ALERTA

Nueva variante del ransomware Helldown a sistemas Linux

COLCERT AL-2211-059

Una nueva variante del ransomware Helldown, dirigida a sistemas Linux y Windows, ha comenzado a expandirse, con un enfoque particular en infraestructuras virtualizadas de pequeñas y medianas empresas.

Este ransomware se basa en el código de LockBit 3.0 y ha sido responsable de ataques a al menos 31 empresas en los últimos tres meses, incluida la sucursal europea de Zyxel, afectando sectores críticos como servicios de TI, telecomunicaciones, manufactura y atención médica.

ANÁLISIS

- **Métodos de infiltración:** Helldown utiliza la explotación de vulnerabilidades en dispositivos Zyxel para obtener acceso inicial a las redes, seguido de actividades como recolección de credenciales y movimientos laterales para desplegar el ransomware.
- **Características técnicas:** La versión de Linux carece de mecanismos de ofuscación y está diseñada para buscar y cifrar archivos sin comunicación externa. Además, acaba máquinas virtuales activas antes del cifrado.
- **Estrategia de extorsión doble:** Al igual que otros grupos de ransomware, Helldown amenaza con publicar datos robados para presionar a las víctimas a pagar rescates.

Implicaciones de no ajustar la postura de seguridad

- **Riesgo aumentado de ataques:** Sin ajustes en la postura de seguridad, las entidades y organizaciones se vuelven más vulnerables a ataques cibernéticos, lo que puede resultar en pérdidas económicas significativas y daños a la reputación.
- **Pérdida de datos críticos:** La falta de medidas adecuadas puede llevar a la pérdida irreversible de datos sensibles, lo que afecta tanto a las operaciones como a la confianza de los clientes.
- **Costos legales y regulatorios:** La filtración de datos personales pueden resultar en sanciones legales y costos asociados a las denuncias de las personas afectadas.
- **Interrupción operativa:** Un ataque exitoso podría causar interrupciones significativas en las operaciones diarias, afectando la productividad y los servicios ofrecidos.

Recomendaciones

- **Actualización continua:** Mantenga todos los sistemas actualizados con los últimos parches de seguridad.
- **Monitoreo activo:** Implemente soluciones para detectar actividades maliciosas e inusuales en la red.
- **Capacitación del personal:** Concientice a los colaboradores sobre las tácticas comunes utilizadas por los atacantes.

NIVEL DE RIESGO

MEDIO

FUENTES:

https://thehackernews.com/2024/11/new-helldown-ransomware-expands-attacks.html
https://www.infosecurity-magazine.com/news/helldown-ransomware-target-vmware/
https://www.bleepingcomputer.com/news/security/helldown-ransomware-exploits-zyxel-vpn-flaw-to-breach-networks/
https://blog.sekoia.io/helldown-ransomware-an-overview-of-this-emerging-threat/

COLCERT