Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

HOSPITAL CLÍNIC DE BARCELONA SE VE AFECTADO POR UN ATAQUE DE RANSOMWARE

07/Marzo /2023

CONTENIDO

INTRODUCCIÓN

El Hospital Clínic de Barcelona sufrió un ataque de ransomware el domingo por la mañana, interrumpiendo gravemente sus servicios de salud después de que las máquinas virtuales de la institución fueran blanco de ataques.

EL FBI Y CISA ADVIERTEN SOBRE EL AUMENTO DE LOS RIESGOS DE ATAQUES DE ROYAL RANSOMWARE

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

ID de alerta:	DSOC-CERT_2023_07_03_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	07/03/2023
Es día cero (0 day):	No

RESUMEN

El Hospital Clínic de Barcelona sufrió un ataque de ransomware el domingo por la mañana, interrumpiendo gravemente sus servicios de salud después de que las máquinas virtuales de la institución fueran blanco de ataques.

El hospital de 819 camas tiene su sede en Barcelona, España, y presta servicios a más de medio millón de personas que buscan atención médica y servicios de salud.

Según un comunicado emitido por la Generalitat de Catalunya, el Hospital Clínic de Barcelona sufrió un ataque por la operación ransomware RansomHouse.

La declaración del gobierno también menciona que el ciberataque afectó a los servicios de emergencia de tres centros médicos asociados al Clínic de Barcelona, entre ellos CAP Casanova, CAP Borrell y CAP Les Corts.

“Este es un ciberataque que se ha producido en entornos virtualizados. Ha sido un ataque sofisticado y complejo que no involucró técnicas clásicas, lo que indica una evolución por parte del atacante”, menciona el anuncio del gobierno de Cataluña.

Ransom House, que normalmente comete actos de este tipo por dinero, ha explicado el director general de la Agència de Ciberseguretat de Catalunya, hasta el momento los criminales no han solicitado ningún rescate, la Generalitat no tiene intención de negociar. “No habrá ningún tipo de negociación para pagar ni un céntimo”, han remarcado.

Desafortunadamente, 150 operaciones no urgentes programadas para las próximas semanas han sido canceladas, y 3.000 citas fueron canceladas.

Estos planes urgentes se mantendrán durante al menos un par de días más, mientras que el tiempo para volver a la normalidad es imposible de determinar actualmente, según el director del hospital Clínic Barcelona, A. Castells.

Al escribir esto, el sitio de fuga de datos RansomHouse no ha filtrado ningún dato perteneciente al hospital español, pero podría ser demasiado pronto para que la víctima aparezca en el sitio del actor de amenazas.

RECOMENDACIONES

- Implemente un plan de recuperación que mantenga y conserve múltiples copias de datos confidenciales o de propiedad y servidores en una ubicación segura, segmentada y separada físicamente (es decir, disco duro, dispositivo de almacenamiento o la nube).
- Implemente la segmentación de la red y mantenga copias de seguridad fuera de línea de los datos para garantizar una interrupción limitada de la organización.
- Realice copias de seguridad de los datos con regularidad y proteja con contraseña las copias de seguridad almacenadas sin conexión. Asegúrese de que las copias de los datos críticos no sean accesibles para su modificación o eliminación desde el sistema donde residen los datos.
- Mantenga actualizado todos los sistemas operativos, y software.
- Instale, actualice periódicamente y habilite la detección en tiempo real del software antivirus en todos los hosts.
- Audite las cuentas de usuarios con privilegios administrativos y configure los controles de acceso, con el principio de privilegios mínimos.
- Desactive los puertos no utilizados.
- Deshabilite las actividades y permisos de línea de comandos y scripting.
- Asegúrese de que todos los datos de copia de seguridad estén encriptados, sean inmutables
- Examine el tráfico de red entrante y saliente, en busca de actividad sospechosa dentro de su red.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20230307_02_RansomHouse

NOTICIA COMPLETA

https://devel.group/blog/hospital-clinic-de-barcelona-se-ve-afectado-por-un-ataque-de-ransomware/

CONTACTOS DE SOPORTE

Correo electrónico: cert@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://www.devel.group/reporta-un-incidente