Investigadores de seguridad cibernética lograron detener este jueves una operación de fraude cibernético en curso, liderada por hackers en Gaza, Cisjordania y Egipto, para comprometer los servidores VoIP de más de 1200 organizaciones en 60 países durante los últimos 12 meses.

Según los hallazgos publicados por Check Point Research, los actores de la amenaza, que se cree que están ubicados en la Franja de Gaza palestina, apuntaron a Sangoma PBX, una interfaz de usuario de código abierto que se utiliza para administrar y controlar los sistemas telefónicos VoIP de Asterisk, particularmente los servidores del Protocolo de Inicio de Sesión (SIP).

> *«Hackear servidores SIP y obtener el control permite a los hackers abusar de ellos de distintas formas. Una de las formas más complejas e interesantes es abusar de los servidores para realizar llamadas telefónicas salientes, que también se utilizan para generar ganancias. Hacer llamadas es una función legítima, por lo que es difícil detectar cuándo se ha explotado un servidor»,* dijo la compañía en su análisis.

Al vender números de teléfono, planes de llamadas y acceso en vivo a servicios VoIP comprometidos de empresas específicas a los mejores postores, los operadores de la campaña han generado cientos de miles de dólares en ganancias, además de equiparlos con capacidades para espiar llamadas legítimas.

## Explotación de vulnerabilidad de omisión de autenticación de administrador remoto

PBX, abreviatura de Intercambio de Sucursales Privadas, es un sistema de conmutación que se utiliza para establecer y controlar llamadas telefónicas entre puntos finales de telecomunicaciones, como teléfonos habituales, destinos en la red telefónica pública conmutada (PSTN) y dispositivos o servicios VoIP.

La investigación de Check Point encontró que el ataque explota la vulnerabilidad CVE-2019-19006, un defecto crítico que afecta la interfaz web del administrador de FreePBX y PBXact, lo que potencialmente permite a los usuarios no autorizados obtener acceso de administrador al sistema mediante el envío de paquetes especialmente diseñados al servidor afectado.

La falla de omisión de autenticación de administrador remoto afecta a las versiones 15.0.16.26 y anteriores de FreePBX, 14.0.13.11 y anteriores, y 13.0.197.13 y anteriores, y fue parcheada por Sangoma en noviembre de 2019.

> *«El ataque comienza con SIPVicious, una popular suite de herramientas para auditar sistemas VoIP basados en SIP. El atacante usa 'svmapmodule' para escanear Internet en busca de sistemas SIP que ejecuten versiones vulnerables de FreePBX. Una vez encontrado, el atacante explota CVE-2019-19006, obteniendo acceso de administrador al sistema»,* dijeron los investigadores.

En un flujo de ataque, se descubrió que se utilizó un shell web PHP inicial para hacerse con la base de datos del sistema FreePBX y las contraseñas para distintas extensiones SIP, lo que les otorgaba a los atacantes acceso sin restricciones a todo el sistema y la capacidad de realizar llamadas desde cada extensión.

En la segunda versión del ataque, se utilizó el shell web inicial para descargar un archivo PHP codificado en base64, que luego se decodifica para iniciar un panel web que permite al adversario realizar llamadas utilizando el sistema comprometido con compatibilidad con FreePBX y Elastix, además de ejecutar comandos arbitrarios y codificados.

La campaña en Pastebin para descargar shells web protegidos con contraseña ha vinculado el ataque a un cargador con el nombre de «INJ3CTOR3», cuyo nombre a la vez está vinculado a una antigua vulnerabilidad de ejecución remota de código SIP (CVE-2020-7235), además de un número de grupos privados de Facebook que se utilizan para compartir exploits del servidor SIP.

Los investigadores aseguran que los atacantes podrían emplear los servidores VoIP pirateados para realizar llamadas a números de tarifa premium internacionales (IPRN) bajo su control. Los IPRN son números especializados que utilizan las empresas para ofrecer compras telefónicas y otros servicios, como poner en espera a las personas que llaman, por una tarifa más alta.

Esta tarifa por lo general se transfiere a los clientes que realizan las llamadas a los números premium, lo que lo convierte en un sistema listo para el abuso. Por lo tanto, cuantas más llamadas reciba el propietario de una IPRN y más esperen los clientes en la fila para completar la transacción, más dinero podrá cobrar a los proveedores y clientes de telecomunicaciones.

> *«El uso de programas IPRN no solo permite al hacker realizar llamadas, sino también abusar de los servidores SIP para generar ganancias. Cuantos más servidores se exploten, más llamadas a la IPRN se pueden realizar»*, dijeron los investigadores.

Esta no es la primera vez que los sistemas de conmutación se aprovechan para el fraude internacional de reparto de ingresos (IRSF), la práctica de obtener acceso ilegalmente a la red de un operador para inflar el tráfico a números de teléfono obtenidos de un proveedor de IPRN.

> *«Nuestra investigación revela cómo los piratas informáticos en Gaza y Cisjordania están ganando dinero, dadas las terribles condiciones socioeconómicas en los territorios palestinos»,* dijo Adi Ikan, jefe de investigación de ciberseguridad de redes en Check Point.

> *«Su operación de fraude cibernético es una forma rápida de ganar grandes sumas de dinero rápidamente. En términos más generales, estamos viendo un fenómeno*

> *generalizado de piratas informáticos que utilizan las redes sociales para escalar la piratería y la monetización de los sistemas VoIP este año».*