Encuentran versiones de Mirai en servidores Linux

El equipo de **Respuesta e Ingeniería de Seguridad de la compañía Netscout Arbor (ASERT)** ha estado monitoreando desde hace varios meses los intentos de **explotación de la vulnerabilidad Hadoop YARN** y sorpresivamente encontró un **payload familiar a Mirai.**

Estas **versiones de Mirai** encontradas se comportan como las originales, pero están **diseñadas para funcionar en servidores Linux y no en dispositivos del llamado Internet de las Cosas (IoT)**, como se reportó en octubre pasado.

Si bien **ASERT** ha publicado hallazgos de **Windows Mirai** anteriormente, esta es la primera vez que observa a este código malicioso fuera del IoT.

Los **Botmasters**, o administradores de Bots, han adquirido gran conocimiento sobre el desarrollo de **malware para el Internet de las Cosas**, y ahora han cambiado su enfoque hacia los servidores Linux. Al igual que muchos dispositivos IoT, los servidores Linux sin actualizaciones permanecen en la red, y los atacantes abusan de ellos a gran escala y enviando exploits a todos los servidores vulnerables que puedan encontrar.

Alertas

El objetivo de los criminales es claro: instalar malware en tantos dispositivos como sea posible. Una vez que se ha establecido Mirai en un servidor Linux, se comporta como un **bot de IoT** y comienza a utilizar nombres de usuario y contraseñas de telnet por medio de un ataque de fuerza bruta. Lo diferente es que, entre los dispositivos pequeños y diminutos de la botnet, ahora se encuentran servidores Linux de gran potencia.

Si encuentra con éxito un **dispositivo vulnerable,** en lugar de instalar directamente el malware en la víctima, informa la dirección IP, el nombre de usuario y la contraseña a un servidor de reporte, donde el atacante puede automatizar la instalación del bot.

Los servidores Linux en los centros de datos tienen acceso a más ancho de banda que los dispositivos IoT en redes residenciales, lo que los convierte en un bot de DDoS mucho más eficiente. Una cantidad de servidores Linux con muchos recursos pueden generar ataques que compitan con una red grande de bots de IoT.

Mirai ya no está apuntando únicamente a dispositivos del IoT. Si bien las técnicas utilizadas para entregar este código malicioso a los servidores tanto de **IoT como de Linux pueden ser similares**, para los atacantes es mucho más fácil ahora atacar servidores de Linux x86 que toda la gama de CPU utilizadas en los dispositivos de Internet de las Cosas. Hay que estar alertas, aseguran los expertos.