Un malware tipo botnet denominado Win32/Napolar afectó a usuarios de Facebook en Latinoamérica, en especial de Perú, Ecuador y Colombia, informa la firma de soluciones de seguridad Eset.

El virus, detalla la compañía, tiene diversos propósitos, entre los que destacan ataques por servicios de Denegación de Servicios (Dos), así como el robo de información de sistemas infectados y se cree que se propaga vía Facebook.

El laboratorio de investigación de la firma detectó que dicho código malicioso puede robar las credenciales de la red social, las cuales pueden ser usadas por el ciberdelincuente para enviar mensajes desde las cuentas comprometidas y tratar de infectar a los amigos de la víctima.

Según informa, el malware extrae los datos que la víctima ingresó en distintos navegadores y sitios web, y ya se han detectado miles de infecciones en la región de Latinoamérica.

El especialista de Awareness & Research de Eset Latinoamérica, André Goujon, subrayó: “Es importante recordar que el usuario debe considerar los riesgos a los que se enfrenta si no utiliza de forma adecuada un dispositivo móvil”. Lo anterior, abunda el experto, es aún de mayor relevancia si se considera que, según una encuesta reciente, 73.9 por ciento de los usuarios de América Latina no respalda la información que almacena en sus equipos. La firma de soluciones de seguridad argumenta que también fueron detectadas vulnerabilidades en iOS 7, las cuales permitían acceder a aplicaciones de los dispositivos sin la necesidad de ingresar un código de desbloqueo. Además, se evidenció la posibilidad de engañar al lector de huellas dactilares incorporado en el iPhone 5s, aunque Apple publicó la actualización 7.0.2 que solucionó dicha vulnerabilidad. En cuanto al lector de huellas dactilares y al método de bloqueo para iPhone, Goujon recomendó habilitar la clave extensa en lugar de los cuatro dígitos por defecto para proteger el dispositivo de accesos no autorizados a la información, actualizar iOS a su última versión, implementar el tipo de bloqueo antes mencionado y modificar algunos parámetros de privacidad.

Amenazas | Más

“App”

También fue detectada una aplicación falsa para Android que simula ser Adobe Flash y fue propagada vía Google Play, lo destacable, dice Eset, fue que los responsables de desarrollar la falsa herramienta se ocuparon de asuntos de ingeniería social, como la descripción, iconos y tipografías de Adobe.

Asimismo, se descubrió Hesperbot, un troyano bancario diseñado para Windows con componentes maliciosos que funcionan en Android, BlackBerry y Symbian, lo que demuestra que los cibercriminales todavía aprovechan plataformas tradicionales, además de las móviles, para obtener beneficios económicos.

Fuente: notimex