GRUPO: 4 - Amenazas

Integrantes:
Carla Antonini
Liliana Ospina
Ramon Colmenares
Maximo Toledo
Andres Tinoco
Diego Araque

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

● ¿Qué tipo de amenaza es?
Kobalos es un malware multiplataforma. Su objetivo es perseguir clusters informáticos de alto rendimiento (servidores) (HPC) y otros objetivos de alto perfil.
Al ser portable para muchos sistemas operativos, incluidos Linux, BSD, Solaris y posiblemente AIX y Windows tiene un gran alcance. Kobalos contiene muchos comandos que no revelan la intención de los atacantes. Entra a través de una puerta trasera, llamadada “backdoor”, que deja en el servidor, por lo cual podemos decir que este malware es un una versión “troyanizada” de openSSH.

ladrón de credenciales

● ¿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.

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.

El código para ejecutar esta en el propio kobalos así como los operadores pueden generar nuevas muestras de Kobalos que utilizan este nuevo servidor de C&C.

Es posible determinar de forma remota si un sistema está comprometido al conectarse al servidor SSH utilizando un puerto de origen TCP específico, puede saber si la conexion esta comprometida.
los investigadores de ESET escanearon Internet para encontrar víctimas potenciales.

todo su código es contenido en una única función que se llama a sí misma de forma recursiva para realizar subtareas.

Esto hace que sea más difícil de analizar. Además, todas las strings están cifradas, por lo que es más difícil encontrar el código malicioso que al mirar las muestras de forma estática.

El uso del backdoor requiere una clave RSA privada de 512 bits y una contraseña de 32 bytes. Una vez autenticadas, las claves RC4 son intercambiadas y el resto de la comunicación es cifrada con ellas.

● ¿Hay más de una amenaza aplicada?

brinda la capacidad de generar sesiones de terminal y permite establecer conexiones de proxy con otros servidores
activará el código del backdoor si la conexión proviene de un puerto de origen TCP específico.
el cliente SSH es comprometido para robar credenciales.
Variantes más nuevas que contienen cierta ofuscación y la capacidad de exfiltrar credenciales a través de la red.

Cualquiera que use el cliente SSH de una máquina comprometida tendrá sus credenciales capturadas.

● ¿Qué solución o medida recomendarían?

ESET informa que la forma para mitigar la amenaza de este malware es configurar autenticación de doble factor para poder conectarse con los servidores SSH.

Malwarebytes Anti-Malware es un programa antivirus muy potente capaz de detectar casi cualquier amenaza, incluso en su versión gratuito