28 de febrero de 2022

El Centro de Informática avisa:

Alerta de seguridad por Ransomware BlackByte

El Centro de Informática alerta a la comunidad universitaria sobre la alerta referente a los ataques del Ransomware BlackByte, según indicó el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), tras recibir el aviso emitido de forma conjunta por el Servicio Secreto de los Estados Unidos (USSS) la Oficina Federal de Investigaciones (FBI).

Este tipo de Ransomware o secuestro de datos, se dedica a cifrar los archivos comprometidos en máquinas con Windows, incluyendo tanto servicios físicos como virtuales.

Para evitar ser víctima de este tipo de ataque, recomendamos lo siguiente:

- Tenga una sólida protección del correo electrónico: el correo electrónico sigue siendo el vector de ataque más grande para muchas amenazas cibernéticas aprovechando el uso del phishing para engañar al usuario. Los correos electrónicos de phishing a menudo contienen enlaces o archivos adjuntos maliciosos. La capacitación continua previene que los usuarios hagan clic en enlaces y archivos adjuntos sospechosos y les brindará el conocimiento para identificar las señales de una campaña de phishing.
- Utilice una política de privilegios mínimos: otorgue a los usuarios la menor cantidad de privilegios, lo que restringe los derechos de un usuario en la red. Esto puede reducir la capacidad de un usuario para moverse lateralmente a través de la red.
- Haga una copia de seguridad de los datos críticos: es importante contar con respaldos de la información que permitan recuperarse en caso de un ataque de ransomware y no verse obligado a pagar el rescate.

- Mantenga actualizados todos sus sistemas tecnológicos, es importante que mantenga todos los equipos, tanto de red como de usuario final, actualizados.
- Implemente la autenticación multifactor (MFA) para cada cuenta. La habilitación de MFA para plataformas de comunicaciones corporativas (como con todas las demás cuentas) proporciona una defensa vital contra este tipo de ataques.
- Aumente los niveles de protección en los equipos que cumplan las funciones de AntiSpam, WebFilter y Antivirus.
- Actualizar el software y los sistemas operativos con los últimos parches. Las aplicaciones y los sistemas operativos obsoletos son el objetivo de la mayoría de los ataques.
- Verifique y controle los servicios de escritorio remoto (RDP).
- Verifique periódicamente los indicadores de compromisos publicados.
- Desactive los servicios innecesarios en las estaciones de trabajo y los servidores de la institución.
- Implemente un sistema de detección de intrusiones, si aún no se ha utilizado,para detectar la actividad en la red potencialmente maliciosa.
- Supervise el tráfico web, se recomienda restrinja el acceso de los usuarios a sitios sospechosos o peligrosos.

Finalmente, en caso de dudas o consultas, puede comunicarse con el Centro de Informática al teléfono 2511-5000 o al correo electrónico ci5000@ucr.ac.cr.