INSTITUTO NACIONAL DE CANCEROLOGÍA — SGSI / CIBERSEGURIDAD

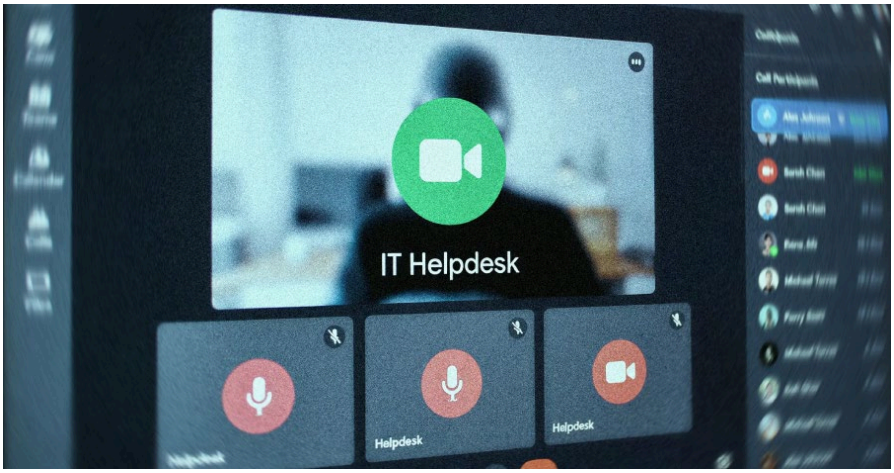
Boletín de Ciberseguridad para Funcionarios

Alerta: Campaña de malware SNOW vía Microsoft Teams

Boletín de seguridad · Mayo 2026 · Dirigido a: todo el personal INC · Clasificación: Informativo

¿Qué está pasando?

El grupo de amenaza UNC6692 está utilizando Microsoft Teams para hacerse pasar por personal de soporte técnico, con el fin de instalar un malware llamado **Snow** y robar credenciales e información sensible. Esta campaña ha sido activa a nivel global y puede afectar a cualquier funcionario que use Microsoft Teams en el INC.



Cómo ocurre el ataque — paso a paso

Paso 1 **Bombardeo de correo**	Le envían cientos de correos basura para generar confusión y angustia, saturando su bandeja de entrada.
Paso 2 **Contacto por Teams**	Un supuesto "agente de soporte" le escribe por Microsoft Teams desde una cuenta externa ofreciéndole ayuda con los correos.
Paso 3 **Página de phishing**	Lo dirigen a un sitio web falso que imita portales legítimos (como Outlook o páginas corporativas) para robar su contraseña.
Paso 4 **Instalación del malware**	Con sus credenciales, los atacantes ejecutan un script que instala Snow malware en su dispositivo, obteniendo control remoto total.

¿Cómo protegerse? — Recomendaciones para todo el personal

✓	Desconfíe de contactos de soporte por Teams que no reconozca. El área de TI del INC nunca le solicitará credenciales ni acceso remoto por chat sin un ticket formal previo.
✓	No haga clic en enlaces enviados por Teams o correo que lleven a páginas que pidan su usuario y contraseña. Verifique siempre la dirección web antes de ingresar cualquier dato.
✓	Si recibe una avalancha inusual de correos no deseados, repórtelo de inmediato a la mesa de ayuda. Puede ser la primera fase de este ataque.

Boletín de Ciberseguridad para Funcionarios

Alerta: Campaña de malware SNOW vía Microsoft Teams

Boletín de seguridad · Mayo 2026 · Dirigido a: todo el personal INC · Clasificación: Informativo

✓	No instale ningún programa ni ejecute ningún archivo que le hayan enviado por Teams, aunque quien lo envíe diga ser del área de sistemas o soporte técnico.
✓	Si sospecha que ya fue víctima, desconecte el equipo de la red institucional y comuníquese de inmediato con el área de TI/Seguridad para contener el incidente.

¿Vio algo sospechoso? Repórtelo

Ante cualquier situación sospechosa en Microsoft TEAMS, comuníquese con la mesa de ayuda / Seguridad Informática del INC antes de tomar cualquier acción.

Importante: No borre evidencia ni apague el equipo (solo proceda a desconectarlo de la red). Su reporte oportuno protege a todos los funcionarios y a los pacientes del instituto.