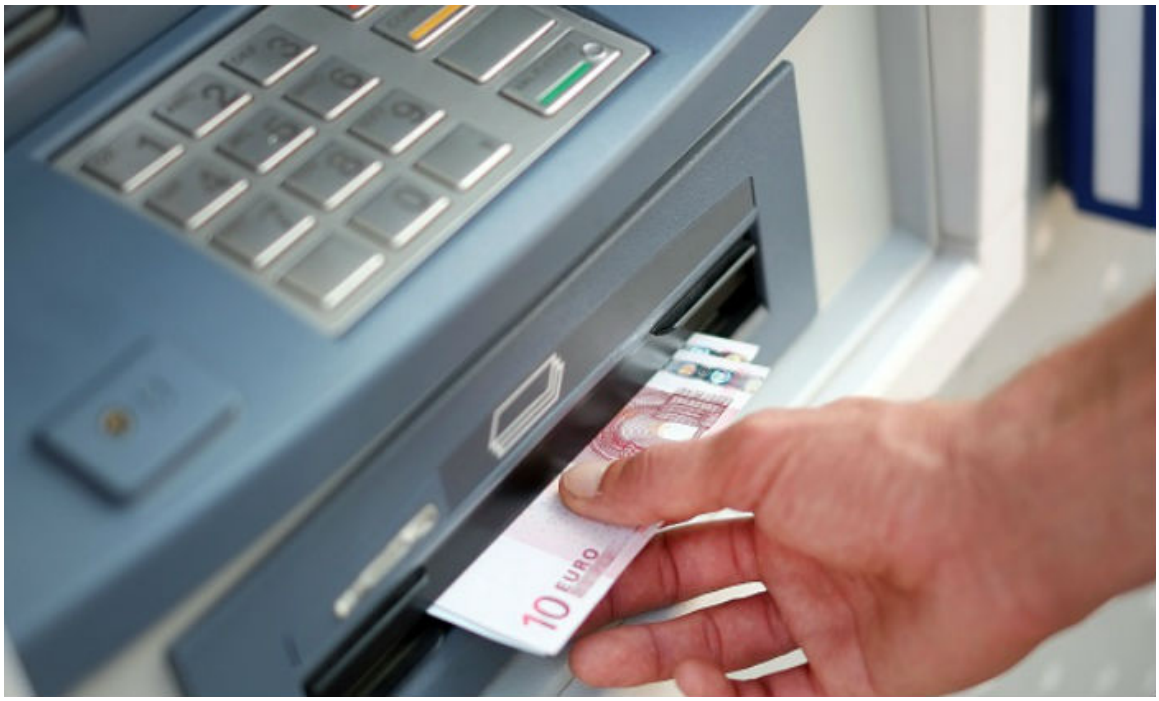
elEconomista.es

Localizado en España un virus que infecta cajeros automáticos para clonar tarjetas

elEconomista.es 19/05/2016 - 17:04



Getty.

Skimer fue el primer programa malicioso, descubierto en 2009, para atacar cajeros automáticos. Ahora, siete años más tarde, los cibercriminales están reutilizando una versión evolucionada del mismo lo que supone una amenaza mucho más grave para los bancos y sus clientes. El malware se extiende por una amplia distribución geográfica ya que se ha localizado en una docena de países, entre los que se encuentra España, según ha explicado Kaspersky Lab.

Skimer inicia sus operaciones al obtener acceso al sistema del cajero automático, ya sea a través del acceso físico o a través de la red interna del banco. Una vez que logra instalarse en el sistema, infecta el núcleo del cajero automático y los cibercriminales pasan a tener el control absoluto de las máquinas que convierten en *skimmers* con el fin de robar información de tarjetas de crédito utilizado en el momento de la transacción, con la finalidad de reproducir o clonar la tarjeta de crédito o débito para su posterior uso fraudulento. Finalmente se elimina la infección para que la detección del rastro de la actividad maliciosa sea más difícil.

Una vez que un cajero automático está infectado con *Backdoor.Win32.Skimer*, los ciberdelincuentes pueden llegar a retirar todos los fondos o robar los datos de las tarjetas utilizadas, aunque existe una gran diferencia de procedimiento entre estas dos opciones. "La retirada de dinero de los casetes se detecta rápidamente, mientras que el malware que roba los datos de las tarjetas puede estar activo por un periodo de tiempo muy largo. Por lo tanto la actividad no es inmediata y son muy cuidadosos ocultando pistas: el malware puede operar en el cajero automático infectado durante varios meses sin realizar ninguna actividad", explican desde Kaspersky Lab.

Para activarlo, es necesario que un cibercriminal inserte una tarjeta concreta, con registros en la banda magnética. Después de leer los registros, Skimer puede ejecutar el comando codificado, o los comandos de solicitud a través de un menú especial activado por la tarjeta. La interfaz gráfica de Skimer aparece en la pantalla cuando se expulsa la tarjeta y el cibercriminal debe insertar la clave de sesión desde el datáfono en menos de 60 segundos.

Desde este menú, el cibercriminal puede activar 21 comandos diferentes, como el de dispensar dinero (40 billetes del casete que se especifica), recogida de datos de las tarjetas insertadas, auto-borrado, actualización (desde el código de malware actualizada incorporado en el chip de la tarjeta), etc. En la mayoría de los casos, los ciberdelincuentes prefieren esperar y recoger los datos de las tarjetas con el fin de crear copias después. Con estas copias se van a un cajero automático diferente, no infectado y retiran dinero de cuentas de los clientes. De esta manera, aseguran que los cajeros automáticos infectados no serán descubiertos a corto plazo.

Amplia distribución geográfica

Skimer se distribuyó ampliamente entre 2010 y 2013, periodo en el que hubo un aumento drástico del número de ciberataques contra cajeros automáticos, con un máximo de nueve familias conocidas de malware diferentes, incluyendo la familia Tyupkin, descubierta en marzo de 2014 y que se ha convertido en la versión más popular extendida. Sin embargo ahora, el laboratorio de ciberseguridad, ha identificado 48 modificaciones de este malware y 37 de ellas van dirigidas a cajeros automáticos. La versión más reciente se descubrió a finales del mes de abril de 201

Des Lab reconocen que "ha sido un reto localizar el inicio de esta actividad. Durante la investigación, el equ s de Kaspersky Lab descubrió la trama criminal así como rastros de una versión mejorada del ma n uno de los cajeros automáticos de un banco. El malware había entrado e instalado un comando que ar en el futuro, una forma inteligente para ocultar los rastros".

En zando muestras de VirusTotal, la compañía ha comprobado que existe una amplia distribución geo cajeros automáticos que pueden estar infectados. Las últimas 20 muestras de la familia Skimer se car de 10 ubicaciones en todo el mundo: Francia, Estados Unidos, Rusia, Macao, China, Filipinas, Esp , Georgia, Polonia, Brasil o República Checa.

Cómo gerse

Par menaza, Kaspersky Lab recomienda hacer análisis regulares de equipo con software especializado y usa e listas blancas, una buena política de gestión de dispositivos, cifrado de disco completo, proteger las jeros automáticos con una contraseña que sólo permita el arranque del disco duro y el aislamiento de l cualquier otra red interna del banco.

"Ex da adicional importante, aplicable en este caso particular. Backdoor.Win32.Skimer comprueba la inf nueve dígitos) de la banda magnética de la tarjeta con el fin de identificar si debe activarse. Hemos det neros codificados utilizados por el malware y están a disposición de los bancos que lo soliciten. Una vez úmeros, los pueden buscar de forma proactiva dentro de sus sistemas, detectar los cajeros aut ncialmente infectados y las mulas de dinero, o bloquear cualquier intento de activar el malware", afir ovanov, analista principal de Seguridad de Kaspersky Lab.

Otras noticias

El resumen anual del IVA no interrumpe la prescripción

Alstom fabricará en Alemania su primer tren de pila de hidrógeno…

La ONU alerta sobre una tercera fase de la crisis financiera que desatará una…

Pedro Sánchez y la inteligencia política

Contenido patrocinado

Olvídate de los robos de coche gracias a este dispositivo. Ya en España
(Ahorrando en la Red)

Consejos para poner a punto un portátil
(IDG)

Los Desplomes de La Bolsa son Oportunidades de Invertir
(Vici)

Entérate hasta donde ha bajado ya el precio de los coches híbridos y eléctricos
(AutoScout24)