Hay cada vez más un creciente llamado a las empresas y usuarios domésticos, para actualizar las instalaciones existentes de Windows XP, a versiones más recientes de Windows, al menos para la mejora de la seguridad y apoyo.

Los cajeros automáticos son las computadoras que controlan el acceso a dinero en efectivo , y resulta que casi el 95 por ciento de ellos operan con versiones de Windows XP.

Con el inminente final de la vida útil para Windows XP, el cual dejará de ser actualizado por Microsoft a partir del próximo ocho de abril, el sector bancario se enfrenta a un grave riesgo de ataques cibernéticos dirigidos a toda su flota de ATM. Este riesgo ya está sucediendo actualmente en diversos países, por lo que los ciberdelincuentes están atacando los cajeros automáticos con técnicas cada vez más sofisticadas.

A finales de 2013, Symantec dio a conocer en su blog sobre un nuevo malware contra cajeros y que fue identificado en México. Mediante este malware se vulneraba los cajeros automáticos que arrojaban dinero en efectivo mediante la utilización de un teclado externo.

Esa amenaza fue nombrada Backdoor.Ploutus. Algunas semanas más tarde, la firma antivirus descubrió una nueva variante que mostró que el malware evolucionó hasta convertirse en una arquitectura modular. La nueva variante también se localizó en inglés, lo que sugiere que el autor de malware estaba expandiendo su franquicia a otros países. La nueva variante fue identificado como Backdoor.Ploutus.B.

Lo interesante de esta variante del Ploutus, asegura Symantec, es que permite a los cibercriminales, solamente con el envío de un SMS al cajero automático intervenido, recoger el dinero en efectivo dispensado por la máquina.

¿Cómo opera este nuevo virus?

-El atacante instala Ploutus en el cajero automático y se conecta un teléfono móvil a la máquina con un cable USB.

-El controlador envía dos mensajes SMS al teléfono móvil en el interior del cajero automático.

-El SMS 1 debe contener un ID de activación válido para permitir Ploutus en el cajero automático.

-ElSMS 2 debe contener un comando de dispensación válida para obtener el dinero.

-El teléfono detecta los mensajes entrantes válidos y las envía a la ATM como un paquete TCP o UDP.

-En el cajero automático, el módulo de monitor de paquetes de red recibe el paquete TCP / UDP y si contiene un comando válido, ejecutará Ploutus.

-Ploutus hace que el cajero automático para arrojar el dinero en efectivo. La cantidad de dinero en efectivo dispensado es pre-configurado dentro del malware.

-El dinero se recoge de la ATM.

Fuente: Vanguardia