El actor de amenazas vinculado a un botnet de tipo peer-to-peer (P2P) denominado FritzFrog ha reaparecido con una variante reciente que utiliza la vulnerabilidad Log4Shell para propagarse internamente en una red que ya ha sido comprometida.

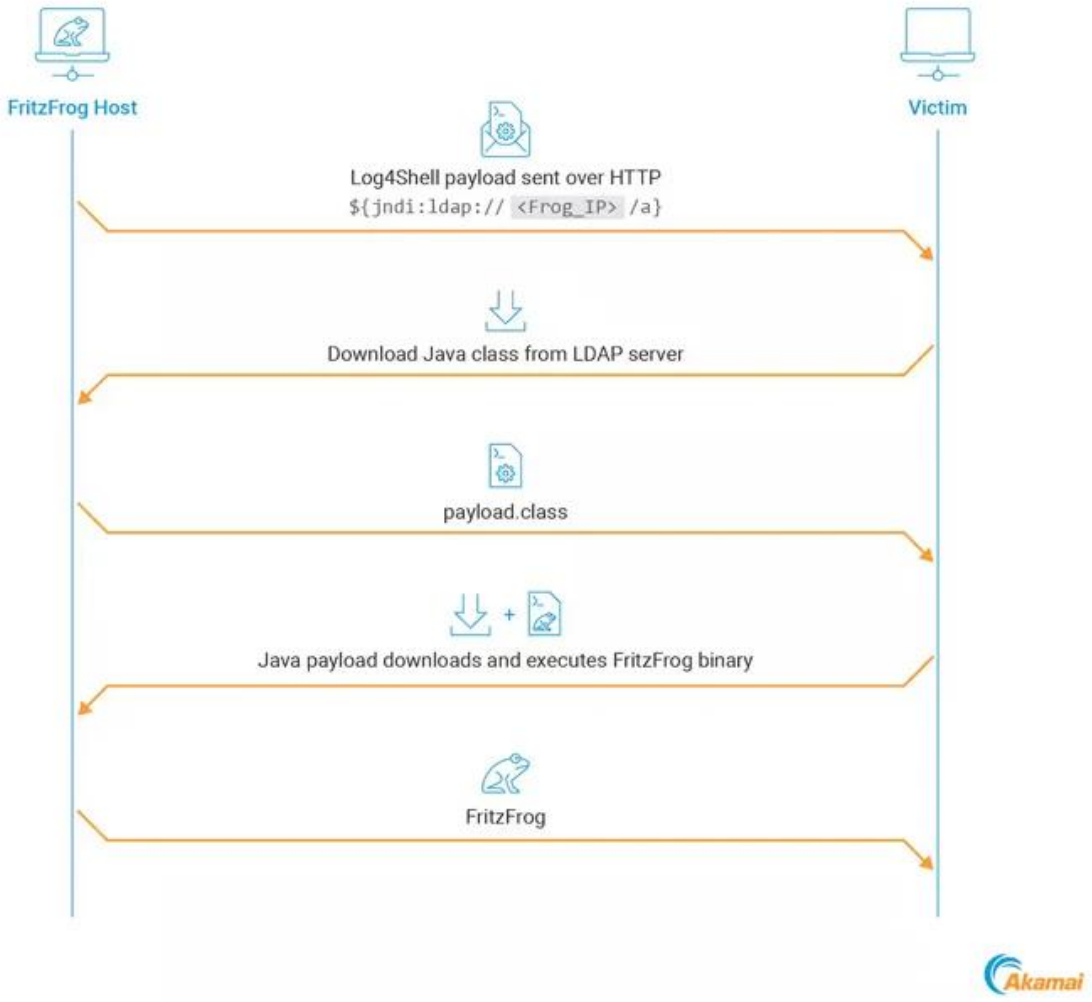
> *«La vulnerabilidad es explotada de manera agresiva, intentando dirigirse a tantas aplicaciones Java vulnerables como sea posible»*, informó la empresa de seguridad y estructura web Akamai en un informe.

FritzFrog, inicialmente identificado por Guardicore (ahora parte de Akamai) en agosto de 2020, es un malware basado en Golang que se centra principalmente en servidores con credenciales SSH débiles expuestas a Internet. Su actividad se remonta a enero de 2020.

A lo largo del tiempo, ha evolucionado para atacar sectores como salud, educación y gobierno, mejorando sus capacidades para finalmente implementar mineros de criptomonedas en los dispositivos infectados.

La novedad de esta versión radica en la utilización de la vulnerabilidad Log4Shell como vector secundario de infección, enfocándose específicamente en hosts internos en lugar de dirigirse a activos accesibles públicamente que presentan vulnerabilidades.

> *«Cuando se descubrió la vulnerabilidad por primera vez, se dio prioridad al parcheo de las aplicaciones expuestas a Internet debido al alto riesgo de compromiso»,* señaló el investigador de seguridad Ori David.
>
> *«En contraste, las máquinas internas, que eran menos propensas a ser explotadas, a menudo fueron descuidadas y permanecieron sin parches, una circunstancia que aprovecha FritzFrog».*



Esto implica que incluso si se han parcheado las aplicaciones expuestas a Internet, un ataque exitoso en cualquier otro punto de la red puede exponer sistemas internos no parcheados y propagar el malware.

El componente de fuerza bruta SSH de FritzFrog también ha sido mejorado para identificar específicamente objetivos SSH, analizando diversos registros del sistema en cada uno de sus objetivos.

Otro cambio destacado en el malware es la utilización de la vulnerabilidad PwnKit, identificada como CVE-2021-4034, para lograr una escalada de privilegios local.

> *«FritzFrog sigue empleando tácticas para mantenerse oculto y evitar la detección. En particular, se esfuerza por evitar dejar archivos en el disco siempre que sea posible»,* afirmó David.

Esto se logra mediante el uso de la ubicación de memoria compartida /dev/shm, que también ha sido empleada por otros malwares basados en Linux como BPFDoor y Commando Cat, y memfd_create para ejecutar cargas de memoria residente.

Esta revelación se produce simultáneamente con el anuncio de que el botnet InfectedSlurs está aprovechando activamente vulnerabilidades de seguridad ya parcheadas (desde CVE-2024-22768 hasta CVE-2024-22772 y CVE-2024-23842) que afectan a diversos modelos de dispositivos DVR de Hitron Systems para llevar a cabo ataques distribuidos de denegación de servicio (DDoS).