Investigadores de seguridad cibernética explicaron los detalles de una botnet sofisticada y multifuncional peer-to-peer (P2P) escrita en GoLang, que ha estado apuntando activamente a servidores SSH desde enero de 2020.

Conocida como FritzFrog, la red de bots modular, multiproceso y de archivos, ha violado más de 500 servidores hasta ahora, infectando universidades conocidas en Estados Unidos y Europa, y una compañía ferroviaria, según el informe de Guardicore Labs.

> *«Cuenta con una infraestructura descentralizada, que distribuye el control entre todos sus nodos. En esta red sin un solo punto de falla, los pares se comunican constantemente entre sí para mantener la red viva, resistente y actualizada»*, dijo Ophir Harpaz, de Guardicore.

Además de implementar un protocolo P2P patentado que se ha escrito desde cero, las comunicaciones se realizan a través de un canal cifrado, con el malware capaz de crear una puerta trasera en los sistemas de las víctimas que otorga acceso continuo a los atacantes.

Aunque se han observado redes de bots basadas en GoLang, como Gandalf y GoBrut, FritzFrog parece compartir algunas similitudes con Rakos, otra puerta trasera de Linux basada en GoLang que se descubrió que se infiltraba en los sistemas de destino por medio de intentos de fuerza bruta en los inicios de sesión SSH.

Pero una característica propia de FritzFrog, es que no tiene archivos, lo que significa que ensambla y ejecuta cargas útiles en la memoria, y es más agresivo al llevar a cabo ataques de fuerza bruta, al mismo tiempo que es eficiente al distribuir los objetivos de forma uniforme dentro de la botnet.

Una vez que se identifica una máquina objetivo, el malware realiza una serie de tareas que implican forzarla, infectar la máquina con cargas maliciosas en caso de una infección exitosa y agregar a la víctima a la red P2P.

Para pasar desapercibido, el malware se ejecuta como ifconfig y NGINX, y comienza a escuchar en el puerto 1234 para recibir más comandos para su ejecución, incluidos aquellos para sincronizar a la víctima con la base de datos de pares de la red y objetivos de fuerza bruta.

Los propios comandos se transmiten al malware a través de una serie de aros diseñados para evitar la detección. El nodo atacante en la botnet primero se engancha a una víctima específica a través de SSH y luego usa la utilidad NETCAT para establecer una conexión con un servidor remoto.

Además, los archivos de carga útil se intercambian entre nodos al estilo BitTorrent, empleando un enfoque de transferencia de archivos segmentados para enviar blobs de datos.

> *«Cuando un nodo A desea recibir un archivo de su par, el nodo B, puede consultar al nodo B qué blobs posee mediante el comando getblobstats. Entonces, el nodo A puede obtener un blob específico por su hash, ya sea mediante el comando P2P getbin o mediante HTTP, con la URL 'https://node_IP:1234/blob_hash'. Cuando el nodo A tiene todos los blobs necesarios, ensambla el archivo usando un módulo especial llamado Ensamblar y lo ejecuta»*, dijeron los investigadores.

Aparte de la codificación de las respuestas de los comandos, el programa malicioso ejecuta un proceso separado, llamado *libexec*, para minar la criptomoneda Monero y deja una puerta trasera para el futuro acceso mediante la adición de una clave pública.

La campaña comenzó el 9 de enero, según la compañía de seguridad, antes de alcanzar un acumulado de 13 mil ataques desde su primera aparición, que abarcan 20 versiones diferentes del binario de malware.

Además de apuntar a las instituciones educativas, se ha descubierto que FritzFrog aplica la fuerza bruta a millones de direcciones IP que pertenecen a organizaciones gubernamentales, centros médicos, bancos y empresas de telecomunicaciones.

Guardicore Labs también puso a disposición un script de detección que verifica si un servidor ha sido infectado por FritzFrog, junto con compartir los otros indicadores de compromiso (IoC).

> *«Las contraseñas débiles son el facilitador inmediato de los ataques de FritzFrog. Recomendamos elegir contraseñas seguras y usar autenticación de clave pública, que es mucho más seguro. Los enrutadores y los dispositivos de IoT a menudo exponen SSH y, por lo tanto, son vulnerables a FritzFrog, considere cambiar su puerto SSH o deshabilitar completamente el acceso SSH a ellos si el servicio no está en uso»,* concluyó Harpaz.