utiliza algoritmos de generación de dominios con más frecuencia. Cuando se utiliza una lista de dominios generados aleatoriamente para actividades de comando y control, las herramientas obsoletas y los métodos de seguridad tradicionales se ven desbordados y no pueden generar las firmas necesarias. Los ataques basados en DNS se han convertido en un fenómeno de tal envergadura que es inútil tratar de combatirlos con unas cuantas firmas.

Además, el uso de listas fijas no da a los responsables de seguridad el contexto que necesitan para entender por completo los ataques dirigidos a la red. Aunque las fuentes de inteligencia sobre amenazas se actualizan periódicamente (a diario o incluso cada hora) con indicadores o artefactos de terceros, este ritmo se queda corto ante la ingente cantidad de datos que genera el tráfico DNS. A menudo, el volumen de tráfico es tan elevado que los equipos de seguridad carecen de visibilidad o recursos para inspeccionarlo a fondo y determinar si contiene elementos peligrosos. Un enfoque tradicional no les permitirá ser proactivos ni mejorar progresivamente su seguridad DNS.

Para protegerse, algunas organizaciones utilizan productos independientes que, si bien pueden resultar adecuados para mejorar aspectos concretos de la seguridad DNS, tienen sus limitaciones. Es algo que sucede hasta con las mejores tecnologías. Por ejemplo, para que estas herramientas funcionen con eficacia, a menudo hay que hacer cambios en la infraestructura DNS. El uso de productos dispares también aísla la inteligencia y los datos sobre amenazas, lo que tal vez dificulte su uso en otras áreas de la estructura de seguridad de la organización. Si cada herramienta genera sus propios datos, los equipos acusarán la falta de coordinación y se verán desbordados. Tener que gestionar distintas herramientas desvinculadas entre sí complicará el trabajo de empleados que ya antes no daban abasto.

No permita que los atacantes utilicen DNS en su contra

¿Quiere saber cómo recuperar el control de su tráfico DNS e impedir que los atacantes utilicen DNS para dañar su organización?
Esto es lo que necesita:

- **Grandes cantidades de datos de seguridad:** recopile la mayor cantidad posible de datos de seguridad, bien por su cuenta, bien por medio de otras fuentes de inteligencia sobre amenazas u organizaciones dedicadas a la ciberseguridad. Los datos y la inteligencia aportados por una comunidad cada vez más numerosa le ayudarán a protegerse cada vez mejor.
- **Análisis y aprendizaje automático:** una vez obtenidos los datos, sus equipos de seguridad deberán analizarlos. Dado que los dominios y la tunelización de DNS son dinámicos por naturaleza, usar el aprendizaje automático es la única forma de identificar sobre la marcha los dominios maliciosos que aún no han salido a la luz. Sin la ayuda del análisis, es imposible prever de forma dinámica qué dominios podrían llegar a usarse para un ataque. Los análisis de comportamiento también pueden servir para determinar el nivel básico de actividad, comprender los patrones generales y determinar qué actividades se consideran normales. Cuando quienes velan por la seguridad de su organización ven algo que les obliga a actuar, el análisis es lo que determina si la acción debe ser automática o manual. Los análisis también permiten comprender qué señales no se pueden ignorar, lo que ayuda a los equipos a distribuir mejor su tiempo y sus recursos.

- **Uso de un cortafuegos de nueva generación integrado que automatice la respuesta:** dada la rapidez con la que se producen muchos ataques basados en DNS, los equipos de seguridad deberían dedicar menos tiempo a responderlos de forma manual. La automatización es la única defensa válida, pues ayuda a determinar muy pronto qué equipos están infectados, a tomar las medidas oportunas sin intervención manual y a contener las amenazas antes de que se propaguen a otras zonas de la red. Los equipos de seguridad necesitan herramientas novedosas que se integren con la infraestructura de seguridad existente y aporten valor añadido sin complicar las operaciones.
- **Protección basada en la nube:** la nube permite ampliar las medidas de protección DNS de forma ilimitada y mantenerlas siempre actualizadas, lo que la convierte en un punto de control fundamental para la detención de ataques que utilizan DNS. Gracias a las novedades que ofrece, los responsables de seguridad pueden desarrollar e implementar nuevas técnicas de detección, así como aprovecharlas de inmediato en su organización. Además, los mecanismos de protección basados en la nube se actualizan al instante, sin que nadie intervenga ni haga cambios en el software, lo que aligera la carga de trabajo de los equipos de los centros de operaciones de seguridad.
- **No más productos independientes:** por último, es importante que los equipos de seguridad dejen de implementar herramientas dispares y mal integradas (o que obliguen a modificar el enrutamiento DNS). En muchos casos, se trata de productos que no están pensados para la automatización, que obligan a los analistas a recopilar manualmente información de muchas fuentes inconexas antes de actuar y que, al no compartir automáticamente datos ni información útil, impiden coordinar la emisión de alertas en todo el entorno de seguridad. Debido a todo esto, los equipos tardan más en responder a las amenazas, ya que no es posible adoptar una estrategia de protección global.

Prácticas recomendadas de seguridad DNS

Implementar la tecnología adecuada no es la única forma de proteger la red de las amenazas que utilizan DNS. Su organización también puede adoptar estas prácticas recomendadas:

- Ponga en marcha un plan de formación y concienciación en materia de seguridad. Enseñe a los empleados a reconocer correos electrónicos sospechosos y a no hacer clic en cualquier enlace sin pensar que tal vez contenga malware. Háblele del phishing para que aprendan a evitar los ataques por correo electrónico, o a reconocerlos y dar la voz de alarma cuando se produzcan.
- Familiarícese con todos los riesgos que existen y cree un programa de inteligencia sobre amenazas que le ayude a comprender las técnicas de ataque. Toda esta información le permitirá saber si cuenta con la tecnología adecuada para proteger su red.
- No preste atención únicamente al tráfico DNS. De poco sirve recopilar logs DNS sin saber qué son ni cómo interpretarlos, o qué medidas ayudan a proteger la red para que los ataques basados en DNS no le hagan mella.
- No piense que un cliente DNS es necesariamente fiable. Si un ciberdelincuente se adueña de un servidor DNS, este podría enviar respuestas falsas para desviar el tráfico a otros sistemas infectados u orquestar un ataque de interposición del tipo «man-in-the-middle».
- Dé indicaciones claras a los trabajadores itinerantes. Los empleados itinerantes ponen en peligro una gran cantidad de datos empresariales. Pida a quienes trabajan a distancia que no utilicen redes inalámbricas desprotegidas, gratuitas o públicas, ya que alguien podría meterse fácilmente entre los empleados y el punto de conexión. Incorpore un sistema de autenticación multifactor. El riesgo de robo o pérdida de dispositivos es muy elevado. Acéptelo y prepare un plan de actuación.
- Aunque un producto prometa solucionar todos sus problemas de seguridad, úselo en combinación con otros. La protección de redes exige un enfoque global, así que hágase con un arsenal de herramientas adecuado para combatir las amenazas modernas, evalúe sus funciones y averigüe si pueden combinarse de manera eficaz. Para poder combatir distintas amenazas, es importante contar con funciones como la prevención de intrusiones, el filtrado de URL y el bloqueo de archivos, entre otras.
- Combine las alertas con un sistema de respuesta automática. Las amenazas avanzan tan rápido que las alertas o señales de anomalía no sirven de mucho. Un analista que recibe una alerta debe evaluar su importancia, confirmar que la amenaza es real, identificarla y determinar su origen. Para cuando termine, es posible que el robo o la infección ya hayan ocurrido. Es importante que las herramientas de seguridad que utilice detecten las amenazas de forma automática y pongan en cuarentena los sistemas que hayan podido verse afectados antes de que el problema se agrave.

¿Se ajusta la estrategia de seguridad DNS de su organización a las prácticas recomendadas? Para asegurarse, solicite una evaluación de prácticas recomendadas Best Practice Assessment.

Oval Tower
De Entrée 99 -179
1101HE Ámsterdam
Países Bajos
Tel.: +31 20 888 1883
www.paloaltonetworks.es

stop-attackers-from-using-dns-against-you-wp-040219-es