Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Hive Ransomware ataca la CCSS de Costa Rica

31/mayo/2022

Contenido

INTRODUCCIÓN

Con este boletín queremos hacer de su conocimiento el reciente ataque de Hive Ransomware al Gobierno de Costa Rica, solicitamos preste atención a nuestras recomendaciones y pueda validar los IOC's que ponemos a su disposición para poder mitigar cualquier posible riesgo de intrusión de parte de los actores de amenazas.

HIVE RANSOMWARE

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

ID de alerta:	DSOC-CERT_2022_05_31_02
Clasificación de alerta:	Amenaza
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**WHITE**
Fecha de publicación:	05/31/2022
Es día cero (0 day):	NO

RESUMEN

La Caja Costarricense de Seguro Social (CCSS) sufrió un ciberataque la madrugada de este martes, obligando a la institución a apagar todos los sistemas informáticos y forzando a sus hospitales a volver a los expedientes de papel para atender pacientes, mientras se determina el nivel de afectación y una posible solución.

En horas de la madrugada algunas de las impresoras de la institución empezaron a imprimir una nota de rescate estandarizada utilizada por Hive Ransonware Group, el cual indica que la red de la institución fue vulnerada y todos los datos fueron encriptados: datos personales, reportes financieros y otros documentos importantes, listos para ser filtrados en Internet en caso de que la Caja no adquiera un programa informático propiedad de los cibercriminales para recuperar sus sistemas.

La nota de rescate advierte a la Caja de no modificar, renombrar o borrar los archivos afectados, pues caso contrario, los datos no podrán desencriptarse; así como tampoco reportar el ataque a la policía o al FBI; no contratar una compañía de recuperación de archivos y no negarse a comprar el programa, bajo amenaza de publicar todo lo sustraído.

De acuerdo con una alerta del Buró Federal de Investigaciones (FBI, por sus siglas en Inglés), Hive Ransomware Group apareció por primera vez en junio del año 2021 y probablemente funciona como un ransomware basado en afiliados, emplea una amplia variedad de tácticas, técnicas y procedimientos (TTP), lo que crea desafíos importantes para la defensa y la mitigación. Hive utiliza múltiples mecanismos para comprometer las redes comerciales, incluidos los correos electrónicos de phishing con archivos adjuntos maliciosos para obtener acceso y el Protocolo de Escritorio Remoto (RDP en Inglés) para moverse una vez en la red.

Según el FBI, después de comprometer la red de una víctima, los actores del ransomware Hive extraen los datos y cifran archivos en la red; y dejan una nota de rescate en cada directorio afectado dentro del sistema de la víctima, que proporciona instrucciones sobre cómo comprar el software de descifrado. La nota de rescate también amenaza con filtrar datos de víctimas exfiltrados en el sitio "HiveLeaks" de acceso en la red profunda a través del navegador Tor.

Según el análisis de la agencia federal estadounidense, el ransomware de Hive busca los procesos de las computadoras y sistemas relacionados con copias de seguridad, antivirus/antispyware y copia de archivos y los obliga a finalizar, para facilitar el cifrado de archivos. Asimismo, el ransomware elimina las copias de seguridad sin notificar a la víctima .

Algunas víctimas informaron al FBI haber recibido llamadas telefónicas de actores de Hive solicitando el pago por sus archivos. El plazo inicial para el pago fluctúa entre 2 y 6 días, pero los criminales han prolongado el plazo en respuesta al contacto de la víctima.

Recomendaciones

1. Favor, descargar documentos de procedencia desconocida.

2. Mantenga su software Antivirus actualizado.

3. Asegurese de mantener RDP habilitado solo cuando personal de IT lo requiera.

4. Solicitar a su SOC que mantengan monitoreo activo ante toda conexión sospechosa y detecciones del software AV.

5. Asegurese de tener debidamente configurada una DMZ para sus servicios y dispositivos críticos.

6. Validar las reglas de su Anti Spam y Anti Phishing, socializar con us colaboradores que ante cualquier correo sospechoso lo reporten inmediatamente al departamento de IT para su respectivo análisis.

7. En todo sistema que este disponible la autenticación de múltiple factor, se recomienda encarecidamente sea habilitada y puesta en marcha a la brevedad.

Noticia Completa

https://delfino.cr/2022/05/hive-ransomware-group-el-grupo-de-cibercriminales-que-ataco-la-ccss-y-tiene-predileccion-por-instituciones-de-salud

https://delfino.cr/2022/05/hackeo-a-la-ccss-fue-un-ataque-excepcionalmente-violento-pero-no-se-vulneraron-bases-de-datos-o-sistemas-criticos

IOC's

https://github.com/develgroup/SOC_IOCs/tree/main/20220506_03_HiveRansomware

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