CAJA COSTARRICENSE DE SEGURO SOCIAL
Auditoría Interna
Teléfono: 2539-0821 ext. 2000-7468
Correo electrónico: auditoria_interna@ccss.sa.cr

AS-AATIC-089-2022
21 de junio de 2022

Máster
Idannia Mata Serrano, subgerente a.i.
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES -1150

Estimado señor:

ASUNTO:	**Oficio de Asesoría en relación con acciones preventivas para minimizar la materialización de riesgos generados por eventuales debilidades en el Active Directory y servidores Exchange que permita la ejecución del ransomware "BlackCat".**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno específicamente en su rol de asesor, esta Auditoría informa sobre la importancia de implementar acciones preventivas, a fin de evitar la materialización de riesgos en materia de Ciberseguridad, generados por eventuales debilidades en el Active Directory y servidores Exchange, que permita la ejecución del ransomware BlackCat una vez que se normalicen las operaciones en la Institución y entre en funcionamiento la plataforma tecnológica de la Caja.

Al respecto, BlackCat es un ransomware que fue creado en noviembre del 2021 bajo la estrategia de ransomware como servicio RaaS (ransomware-as-a-service) con la particularidad que se produjo mediante el lenguaje de programación no convencional Rust, por lo que al utilizar un lenguaje moderno para su carga útil, le permite evadir la detección de soluciones de seguridad convencionales que aún no han actualizado su capacidad de detección de códigos escritos en este lenguaje, considerando además que es un ransomware operado por humanos basado en línea de comandos, permitiéndoles moverse lateralmente y adquirir privilegios de administrador para propagarse a otras computadoras, cifrar dispositivos, borrar información imposible de recuperar incluyendo copias de respaldo y máquinas virtuales, lo anterior como producto de debilidades en la configuración del Active Directory, donde el atacante toma el control completo del dominio.

Si bien lo más común es que BlackCat ingrese mediante aplicaciones de escritorio remoto, así como de credenciales comprometidas vía Active Directory, también se han identificado que este ransomware aprovecha las vulnerabilidades del servidor de Exchange para obtener acceso a la red de destino, esto por cuanto la estrategia RaaS consiste en la intervención de múltiples actores entre acces brokers que lo que realizan es comprometer las redes y mantener la persistencia, los RaaS operators que desarrollan las herramientas de filtración, y los RaaS affiliates quienes se mueven lateralmente a través de la red y filtra datos antes de lanzar finalmente la carga útil del ransomware, es por esto que se ha identificado que entre los afiliados RaaS que han adoptado BlackCat se encuentra Conti y Hive, organizaciones que han sido ligados a los recientes ciberataques en las instituciones públicas del país.

BlackCat puede omitir el control de cuentas de usuario (UAC) por lo que se podría ejecutar incluso desde un contexto que no es administrador, esto por cuanto si no se ejecuta con privilegios de administrador ejecuta un proceso secundario en el dllhost.exe, con los permisos suficientes para cifrar el número máximo de archivos en el sistema, asimismo, el ransomware puede determinar el nombre del equipo, el nombre del dominio y el nombre de usuario del Active Directory en un dispositivo y si este tiene privilegios de administrador, aumenta la capacidad de propagación a más dispositivos, aunado a esto, BlackCat detecta todos los servidores que están conectados en la red difundiendo mensajes de servicio de NETBIOS para buscar dispositivos adicionales, intentando replicarse en los servidores de respuesta mediante credenciales especificadas en la configuración mediante el PxExec, lo anterior hace que BlackCat presente números métodos para dificultar los esfuerzos de recuperación.

Por lo anterior, entre las recomendaciones brindadas por los expertos en esta temática, para contrarrestar las posibilidades de que se materialicen vulnerabilidades mediante este mecanismo se encuentran:

- Proteger todos los dispositivos institucionales utilizando soluciones de ciberseguridad de confianza
- Dar a conocer a los usuarios los conceptos básicos de ciberseguridad y seguridad de la información de manera periódica.
- Disponer de una estrategia antiransomware de varios niveles para estar preparados ante algún incidente.
- Proteger el Active Directory utilizando modelos de protección integrales que incluya detección y prevención de las actividades de reconocimiento que realizan los atacantes, así como otros parámetros que puedan indicar que los dominios se están comprometiendo.
- Implementación de herramientas IDR como mecanismo de protección de credenciales de los usuarios y los objetos del Active Directory mientras reducen la superficie de ataque con el uso de herramientas de visibilidad de las exposiciones locales y en la nube.

En este sentido, esta Auditoría informa sobre lo descrito con el objetivo de que se analice la información expuesta y se profundice en el tema de así requerirlo, reforzando los mecanismos de ciberseguridad una vez que se hayan reestablecido los servicios tecnológicos institucionales, de tal forma que se reduzca la posibilidad de que se materialicen riesgos que afecten las actividades sustantivas de la institución y teniendo un efecto directo en la atención de la población que hace uso de los servicios institucionales.

Lo anterior, en apego a lo indicado en las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, que establecen dentro de los procesos del marco de gestión de TI, lo correspondiente a la “Seguridad y Ciberseguridad”, a saber:

> *“XI. SEGURIDAD Y CIBERSEGURIDAD*
>
> *La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.*
> *La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información (…).*
>
> *Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.*
>
> *La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información (…)”.*

En virtud de lo expuesto, se da conocer la información descrita, con el propósito de ser sometida a valoración y revisión por esa Administración y así coadyuvar al cumplimiento de los objetivos institucionales, garantizando un marco adecuado para el resguardo de la información institucional y de la seguridad informática.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)
Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.06.21 15:15:23 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

Referencias utilizadas:

Microsoft (2022). The many lives of BlackCat ransomware. Recuperado de: https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

Díaz Granados, Hernán (2022). BlackCat: un nuevo jugador en el negocio del ransomware. Recuperado de: https://latam.kaspersky.com/blog/black-cat-ransomware/24673/#:~:text=Los%20creadores%20del%20ransomware%20BlackCat%20ofrecen%20sus%20servicios,y%2C%20a%20cambio%2C%20obtienen%20una%20parte%20del%20rescate.

Vásquez. Juan Carlos (2021). BlackCat, el nuevo ransomware que va a la caza del Active Directory. Recuperado de: https://www.computerweekly.com/es/ehandbooks

OSC/RJS/RAHM/LDP/ghc

C. Doctor Roberto Cervantes Barrantes, gerente, Gerencia General -1100.
Auditoría