Una puerta trasera recientemente descubierta ha afectado a los clústeres informáticos de alto rendimiento pertenecientes a redes universitarias, así como servidores asociados con agencias gubernamentales, proveedores de seguridad de puntos finales y proveedores de servicios de Internet. Dicha backdoor brinda a los atacantes la capacidad de ejecutar comandos arbitrarios en los sistemas de forma remota.

La compañía de seguridad cibernética ESET nombró al malware Kobalos, en referencia a una criatura traviesa de la mitología griega, por su *«tamaño de código diminuto y muchos trucos».*

> *«Kobalos es una puerta trasera genérica en el sentido de que contiene comandos amplios que no revelan la intención de los atacantes. En resumen, Kobalos otorga acceso remoto al sistema de archivos, brinda la capacidad de generar sesiones de terminal y permite conexiones de proxy a otros servidores infectados por Kobalos»*, dijeron los investigadores Marc-Etienne M. Léveillé e Ignacio Sanmillan.

Además de rastrear el malware hasta los ataques contra una serie de objetivos de alto perfil, ESET dijo que el malware es capaz de apuntar a Linux, FreeBSD, Solaris y posiblemente máquinas AIX y Windows, con referencias de código que apuntan a Windows 3.11 y Windows 95 heredado.

Al parecer, las infecciones por Kobalos comenzaron a fines de 2019 y desde entonces siguieron activas durante 2020.

El vector de compromiso inicial utilizado para implementar el malware y el objetivo final del actor de la amenaza aún no está claro, pero la presencia de un cliente OpenSSH con troyanos en uno de los sistemas comprometidos alude a la posibilidad de que *«el robo de credenciales podría ser una de las formas en que Kobalos se propaga».*

No se encontraron otros artefactos de malware en los sistemas, ni hubo ninguna evidencia que pudiera revelar la intención de los atacantes.

> *«No hemos encontrado ninguna pista que indique si roban información confidencial, persiguen ganancias monetarias o buscan otra cosa»,* dijeron los investigadores.

Pero descubrieron que el malware multiplataforma alberga algunas técnicas inusuales, incluidas las características que podrían convertir cualquier servidor comprometido en un servidor de comando y control (C&C) para otros hosts comprometidos por Kobalos.

Dicho de otro modo, las máquinas infectadas se pueden usar como proxies que se conectan a otros servidores comprometidos, que luego pueden ser aprovechados por los operadores para crear nuevas muestras de Kobalos que usan este nuevo servidor C&C para crear una cadena de proxy que comprende múltiples servidores infectados para llegar a sus objetivos.

Para mantener el sigilo, Kobalos autentica las conexiones con las máquinas infectadas utilizando una contraseña de 32 bytes que se genera y luego se cifra con una clave privada RSA de 512 bits. Posteriormente, se utiliza un conjunto de claves RC4, una para el tráfico entrante y el tráfico saliente, y para las comunicaciones con el servidor C&C.

La puerta trasera también aprovecha un mecanismo de ofuscación complejo para frustrar el análisis forense llamando de forma recursiva al código para realizar una amplia gama de subtareas.

> *«Las numerosas funciones bien implementadas y las técnicas de evasión de la red muestran que los atacantes detrás de Kobalos tienen mucho más conocimiento que el típico autor de malware que apunta a Linux y otros sistemas que no son Windows»,* dijeron los investigadores.

> *«Sus objetivos, que tienen un perfil bastante alto, también muestran que el objetivo de los operadores de Kobalos no es comprometer tantos sistemas como sea posible. Su pequeña huella y sus técnicas de evasión de red pueden explicar por qué no fue detectado hasta que nos acercamos a las víctimas con los resultados de nuestro escaneo en Internet»,* agregaron.