Mesa 4

Nota :
https://www.welivesecurity.com/la-es/2021/02/02/kobalos-amenaza-linux-afecta-infraestructuras-informaticas-alto-rendimiento/

¿Qué tipo de amenaza es?

Backdoor

¿Cómo comienza y cómo se propaga esta amenaza?

Kobalos se propaga en las maquinas que usen el cliente SSH. Al usarlo, la máquina comprometida tendrá sus credenciales capturadas. Estas credenciales podrán entonces ser usadas por los atacantes para instalar Kobalos en los nuevos servidores.

Mesa 4

¿Hay más de una amenaza aplicada ?

Kobalos no se dirige exclusivamente a los HPC: se descubrió que un gran ISP asiático, un proveedor de soluciones de seguridad para endpoints de Estados Unidos, así como algunos servidores personales, también fueron comprometidos por esta amenaza.

¿Qué solución o medida recomendarían ?

Desde una perspectiva de red, es posible detectar Kobalos buscando tráfico que no sea SSH en el puerto atribuido a un servidor SSH.

Los productos de ESET detectan el malware Kobalos.