Se ha observado una nueva variedad de malware para cajeros automáticos denominada FiXS, que está dirigida a bancos mexicanos desde inicios de febrero de 2023.

> *«El malware para cajeros automáticos está oculto dentro de otro programa que no parece malicioso»,* dijo la compañía latinoamericana de ciberseguridad Metabase Q.

Además de requerir la interacción por medio de un teclado externo, el malware para cajeros automáticos basado en Windows también es independiente del proveedor y es capaz de infectar cualquier cajero automático que admita CEN/XFS (abreviatura de extensiones para servicios financieros).

Se desconoce el modo exacto de compromiso, pero Dan Regalado de Metabase Q le dijo a THN que es probable que *«los atacantes hayan encontrado una forma de interactuar con el cajero automático a través de la pantalla táctil».*

También se cree que FiXS es similar a otra variedad de malware para cajeros automáticos con nombre en código Ploutus que ha permitido a los ciberdelincuentes extraer efectivo de los cajeros automáticos usando un teclado externo o enviando un mensaje SMS.

Una de las características notables de FiXS es su capacidad de dispensar dinero 30 minutos después del último reinicio del cajero automático aprovechando la API GetTickCount de Windows.

La muestra analizada por Metabase Q se entrega a través de un cuentagotas conocido como Nesha (conhost.exe), un virus que infecta archivos, codificado ne Delphi y que fue detectado inicialmente en 2003.

> *«FiXS se implementa con las API CEN XFS que ayudan a ejecutarse principalmente en todos los cajeros automáticos basados en Windows con pequeños ajustes, similar a otro malware como RIPPER. La forma en que FiXS interactúa con el*

> *criminal es a través de un teclado externo»,* dijo la compañía de seguridad cibernética.

Con este desarrollo, FiXS se convierte en el último de una larga lista de malware como Ploutus, Prilex, SUCEFUL, GreenDispenser, RIPPER, Alice, ATMitch, Skimer y ATMii, que se han dirigido a los cajeros automáticos para el desvío de dinero.

Desde entonces, Prilex también se ha convertido en un malware modular de punto de venta (PoS) para realizar fraudes con tarjetas de crédito por medio de una variedad de métodos, incluyendo el bloqueo de transacciones de pago sin contacto.

> *«Los ciberdelincuentes que comprometen las redes tienen el mismo objetivo final que aquellos que realizan ataques por medio del acceso físico: entregar efectivo»* dijo Trend Micro en un informe detallado sobre malware para cajeros automáticos publicado en septiembre de 2017.

> *«Sin embargo, en lugar de instalar malware manualmente en los cajeros automáticos por medio de USB o CD, los delincuentes ya no necesitarían ir a las máquinas. Tienen mulas de dinero en espera que recogerían el efectivo y se irían».*