Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

EL RANSOMWARE KILLSEC ATACA HOSPITALES Y CLÍNICAS, PONIENDO EN RIESGO LA ATENCIÓN MÉDICA

16/ 09/2025

CONTENIDO

INTRODUCCIÓN

Un nuevo y peligroso ransomware, conocido como KillSec, ha surgido en la escena del cibercrimen, enfocándose de manera específica en el sector de la salud en América Latina.

En tan solo una semana desde su aparición a principios de septiembre, KillSec ha logrado comprometerse a más de una docena de entidades de salud, demostrando una alta sofisticación en sus ataques.

EL RANSOMWARE KILLSEC ATACA HOSPITALES Y CLÍNICAS, PONIENDO EN RIESGO LA ATENCIÓN MÉDICA

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_09_16_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	16/09/2025
Es día cero (0 day):	No

RESUMEN

Un nuevo y peligroso ransomware, conocido como KillSec, ha surgido en la escena del cibercrimen, enfocándose de manera específica en el sector de la salud en América Latina.

En tan solo una semana desde su aparición a principios de septiembre, KillSec ha logrado comprometerse a más de una docena de entidades de salud, demostrando una alta sofisticación en sus ataques.

Anatomía del ataque

Los operadores de KillSec utilizan una combinación de tácticas simples y avanzadas:

- Explotación inicial: El ransomware se infiltra en las redes al explotar vulnerabilidades en aplicaciones web sin parches, configuraciones incorrectas en la nube o a través de cadenas de suministro de software comprometidos. En un caso documentado, el ataque se inició con una factura en PDF que contenía una vulnerabilidad de día cero, ejecutando un comando de PowerShell malicioso.
- Evasión de defensas: El malware utiliza un cargador ligero y una rutina de cifrado personalizada AES-256. Una vez dentro, se inyecta directamente en la memoria del sistema (lsass.exe) para evitar ser detectado por los antivirus tradicionales que se basan en firmas.
- Persistencia y exfiltración: El ransomware se propaga a través de protocolos administrativos legítimos, lo que le permite pasar desapercibido durante días. Antes de iniciar el cifrado, exfiltra datos sensibles, como registros de pacientes e información de identificación personal (PII), totalizando más de 34 GB de datos robados.
- Doble extorsión: Después de robar los datos, el ransomware inicia un proceso de cifrado de varias etapas. La filtración de los archivos robados ha obligado a las entidades de salud a notificar a las autoridades reguladoras, lo que demuestra la estrategia de “doble extorsión” de los atacantes (piden rescate por el descifrado y también amenazan con publicar los datos robados).

RECOMENDACIONES

- Aplique parches de inmediato. KillSec se aprovecha de aplicaciones web sin parches y de vulnerabilidades en la cadena de suministro de software. Es fundamental mantener todos tus sistemas y aplicaciones actualizados para cerrar las puertas de entrada.
- Refuerza la seguridad de la red. El ransomware utiliza protocolos de administración legítimos para moverse. Asegúrese de tener una segmentación de red estricta y de usar firewalls para restringir la comunicación solo lo que sea absolutamente necesario.
- Implementa una seguridad avanzada de endpoints. Dado que KillSec se inyecta en la memoria del sistema (lsass.exe) para evadir los antivirus tradicionales, necesita una solución de seguridad de endpoints (EDR) que pueda detectar comportamientos maliciosos en la memoria y no solo las firmas de los archivos.
- Capacita a tus empleados. El ataque puede comenzar con una simple factura en PDF. Educar a los usuarios para que desconfíen de archivos adjuntos inesperados y para que verifiquen la autenticidad de los remitentes es una de las defensas más efectivas.

NOTICIA COMPLETA

https://devel.group/blog/el-ransomware-killsec-ataca-hospitales-y-clinicas-poniendo-en-riesgo-la-atencion-medica/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group