Investigadores israelíes de seguridad cibernética revelaron los detalles sobre una nueva falla que afecta el protocolo DNS que se puede explotar para lanzar ataques de denegación de servicio (DDoS) amplificados y a gran escala para eliminar sitios web específicos.

Llamado NXNSAttack, la falla depende del mecanismo de delegación de DNS para obligar a los solucionadores de DNS a generar más consultas DNS a los servidores autorizados de elección del atacante, lo que podría causar una interrupción a escala de botnet en los servicios en línea.

> *«Mostramos que el número de mensajes DNS intercambiados en un proceso de resolución típico podría ser mucho mayor en la práctica de lo que se espera en teoría, principalmente debido a una resolución proactiva de las direcciones IP de los servidores de nombres»,* según los investigadores.
>
> *«Mostramos cómo esta ineficiencia se convierte en un cuello de botella y podría usarse para montar un ataque devastador contra uno o ambos, resolutivos recursivos y servidores autorizados»,* agregaron.

Después de la divulgación responsable de NXNSAttack, varias de las compañías a cargo de la infraestructura de Internet, incluidas PowerDNS (CVE-2020-10995), CZ.NIC (CVE-2020-12667), Cloudflare, Google, Amazon, Microsoft, Dyn de Oracle, Verisign e IBM Quad9, parchearon su software para solucionar el problema.

La infraestructura DNS estuvo previamente en el extremo receptor de una serie de ataques DDoS a través de la botnet Mirai, incluidos aquellos contra el servicio Dyn DNS en 2016, paralizando algunos de los sitios más grandes del mundo, incluidos Twitter, Netflix, Amazon y Spotify.

Método NXNSAttack

Una búsqueda DNS recursiva ocurre cuando un servidor DNS se comunica con varios servidores DNS autorizados en una secuencia jerárquica para ubicar una dirección IP asociada con un dominio (por ejemplo, google.com), y devolverla al cliente.

Esta resolución generalmente comienza con la información DNS controlada por sus ISP o servidores DNS públicos, como Cloudflare (1.1.1.1) o Google (8.8.8.8), lo que esté configurado en el sistema.

La resolución pasa la solicitud a un servidor de nombres DNS autorizado si no puede localizar la dirección IP de un nombre de dominio determinado.

Pero si el primer servidor de nombre DNS autorizado tampoco contiene los registros deseados, devuelve el mensaje de delegación con direcciones a los servidores autorizados a los que puede consultar el solucionador DNS.

Dicho de otra forma, un servidor autorizado le dice al solucionador recursivo: *«No sé la respuesta, vaya y consulte estos y estos servidores de nombres, por ejemplo, ns1, ns2, etc».*

Este proceso jerárquico sigue hasta que el solucionador DNS llega al servidor autorizado correcto que proporciona la dirección IP del dominio, lo que permite al usuario acceder al sitio web deseado.

Los investigadores descubrieron que estos grandes gastos generales no deseados se pueden explotar para engañar a los resolutivos recursivos para que envíen de forma contundente una gran cantidad de paquetes a un dominio objetivo en lugar de servidores legítimos autorizados.

Para organizar el ataque por medio de un resolutor recursivo, el atacante debe estar en

posesión de un servidor autorizado, según los investigadores.

> *«Esto se puede lograr fácilmente al comprar un nombre de dominio. Un adversario que actúa como un servidor autorizado puede diseñar cualquier respuesta de referencia NS como respuesta a distintas consultas DNS»,* dijeron los investigadores.

El NXNSAttack funciona enviando una solicitud de un dominio controlado por el atacante a un servidor de resolución DNS vulnerable, que reenviaría la consulta DNS al servidor autorizado controlado por el hacker.

En lugar de devolver las direcciones a los servidores autorizados reales, el servidor autorizado controlado por el atacante responde a la consulta DNS con una lista de nombres de servidor falsos o subdominios controlados por el actor de la amenaza que apunta a un dominio DNS víctima.

El servidor DNS después reenvía la consulta a todos los subdominios inexistentes, creando un aumento masivo en el tráfico al sitio de la víctima.

Los investigadores aseguran que el ataque puede amplificar la cantidad de paquetes intercambiados por el solucionador recursivo hasta en un factor de más de 1620, abrumando no solo a los que resuelven DNS con más solicitudes que pueden manejar, sino también inundando el dominio objetivo con solicitudes superfluas y descargarlo.

Además, utilizar una botnet como Mirai en función de cliente DNS, puede aumentar más la escala del ataque.

> *«Controlar y adquirir un gran número de clientes y un gran número de NS autorizados por un atacante es fácil y barato en la práctica»,* dijeron los investigadores.

> *«Nuestro objetivo inicial era investigar la eficiencia de los resolutivos recursivos y su comportamiento bajo diferentes ataques, y terminamos encontrando una nueva vulnerabilidad seria, el NXNSAttack»*, agregaron.

Es recomendable que los administradores de red que ejecuten sus propios servidores DNS, actualicen su software de resolución DNS a la última versión.

> *«Los ingredientes clave del nuevo ataque son (I), la facilidad con la que uno puede poseer o controlar un servidor de nombre autorizado, (II), el uso de nombres de dominio inexistentes para servidores de nombres, y (III), la redundancia adicional colocada en la estructura DNS para lograr tolerancia a fallas y tiempo de respuesta rápido».*