



El CERT de Ucrania advierte sobre ataques de phishing utilizando cuentas de correo comprometidas

El Equipo de Respuestas a Emergencias Informáticas de Ucrania (CERT-UA) advirtió sobre nuevos ataques de phishing dirigidos a sus ciudadanos al aprovechar cuentas de correo electrónico comprometidas pertenecientes a tres entidades indias diferentes, con el objetivo de comprometer sus bandejas de entrada y robar información confidencial.

La [agencia advirtió](#) que los correos electrónicos llegan con el asunto «Увага», que significa «Atención», y aseguran ser de un servicio de correo electrónico nacional llamado Ukr.net, cuando en realidad la dirección de correo electrónico del remitente es «*muthuprakash.b@tvsrubber[.]com*».

Los mensajes supuestamente advierten a los destinatarios de un intento no autorizado de iniciar sesión en sus cuentas desde una dirección IP con sede en la ciudad de Donetsk, en el este de Ucrania, lo que los incita a hacer clic en un enlace para cambiar sus contraseñas con efecto inmediato.

«Luego de seguir en enlace e ingresar la contraseña, llega a los atacantes. De esta forma, obtienen acceso a las bandejas de entrada de correo electrónico de los ciudadanos ucranianos», dijo CERT-UA en Facebook.

TVS Rubber es una empresa automotriz con sede en la ciudad india de Madurai, lo que sugiere que los ataques aprovecharon una cuenta de correo electrónico ya comprometida para distribuir los correos electrónicos de phishing.

CERT-UA, en una [actualización posterior](#), dijo que detectó 20 direcciones de correo electrónico adicionales que se utilizaron en los ataques, algunas de las cuales pertenecen a administradores de sistemas y profesores de la Universidad de Ciencias Aplicadas de Ramaiah, una situación académica ubicada en la ciudad india de Bangalore.

También se incluye en la lista una dirección de correo electrónico de otra empresa automotriz con sede en India, llamada Hodek Vibration Technologies Pvt. Ltd., que diseña y fabrica amortiguadores para automóviles, vehículos comerciales ligeros y pesados.



El CERT de Ucrania advierte sobre ataques de phishing utilizando cuentas de correo comprometidas

«Todos estos buzones se han visto comprometidos y están siendo utilizados por los servicios especiales de la Federación Rusa para llevar a cabo ataques cibernéticos contra ciudadanos ucranianos», dijo la agencia.

El desarrollo se produce cuando las naciones de la OTAN votaron por unanimidad para admitir a Ucrania en el Centro Cooperativo de Excelencia en Defensa Cibernética (CCDCOE) como un «participante contribuyente», ya que la invasión militar del país por parte de Rusia siguió hasta la segunda semana y los ataques cibernéticos llovieron sobre objetivos gubernamentales y comerciales.

«La presencia de Ucrania en el Centro mejorará el intercambio de experiencia cibernética entre Ucrania y las naciones miembros del CCDCOE. Ucrania podría aportar un valioso conocimiento de primera mano de varios adversarios dentro del dominio cibernético para ser utilizado para investigación, ejercicios y capacitación», [dijo](#) el Coronel Jaak Tarien, director del CCDCOE.