CLASE 24

Nota:

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

¿Qué tipo de amenaza es?

Backdoor genérico

¿Cómo comienza y cómo se propaga esta amenaza?

“Kobalos garantiza el acceso remoto al sistema de archivos, brinda la capacidad de generar sesiones de terminal y permite establecer conexiones de proxy con otros servidores infectados por Kobalos. Los operadores tienen varias formas de llegar a una máquina infectada con Kobalos. El método que más hemos visto es en el cual Kobalos está embebido en el ejecutable del servidor OpenSSH (`sshd`) y activará el código del backdoor si la conexión proviene de un puerto de origen TCP específico. Hay otras variantes independientes que no están embebidas en `sshd`. Estas variantes o se conectan a un servidor C&C que actuará como intermediario o esperan una conexión entrante en un puerto TCP determinado. Algo que hace único a Kobalos es el hecho de que el código para ejecutar un servidor de C&C está en el propio Kobalos. Los operadores pueden convertir cualquier servidor comprometido por Kobalos en un servidor de C&C enviando un simple comando. Como las direcciones IP y los puertos del servidor C&C están hardcodeados en el ejecutable, los operadores pueden generar nuevas muestras de Kobalos que utilizan este nuevo servidor de C&C.”

¿Hay más de una amenaza aplicada?

Si, los investigadores de ESET escanearon Internet para encontrar víctimas potenciales. Pudimos identificar múltiples blancos de ataque de Kobalos, incluidos sistemas HPC, ubicados en: América del norte, Europa y Asia.

¿Qué solución o medida recomendarían?

Antivirus de protección avanzada que detectan el malware Kobalos.
Configurar el doble factor de autenticación (2FA) antes de realizar la conexión a un servidor SSH.