ALERTA

Propagación de Botnet

[COLCERT AL-0527-026]

TLP:CLEAR

” Botner Ebury continua su accionar mediante la explotación de nuevas vulnerabilidades”

Botnet Ebury

El Botnet Ebury, activo desde 2009, ha comprometido más de 400.000 servidores Linux, con más de 100.000 aún vulnerables a finales de 2023.

Técnicas utilizadas

Esta amenaza puede afectar dispositivos mediante:

- **Robo de credenciales:** Obtiene acceso no autorizado a sistemas y datos sensibles.
- **Redirección de tráfico web:** Desvía a los usuarios a sitios web fraudulentos o maliciosos.
- **Distribución de spam:** Inunda las bandejas de entrada con correos electrónicos no deseados.

Impacto en la seguridad digital

Esta amenaza altamente sofisticada busca lucro financiero a través de diversas actividades maliciosas, incluyendo:

- **Robo de criptomonedas:** Retira a los usuarios de sus activos digitales.
- **Ataques AitM (Adversary-in-the-Middle):** Intercepta y manipula las comunicaciones entre dispositivos.

Para protegerse contra esta amenaza:

1. **Actualizar sistemas Linux:** Cerrar vulnerabilidades explotadas por el botnet.
2. **Reforzar la seguridad de los proveedores de alojamiento:** Implementar medidas de seguridad robustas.
3. **Utilizar autenticación fuerte en SSH:** Usar mecanismos de autenticación robustos, como claves SSH.
4. **Monitorear la actividad de la red:** Implementar herramientas de monitoreo para detectar actividades inusuales.
5. **Realizar copias de seguridad regulares:** Hacer copias de seguridad de datos críticos.

Es importante aplicar las actualizaciones de los sistemas indicados para evitar la explotación de estas vulnerabilidades.

NIVEL DE RIESGO

MEDIO

FUENTES:

1. https://www.securityweek.com/400000-linux-servers-hit-by-ebury-botnet/
2. Guía de seguridad para servidores Linux: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/index

COLCERT