Un troyano en Latinoamérica que secuestra datos: cómo evitarlo

ESET ha descubierto un virus llamado **Nymaim** que es capaz de introducirse en los equipos y extorsionar a las víctimas a donar 150 dólares a cambio de poder volver a controlar sus propios terminales.

Dice la empresa que "en el último tiempo, se ha registrado en la región un importante aumento de casos de códigos maliciosos que cifran la información o bloquean el **acceso del sistema a cambio de dinero**" (una práctica conocida como ransomware).

Por otro lado, destaca ESET que ha encontrado un fallo en la aplicación WhatsApp y que podría permitir que un tercero intercepte y descifre los mensajes que se transmiten a través de esta aplicación de mensajería instantánea.

Según explica André Goujon Especialista de Awareness & Research, en el bog de ESET, "los casos de códigos maliciosos del tipo ransomware han aumentado en los últimos meses tanto en el mundo como en América Latina". Los ciberdeliencuentes son capaces, mediante este virus de robar directamente información sensible, y extorsionar la víctima cifrando los datos del usuario o imposibilitando el acceso al sistema operativo. Posteriormente, los cibercriminales solicitan una suma de dinero, como sucede con **Nymaim**.

La firma de seguridad advierte que "pagar por el rescate no hace más que incentivar dicho modelo de negocio ilícito, por lo tanto, en ninguna circunstancia es recomendable hacerlo". Por ello, los expertos de seguridad recomiendan a los usuarios contar con copias de seguridad de su información importante, para que sea fácil recuperar los datos "secuestrados". Asimismo y debido a la complejidad de algunas muestras, en ciertos casos resulta prácticamente imposible recuperar la información cifrada si no se cuenta con la copia de seguridad adecuada.

Además se ha identificado un error en la implementación del sistema de cifrado de WhatsApp que facilita que un tercero pueda obtener las conversaciones de un usuario debido a la estructura predecible de los mensajes. ESET recomienda, en espacios públicos, utilizar tecnología 3G/4G frente a otros tipos de conexiones inalámbricas.