Ataque SAD DNS

BCSC_ALERTA_SAD_DNS

TLP:WHITE

www.basquecybersecurity.eus

Noviembre 2020

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

RESUMEN EJECUTIVO

Investigadores de las Universidades de California y Tsinghua han publicado una serie de fallos de seguridad en el protocolo DNS que recuerdan al fallo descubierto por Dan Kaminsky, y que fue considerado como uno de los fallos más graves de Internet.

En 2008, Kaminsky descubrió una vulnerabilidad, que afectaba al protocolo DNS, básico en toda la arquitectura de Internet, y que permitía a los posibles atacantes comprometer los servidores de nombres pudiendo redirigir cualquier petición hacia una dirección a sitios falsos. Este ataque fue conocido como DNS cache poisoning attack y mitigado mediante un parche emitido en ese mismo año.

Este nuevo ataque se ha denominado **"SAD DNS" o "Side-channel Attacked DNS"** y consiste en la identificación del puerto UDP abierto por el cliente con el servidor para la resolución de un nombre. Para falsear una petición DNS, un atacante necesita conocer el TXID (ID de transacción) y el puerto origen UDP.

SAD DNS se aprovecha de un parámetro utilizado para no saturar las respuestas ICMP, el límite máximo de respuestas de "error puerto cerrado" ante peticiones ICMP para consultar puertos UDP.

Se han publicado varias posibles soluciones que se recogen en el apartado Mitigación / Solución.

ANÁLISIS TÉCNICO

El protocolo **DNS (Domain Name Systems**) es una parte esencial de Internet, que realiza la tarea de traducir nombres en direcciones IP. Actualmente, además, ofrece características para la securización de las comunicaciones y es parte imprescindible en la emisión de certificados TLS, que se adquieren asociados actualmente a nombres de dominio.

DNS es también, además de un protocolo, el sistema que define la jerarquía de los equipos que manejan todos los datos relaciones con los nombres en una red.

Los mensajes DNS utilizan mayoritariamente el protocolo de transporte UDP y dado que UDP es un protocolo no orientado a conexión y no autenticado, cualquiera puede enviar respuestas mediante la falsificación de la dirección y puerto utilizados.

Para reforzar la seguridad ante la inseguridad que ofrece UDP, DNS incorpora dentro de su mensaje, en los dos primeros bytes, un campo denominado Transaction ID (TxID) el cual debe ser igual tanto en la petición como en la respuesta:

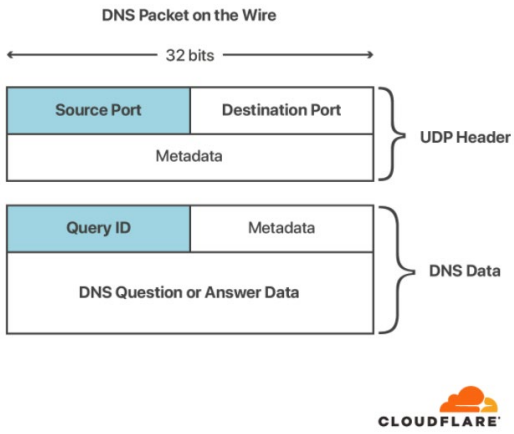

Figura 1. Descripción paquete DNS encapsulado en UDP

Por tanto, para que un atacante pueda falsear una petición DNS necesitará dos datos: el puerto UDP abierto en el servidor por el cliente al realizar la petición y el TxID, cada uno de ellos con un tamaño de 16 bits. En la figura 1 se pueden observar en azul estos dos campos dentro del paquete DNS. Esto hace un total de 32 bits a obtener por parte del atacante para tener éxito.

Antes del descubrimiento de **Kaminsky en 2008 del DNS cache poisoning attack**, los sistemas de resolución recursiva utilizaban típicamente el puerto 53 para el envío y recepción de mensajes. Debido a esto, la única variable que necesitaba adivinar un atacante eran los 16 bits que componen el TxID.

El mecanismo del DNS cache poisoning attack consistía en aprovechar mientras un resolutor recursivo consultase el servidor de nombres autorizado de un dominio determinado, para inundar a dicho resolutor con respuestas DNS para los 65 mil (2^{16}) o más posibles TxID. Si la respuesta maliciosa con el TxID correcto

llegaba antes que la del servidor autorizado, entonces la memoria caché del DNS quedaría envenenada. Así se devolvía la respuesta falseada elegida por el atacante en lugar de la real durante el tiempo de vida de la respuesta DNS (TTL).

Para solucionar este problema, se comenzó a implementar en los resolutores DNS la aleatorización del puerto origen de modo que se requiriese obtener, no sólo el TxID si no también el puerto UDP. Con ello, las posibilidades pasaron de unas decenas de miles a un billón ($2^{16}+2^{16}$) lo que hacía el ataque inviable.

En la RFC 5452 se publicaron, además, métodos para reforzar DNS y dificultar la obtención de los datos.

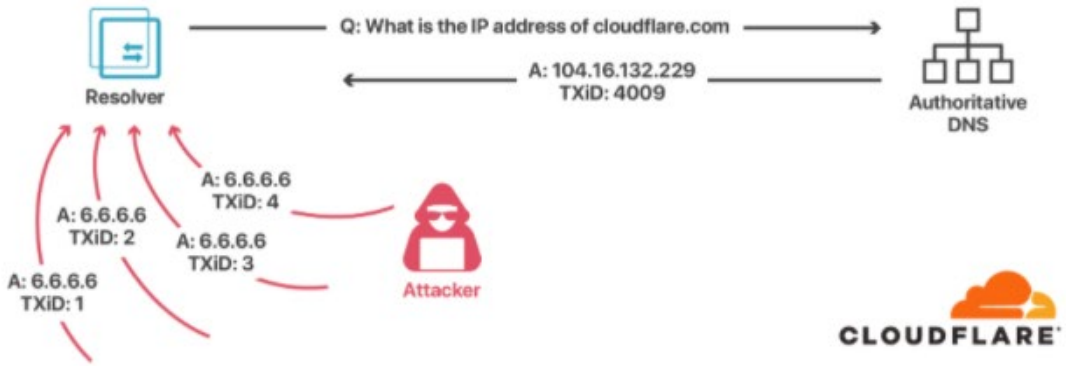

Figura 2. DNS cache poisoning attack - Cloudfare

La reciente publicación de las **Universidades de California y Tsinghua** reporta y analiza una debilidad del software, a la que se ha denominado **SAD DNS** (por sus siglas en inglés **Side-channel Attacked DNS**), utilizado en la infraestructura DNS que permitiría obtener el puerto UDP utilizado para la conexión. Esto dejaría de nuevo en la posición en que sólo es necesario lograr obtener el TxID (16 bits) en vez de los dos parámetros.

Si se quisiera obtener el puerto abierto, lo más fácil sería escanear todos los puertos UDP y ver cuál de ellos está abierto. No obstante, esto lleva demasiado tiempo y para cuando se terminase el escaneo, dicho puerto estaría obsoleto.

El método que utiliza SAD DNS, se basa en aprovecharse del límite que establece el servidor a las respuestas ICMP de “error puerto cerrado”. Este límite se establece para proteger de saturación el servidor y se implementa actualmente en todos los Sistemas Operativos. Este límite fija el número máximo de respuestas “error puerto cerrado” que se van a recibir.

Los investigadores de California y Tsinghua centran su análisis en servidores Linux, al ser los más ampliamente utilizados. En Linux existen dos límites a los paquetes de error ICMP, uno global y otro por IP. El límite por defecto de la tasa por IP es de 1 por segundo y de 1000 el caso de la tasa global (en ráfagas de máximo 50).

Es posible aprovechar la técnica IP spoofing para evitar la tasa por IP y utilizar el límite global para descubrir si las sondas falsas han encontrado un puerto origen correcto o no (es decir, si han tenido respuestas de “error puerto cerrado” o no) mediante lo siguientes pasos:

1- Se envía el número máximo de peticiones (1000/segundo) hacia el DNS Resolver víctima desde direcciones IP falseadas. En realidad, debido al límite de ráfagas de 50, se realiza en bloques de 50 cada 20ms.
2- Dado que las direcciones IP están falseadas, el atacante no va a ver las respuestas, pero eso no importa. Antes de terminar el rango de tiempo para esa ráfaga se envía una petición a un puerto UDP cualquiera que se sabe si está cerrado.
3- Si se recibe un error ICMP de “puerto cerrado” significa que no se ha alcanzado el límite, por tanto, en el rango había al menos un puerto UDP abierto.
4- De este modo, mediante tandas de consultas, se va comprobando si se alcanza o no el límite, con lo que se deducirá qué puertos están abiertos.

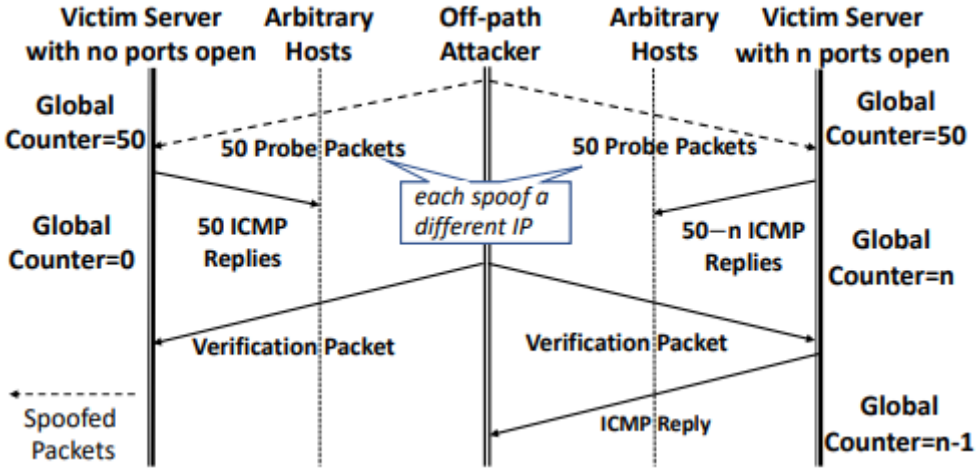

Figura 3. Esquema del ataque, publicado en el paper original.

RECURSOS AFECTADOS

Este fallo afecta a los sistemas operativos Linux (kernel 3.18-5.10), Windows Server 2019 (versión 1809) y posteriores, macOS 10.15 y posteriores, y FreeBSD 12.1.0 y posteriores.

Según indican los investigadores, los principales servicios DNS de Internet, como Google y Cloudfare se ven afectados por el fallo, así como un alto porcentaje de los resolvers abiertos.

MITIGACIÓN / SOLUCIÓN

Se han publicado varias posibles opciones para la mitigación del ataque SAD DNS:

- Bloqueo de los mensajes salientes ICMP “puerto cerrado”.
- Utilización de DNSSEC (Domain Name System Security Extensions) que añade una comprobación de integridad y autenticidad al protocolo DNS, con lo cual se previenen los ataques de suplantación y falsificación. Servidores que implementen DNSSEC no son vulnerables al ataque SAD DNS. No obstante, el uso de DNSSEC aún no está ampliamente extendido.

  Guía de implantación y buenas prácticas de DNSSEC – Incibe-CERT
- Recientemente se ha publicado una actualización del Kernel de Linux específica para mitigar este ataque que utiliza límites de la tasa global de mensajes “error puerto cerrado” aleatorios e impredecibles.

REFERENCIAS ADICIONALES

- Paper original con la publicación de la investigación del análisis – Universidades de California y Tsinghua
- Cloudfare – SAD DNS Explained
- RFC 5452
- Hackplayers – SAD DNS
- Incibe – DNSSEC Asegurando la integridad y autenticicad de tu dominio web

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?