El grupo de amenazas conocido como ChamelGang ha sido detectado utilizando un implante previamente desconocido para infiltrar sistemas Linux, lo que representa una nueva ampliación de las capacidades de este grupo de amenazas.

El malware, denominado ChamelDoH por Stairwell, es una herramienta basada en C++ que permite la comunicación a través de túneles DNS-over-HTTPS (DoH).

ChamelGang fue revelado por primera vez por la empresa de ciberseguridad rusa Positive Technologies en septiembre de 2021, detallando sus ataques contra la industria de producción de combustible, energía y aviación en Rusia, Estados Unidos, India, Nepal, Taiwán y Japón.

Las cadenas de ataque utilizadas por este grupo han aprovechado vulnerabilidades en servidores de Microsoft Exchange y Red Hat JBoss Enterprise Application para obtener acceso inicial y llevar a cabo ataques de robo de datos mediante una puerta trasera pasiva llamada DoorMe.

> *«Se trata de un módulo nativo de IIS que se registra como un filtro a través del cual se procesan las solicitudes y respuestas HTTP. Su funcionamiento es peculiar: la puerta trasera solo procesa las solicitudes en las que se establece correctamente el parámetro de la cookie»,* mencionó Positive Technologies en ese momento.

En cuanto a la puerta trasera para Linux descubierta por Stairwell, ha sido diseñada para recopilar información del sistema y tiene la capacidad de realizar operaciones de acceso remoto, como carga, descarga y eliminación de archivos, así como ejecución de comandos de shell.

Lo que hace que ChamelDoH sea especial es su método innovador de comunicación

mediante el uso de DoH, que se utiliza para realizar resoluciones del Sistema de Nombres de Dominio (DNS) a través del protocolo HTTPS, y enviar solicitudes de DNS TXT a un servidor de nombres malicioso.

> *«Debido a que estos proveedores de DoH son servidores DNS ampliamente utilizados [como Cloudflare y Google] para tráfico legítimo, no se pueden bloquear fácilmente a nivel empresarial»,* dijo Daniel Mayer, investigador de Stairwell.

El uso de DoH para el control y comando (C2) también brinda ventajas adicionales al actor de amenazas, ya que las solicitudes no pueden ser interceptadas mediante un ataque de intermediario (AitM) debido al uso del protocolo HTTPS.

Esto también implica que las soluciones de seguridad no pueden detectar ni prohibir las solicitudes maliciosas de DoH y cortar las comunicaciones, lo que convierte este método en un canal cifrado efectivo entre un host comprometido y el servidor C2.

> *«El resultado de esta táctica es similar a la ocultación del control y comando detrás de un dominio legítimo, donde el tráfico se envía a un servicio legítimo alojado en una red de distribución de contenido (CDN), pero se redirige al servidor C2 a través del encabezado 'Host' de la solicitud; tanto la detección como la prevención resultan difíciles»,* explicó Mayer.

La empresa de ciberseguridad con sede en California informó que detectó un total de 10 muestras de ChamelDoH en la base de datos de malware de VirusTotal, una de las cuales se subió el 14 de diciembre de 2022.

Los últimos hallazgos demuestran que *«el grupo también ha dedicado un tiempo considerable y ha realizado un gran esfuerzo para investigar y desarrollar un conjunto de herramientas igualmente sólido para las intrusiones en sistemas Linux»,* dijo Mayer.