Nombre de la Materia:

Taller de Legislación Informática

Act 1
Delito informático

Unidad: 6

Profesora:

Daniela Adriana Sanchez Vizcarra

Alumno(s):
Gasca Aguilar Jaaziel Alberto (20212552)
Paniagua Armenta Paola (20213032)
Patiño Espinoza Jose Fernando (20210950)

Fecha de entrega:

31/Mayo/2022

Delito informático:

Este delito informático se originó en el 2019 y fue un ataque a usuarios corporativos de bancos en Brasil a través de envíos de formularios que eran falsos y solo extraían la información de la víctima.

En abril del 2021 desde ESET Research se publicó un reporte en el cual se analiza un troyano bancario enfocado en usuarios corporativos de Brasil. Se denomina como "Familia de malware" en referencia a su principal técnica: el uso de ventanas emergentes falsas especialmente diseñadas que se superponen y se hacen pasar por el sitio web de distintos bancos populares de Brasil. De esta manera, el troyano intenta engañar a la potencial víctima mostrando un formulario falso para que ingrese datos personales que serán enviados automáticamente al atacante.

Al momento del primer análisis, una de las características más destacables que observamos en Janeleiro era que cada vez que se ejecutaba en un equipo comprometido descargaba las IP de los servidores de Comando y Control (C&C), y desde este repositorio era actualizado diariamente por los atacantes a fin de mantener al troyano constantemente en contacto con ellos para poder monitorear a sus víctimas.

A raíz de esto se ha identificado una variante que ha llegado al país de México, que está monitorea a la víctima y le presenta los formularios falsos de bancos que le puedan permitir el robo de información confidencial.
Normalmente este tipo de formularios los aplican cuando la víctima esta haciendo una compra o se trata de hacer una operación en línea y llega un correo para validar lo que son los datos, es una simulación como si te estuvieras metiendo a la página oficial del banco.

Después de que se logra infectar el equipo a través de los formularios, el malware Janeleiro monitorea activamente las ventanas que la víctima abre y compara el nombre de dichas ventas con los nombres disponibles a los bancos a los que intentara acceder para así poder manipular los formularios bancarios y la información.

Referencias

Garduño, M. (2021, 2 agosto). *Conoce cómo blindarte del malware Janeleiro que llegó a México*. Forbes México. Recuperado 31 de mayo de 2022, de https://www.forbes.com.mx/tecnologia-conoce-como-blindarte-malware-janeleiro-llego-mexico/?fbclid=IwAR0HJLh_s31yclimReuDTiYiDjpHxWsMdZZMQKfNHC5--ZTQmonln2CtDUY

Metabase Q - Informe sobre amenaza Janeleiro.mx. (s. f.). . Recuperado 31 de mayo de 2022, de https://www.metabaseq.com/recursos/janeleiro-mx-la-nueva-variante-infectando-tarjetahabientes-en-mexico