La firma de seguridad en Internet Kaspersky Lab alertó este martes sobre 'La Máscara', una de las amenazas más avanzadas en este momento que incluye un programa malicioso para Mac y Linux que ha infectado a más de 380 víctimas entre más de 1,000 direcciones de Internet (IPs) en todo el mundo.

Se trata del primer código malicioso de habla hispana y ha sido dirigido a instituciones gubernamentales, compañías privadas y diplomáticos, provocando infecciones en 31 países de Medio Oriente, Europa, África y del continente americano, incluidos, México, Argentina, Brasil, Colombia, Costa Rica y Venezuela.

La campaña de 'La Máscara' se basa en el envío de mensajes de correo electrónico (phishing) con vínculos a un sitio web malicioso que contiene una serie de Exploits diseñados para infectar a los visitantes en función de la configuración del sistema.

Después de la infección, el sitio malicioso redirige al usuario a la página web legítima de referencia en el correo electrónico, que puede ser una película de YouTube o un portal de noticias.

Conocido también como 'Careto' intercepta todos los canales de comunicación y recoge la información más vital del equipo de la víctima, recopila datos sensibles, claves de cifrado, configuraciones de VPN (Red Privada Virtual), claves SSH (que sirve como medio de identificación de un usuario a un servidor SSH) y archivos RDP (utilizado para abrir automáticamente una conexión a una computadora reservada).

«Existen varias razones que nos hacen creer que esto podría ser una campaña patrocinada por un Estado. Se ha observado un alto grado de profesionalismo en los procedimientos operativos del grupo que está detrás de este ataque", afirmó Costin Raiu, director del equipo de Investigación y análisis de Kaspersky Lab.

Kaspersky Lab detectó a ‘Careto’ por primera vez el año pasado, cuando observaron intentos de aprovechar una vulnerabilidad en los productos de la compañía y se descubrió que ha estado involucrada en operaciones globales de ciberespionaje al menos desde 2007, actualmente todos sus productos detectan y eliminan todas las versiones conocidas de este malware.

La ‘Máscara’ ha utilizado subdominios web que simulan ser periódicos internacionales como The Guardian, The Washington Post, entre otros, y también amenaza a plataformas como Android y iOS.

Fuente: cnnexpansion