



20 de marzo de 2024

El Centro de Informática avisa:

Nuevo ciberataque podría poner en riesgo su información

El Centro de Informática avisa a toda la comunidad universitaria sobre un nuevo ciberataque que se propaga a través de archivos adjuntos maliciosos en correos electrónicos (phishing) y podría poner en riesgo su información, según indicó el Centro de Respuesta a Incidentes (CSIRT) del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) mediante una alerta técnica.

Este ciberataque es capaz de adaptarse a diferentes situaciones (versátil) y permite a los actores de amenazas implementar el software malicioso (Malware) de su elección u obtener un control total sobre la red de la víctima utilizando un Malware tipo troyano de acceso remoto (RAT por sus siglas en inglés) conocido como "NobellLaunch".

Para evitar ser víctima de este tipo de ataques, siga estas recomendaciones:

- 1) Utilice soluciones de seguridad de correo electrónico que ejecuten comprobaciones automáticas en busca de atributos de comportamiento sospechoso.
- 2) Manténgase al tanto de las campañas de ingeniería social y phishing con el fin de obtener el conocimiento y las herramientas necesarias para identificar este tipo de intentos de estafa.
- 3) Actualice de forma periódica el software y sistema operativo utilizado tanto en su computador, así como en sus dispositivos móviles.
- 4) Realice copias de seguridad en diferentes medios de su información, bajo la estrategia 3,2,1,1,0: 3 respaldos en al menos 2 diferentes medios, 1 copia



UNIVERSIDAD DE
COSTA RICA

CI Centro de
Informática

fuera del sitio de trabajo, 1 inmutable previamente revisada y 0 problemas para recuperar la información.

- 5) Habilite y use lo posible el Múltiple Factor de Autenticación (MFA) en todos los portales, sitios web y redes sociales.

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