Seguridad de la Información basada en el estudio de Troyanos Bancarios

Bismark Francachs Castro
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
bfrancachs@gmail.com

***Resumen*—La implementación de la tecnología en el Sistema Financiero representa un avance en la simplificación de procesos que requerían la presencia física de clientes y usuarios en oficinas de las entidades, además de representar la reducción de costos y tiempo de atención. Esto también implica que el uso de la tecnología también se convierte en una preocupación para dichas instituciones, no solo porque la reglamentación exija que se apliquen estándares que aseguren la información de las entidades, usuarios y clientes, sino también porque la complejidad de los ataques dirigidos al robo de datos en el sistema financiero se va volviendo cada vez más sofisticado y evoluciona a la par de la con la tecnología. Entre estas amenazas las que permanecen latentes son los Troyanos Bancarios, los cuales pese a la legislación y modelos de seguridad implementados siguen como una amenaza activa en el ciberespacio.**

Palabras clave—Sistema, Tecnología, Troyano, Ciberataques, Fraude, Delincuente Informático.

I. Introducción

El fenómeno causado por el uso de las Tecnologías de la Información y Comunicación en el siglo XXI ha permitido que las personas puedan acortar distancias en comunicación y simplificar tareas que antes debían ser realizadas de forma presencial.

Esto ha permitido que empresas de diversos rubros puedan aplicar tecnología en sus procesos simplificando los mismos y bajando los costos operativos, además de beneficiar a clientes o usuarios mediante el uso de servicios tecnológicos. De esta forma se ha creado un ambiente de competitividad entre las empresas, para poder brindar un mejor servicio y así obtener la ventaja. Entre estas empresas se encuentran las del rubro financiero, las cuales han adecuado su modelo de negocio de acuerdo con el avance de la tecnología y exigencia de sus clientes y usuarios, esto con el fin de brindar un servicio más rápido, eficiente y seguro [1].

Cuando se habla de seguridad, este se convierte en uno de los aspectos que más preocupa a las instituciones financieras, ya que no solo deben cumplir con los entes regulatorios respecto a la seguridad de la información que manejan, sino que también deben brindar la seguridad a los clientes y usuarios de que su dinero y otros datos personales están siendo manejados de forma adecuada y no corren riesgo de ser perjudicados al usar los servicios de estas instituciones por medios tecnológicos. En este escenario se puede observar por sobre todo la implementación de pagos vía medios electrónicos y transferencias entre cuentas.

El ingreso del sistema financiero en la era tecnológica ha llamado la atención de organizaciones criminales y delincuentes informáticos, los cuales buscan hacerse con la información que es manejada tanto por las empresas del rubro financiero como por los clientes que hacen uso de los servicios tecnológicos.

Para esto los delincuentes informáticos buscan diferentes formas de realizar ataques informáticos que comprometan la infraestructura y sistemas de estas instituciones, así como los dispositivos de los usuarios.

Entre los ataques más comunes se pueden citar por ejemplo el Phishing o los Virus Troyanos, identificados específicamente en los Campos de la Seguridad Informática y Seguridad de la Información como Troyanos Bancarios.

En este artículo se hará un repaso sobre la evolución de los Troyanos Bancarios y como esta evolución podría ayudar a mejorar sus niveles de seguridad.

II. Marco Teórico

A. *Implementación de Tecnología en el Sistema Financiero*

Si se quiere hablar del uso de la tecnología en el Sistema financiero hasta llegar al concepto de la digitalización financiera debemos remontarnos al año 1914 donde la Empresa Western–Union, crea la primera tarjeta para sus clientes selectos con la finalidad de dar un trato preferente a sus clientes sino también de brindarles una línea de crédito y así fidelizar a sus clientes, este modelo fue replicado por diferentes instituciones [2].

En el año 1948 se crean las tarjetas de crédito como las conocemos en la actualidad, esto con el fin de poder usar las tarjetas para realizar pagos en diferentes establecimientos. En 1958 se lanzan las tarjetas American Express y Bank Of América la cual se convertiría más adelante en VISA [2].

En 1968 El primer dispositivo de cajero automático es creado de forma anecdótica por John Sheperd-Barron, al cual se le ocurre la idea debido a que no pudo hacer el cobro de un cheque en Londres debido a que la sucursal del Banco donde debía cobrarlo se encontraba cerrada [2].

En 1994 con los inicios del Internet aparece la Banca On-Line de Standford Credit Union, lo que desencadena en una revolución en todos los bancos para que a principios del siglo XXI todos los bancos ofrecían los servicios On-Line [2].

A partir del 2008 se da el gran estallido e irrupción de la digitalización financiera, siendo que a partir de los primeros

Para referenciar este artículo (IEEE):
[N] B. Francachs, «Seguridad de la Información basada en el estudio de Troyanos Bancarios», *Revista PGI. Investigación, Ciencia y Tecnología en Informática,* nº 7, pp. 7-10, 2020.

años del siglo XXI se crean los primeros Smartphones llevando a que en los últimos años y gracias al impacto tecnológico en los sistemas de comunicación las empresas del rubro financiero logran implementar medios tecnológicos cada vez más sofisticados que simplifican no solo las operaciones de las instituciones sino el uso de los servicios a los clientes. Todo esto se debe al movimiento Fintech que encendió la chispa en el mundo digital de la bancarización. Con el Fintech llega el uso de los dispositivos digitales para realizar pagos y transferencias, el uso de la Inteligencia Artificial como herramienta de apoyo en atención al cliente, el Internet de las Cosas y el (IOT) y llegando a utilizarse los siguientes términos en el actual sistema financiero:

Neobancos: Donde todos los servicios financieros se realizan a través de los Smartphones.

Bigtech: Usado por empresas tecnológicas grandes como Google, Amazon Facebook y Apple creando sus propios medios de pago.

Telecos: Que pretenden que el número de teléfono o IBAN se utilice como una cuenta bancaria [2].

B. *Historia de los Troyanos Bancarios*

De la misma manera en que la tecnología ha sido de gran ayuda al sistema financiero se ha convertido en una brecha la cual debe ser monitoreada y controlada por las entidades financieras y los entes reguladores.

Desde los años 80 aparece un escenario, el fraude financiero, el cual es de gran preocupación porque va adoptando nuevas tácticas evolucionando y siendo cada vez más sofisticado con el uso de tecnología.[3]. En la década de los 80 los criminales robaban las tarjetas para cometer los fraudes de forma física, las victimas generalmente se trataban de personas que no tomaban medidas de seguridad adecuadas, utilizando claves simples que incluso quedaban anotadas en las mismas tarjetas.

De la misma manera con la aparición de la Banca On-Line se dio un fenómeno similar solo que esta vez la tecnología juega un papel fundamental en el robo de datos y el fraude informático, esto sucede debido a que los delincuentes informáticos y otras organizaciones delictivas ya no se interesen en el medio físico de acceso al dinero efectivo del usuario, sino a los datos almacenados en los dispositivos y que son intercambiados en las transacciones en puntos de venta.

Evolución del fraude con tarjetas en Europa y Estados Unidos					
	1980	1990	2000	2010	2015
Criminales	Operaban de manera individual	Equipos criminales en ciertos países	Redes de crimen local en ciertos países	Redes de crimen global *hackers*	Redes de crimen global con organizaciones descentralizadas y *hackers*
Blanco/Objetivo	Consumidores	Pequeños comerciantes	Grandes comerciantes	Procesadores de la banca	Toda la Industria del pago
Principales tipos de fraude	Extraviadas, robadas o interceptadas.	Falsificación / clonación.	Falsificación / clonación. *Phishing*, robo de datos financieros en la basura.	Falsificación / clonación. *Skymmer Phishing*, robo de datos financieros en la basura, alteración de cajeros, robo de identidad.	Falsificación / clonación. *Skymmer Phishing*, robo de datos financieros en la basura, alteración de cajeros, robo de identidad. *Pharming, Hacking*
Tipo de plásticos/ tarjetas que son objetivo de fraude	Tarjetas de viajes y entretenimiento	Tarjetas de crédito Premium	Tarjetas de crédito de mercado masivo	Todos los tipos: tarjetas de crédito, tarjetas de débito, tarjetas prepagadas	Todos los tipos: tarjetas de crédito, tarjetas de débito, cuentas bancarias de prepago
Recursos necesarios	Oportunismo o descuido	Conocimiento rudimentario.	Conocimientos técnicos	Conocimientos técnicos	Conocimientos técnicos

Fig. 1. Evolución del fraude con tarjetas en Europa y Estados Unidos extraído de [3]

Existen diferentes tipos de brechas que deben asegurarse dentro del sistema financiero para poder hacer el uso de la tecnología de una manera adecuada. De la misma manera los mecanismos para el robo de información electrónica varían desde la simple pero efectiva ingeniería social, pasando por el Phishing y Keyloggers, Skimmers y los más peligrosos los Virus entre los que se encuentra una clasificación conocida como los Troyanos Bancarios.

Un troyano bancario es un término que identifica a un grupo específico de malware que persigue el robo de datos de cuentas bancarias, con el fin de desviar dinero, hacer operaciones de compra con dinero de las víctimas o subastar los datos obtenidos en sitios de la Dark Net o Deep Web.

Los troyanos bancarios empezaron a aparecer en 2004, donde se notó una evolución en los keyloggers [4].

De acuerdo con un artículo publicado en la página de Universidad libre las familias de troyanos bancarios más populares que efectúan ataques dirigidos contra entidades bancarias. Son las siguientes:

- bancos
- bank
- banker
- silentbanker
- zbot
- sinowal
- torpig
- fraud
- zeus
- infostealer
- ambler
- stealer
- yessim
- yaludle
- banload
- bankpatch
- multibanker
- nethell
- chromeinject
- goldun
- banspy
- bancodoor
- bancodo

C. *Ataques de mayor magnitud*

De acuerdo con un artículo de Juan Manuel Harán, investigador de ESET, los ciberataques más importantes dirigidos al sistema financiero de los últimos tiempos han sido ataques de denegación de servicio DDoS, uso de malware en puntos de venta (POS) o ATM's, explotación de vulnerabilidades y Watering Hole, donde los sitios web son alterados para llevar a cabo actividad maliciosa sin que los usuarios puedan darse cuenta [5].

Entre los ataques más importantes que se pueden citar están los siguientes:

- 2015: Ataques DDos a bancos griegos a cambio de Bitcoins

- 2016: Ataque DDos a la filial del Reino Unido del Banco HSBC dejando sus sistemas fuera de servicio por un tiempo.
- 2017: Se da un ataque a bancos de Polonia y bancos de México y Uruguay utilizando un ataque Watering Hole, en el cual se compromete un sitio de confianza redirigiendo a usuarios a una página fraudulenta que escondía un exploit.

D. *Grupo Magecart*

De acuerdo con un artículo publicado por Panda Security a principios de Julio de 2019 la Aerolínea British Airways fue multada por la Oficina del Comisionado de Información, esto debido a que una brecha de seguridad afecto a 500.000 clientes en 2018 por un robo de datos masivo [6].

Esto fue debido a que un grupo de atacantes identificados como el grupo Magecart inserto código malicioso en las webs de comercio de British Airways haciendo uso de Skimmers Digitales.

Otros sitios afectados fueron los de Ticketmaster, Forbes y Amazon CloudFront.

Según Sanguine Security Magecart dirigió una campaña durante 24 horas que afectó a 962 sitios Web de Comercio Electrónico robando datos bancarios de los usuarios de dichos sitios. Aparentemente el grupo Magecart lleva operando desde 2016.

E. *Situación de los ataques informáticos en Bolivia*

En un artículo publicado en la página del matutino boliviano El Diario del 6 de junio de 2018 en una entrevista a Ángel Mendoza, investigador del grupo ESET Latinoamérica, se advierten sobre los riesgos de los ciberataques no solo en cuanto a pérdidas económicas sino también al daño de la imagen y reputación de las empresas afectadas, resaltando que los sistemas de la banca son los blancos más codiciados por los delincuentes informáticos [7].

III. Resultados

Como resultados preliminares de la investigación que se llevó a cabo para este artículo, se pueden observar que la tendencia al uso de la tecnología en el sistema financiero es un punto en el cual se debe trabajar con mayor énfasis para lograr no solo brindar un servicio eficiente al cliente sino también un servicio que asegure al mismo en todo momento en el que emplea la tecnología para hacer transacciones.

Esto implica que deben estudiarse los mecanismos que usan los delincuentes informáticos con la finalidad de hacer una reingeniería y aprender cómo evolucionan los ataques, cual podría ser su comportamiento a futuro y el cómo podrían las instituciones financieras adelantarse a posibles ataques de malware u otros tipos de ataques informáticos.

De acuerdo con un artículo publicado por Juan Manuel Harán para el blog We Live Security de la compañía ESET, el informe anual de ESET Security Report 2020 revela que a nivel Latinoamérica solo el 33% de las empresas encuestadas cuenta con un plan de continuidad del negocio, donde solo un 28% de las empresas cuenta con la clasificación para su información [8].

En la región el 60% de las empresas de la región también indica haber sufrido por lo menos un incidente en el último año. Siendo Emotet una variante de troyano bancario una de las amenazas con mayor incidencia detectadas en diciembre de 2019 [8].

Dadas las circunstancias a nivel mundial con la pandemia de COVID-19 desatada en Enero del 2020, muchas empresas han tenido que recurrir a la transformación digital de sus negocios sobre todo en el aspecto de cobros de sus servicios por lo cual han trabajado en la implementación de sus propias Aplicaciones y/o usando Aplicaciones de terceros. Siendo las Aplicaciones móviles uno de los estándares utilizado en mayor porcentaje.

El informe sobre malware de Secure List detalla que hasta Septiembre del 2020 se detectaron 1.245.894 paquetes de instalación con código malicioso. De los cuales un 3,13% de los paquetes corresponden a Troyanos Bancarios teniendo una mayor incidencia en el primer trimestre de 2020 [9].

Estas cifras nos llevan a pensar en los estándares y leyes en nuestro país, si bien en nuestro medio el pago electrónico es usado y no se han dado alertas directas en nuestro país respecto a la aparición de troyanos bancarios, no implica que este escenario nunca vaya a materializarse o no se den otras variaciones que impliquen el robo de datos bancarios de usuarios en nuestro medio.

Por esto se debe poner énfasis en el desarrollo seguro de Aplicaciones Web y móviles, siendo que las empresas deben contar con una estrategia para la implementación de su software ya sea propio o por medio de un tercero. Esta estrategia puede tener base en el estudio y entendimiento de los Troyanos Bancarios y servir como una guía para las empresas de Bolivia cuenten o no con áreas y planes de Seguridad de la Información.

La finalidad de este trabajo de investigación es plantear una estrategia para la implementación de software seguro para el ámbito financiero, tomando en cuenta buenas prácticas de seguridad y desarrollo además de basarse en el estudio de los troyanos bancarios y sus variantes.

IV. Discusión

Si bien el Sistema Financiero en Bolivia se encuentra Regulado, y se tienen normas y estándares, habría que preguntarse si estos aseguran y en qué porcentaje que las instituciones financieras puedan operar con tecnología brindando la confiabilidad a sus clientes y usuarios de que la información manejada por ellos no va a ser afectada por algún tipo de ataque.

En Bolivia se tienen antecedentes de desfalcos realizados por personal de instituciones financieras que operaban tecnología, y, aun así, pese los controles de seguridad llegaron a cometer ilícitos. Esto nos lleva a preguntarnos que, si los usuarios internos pueden afectar de esta manera a una institución, ¿Cómo podría afectar uno de estos ataques a los clientes o instituciones financieras si se lleva a cabo desde afuera de la institución?, ¿y cómo se podrían anticipar las instituciones a que estas eventualidades sucedan? [10].

V. Conclusiones

El uso de los estándares de seguridad no garantiza al 100% que eventualidades o incidentes informáticos puedan materializarse.

Antes de usar o crear un nuevo estándar se debe aprender de los incidentes informáticos y los diversos ataques y como estos

podrían evolucionar para plantear una estrategia de defensa más eficiente.

REFERENCIAS

[1] Artículo sobre Tendencias en la Tecnología en Banca Recurso disponible en: https://blog.atrivity.com/es/tendencias-tecnologia-en-banca

[2] Artículo sobre 100 Años de la Digitalización Financiera. La Evolución de la Tecnología en las Finanzas Recurso disponible en: https://nuevofinanciero.com/digitalizacion-financiera-evolucion/

[3] Artículo sobre Evolución del Fraude Financiero Recurso disponible en: https://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/829-evolucion-del-fraude-financiero

[4] Artículo sobre ¿Qué son y cómo funcionan los troyanos bancarios? Recurso disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/260-que-son-y-como-funcionan-los-troyanos-bancarios

[5] Artículo sobre Los ciberataques dirigidos a bancos más importantes de los últimos tiempos recurso disponible en: https://www.welivesecurity.com/la-es/2018/06/01/ciberataques-dirigidos-bancos/

[6] Artículo sobre Magecart una Amenaza para el comercio Electrónico Recurso disponible en: https://www.pandasecurity.com/spain/mediacenter/noticias/magecart-amenaza-comercio-electronico/

[7] Artículo sobre Ciberataques al sistema Financiero en Bolivia Recurso disponible en: https://www.eldiario.net/noticias/2018/2018_06/nt180606/economia.php?n=29&-ciberataques-ocasionan-danio-y-costos-al-sistema-bancario

[8] Artículo sobre empresas con planes de continuidad del negocio en América Latina disponible en: https://www.welivesecurity.com/la-es/2020/08/13/un-tercio-empresas-america-latina-tiene-plan-continuidad-negocio/

[9] Artículo sobre Desarrollo de las amenzadas informaticas en el Segundo trimester del 2020 disponible en: https://securelist.lat/it-threat-evolution-q2-2020-mobile-statistics/90975/

[10] Artículo sobre Banca y Desfalcos Recurso disponible en: https://www.paginasiete.bo/inversion/2018/6/3/banca-desfalcos-181981.html

Breve CV del autor

Bismark Francachs Castro es Ingeniero de Sistemas por la Universidad de Aquino, Bolivia. Actualmente realiza la Maestría en Informática Forense, Seguridad de la Información y Auditoria Informática en el Postgrado en Informática UMSA.
Miembro del comité editorial-científico de la Revista PGI – Ciencia, Innovación y Tecnología en Informática (2019-2020).
Miembro del grupo de investigación GI-FORSAI UMSA. Ha trabajado como desarrollador en Banco Solidario S.A., La Boliviana Ciacruz Seguros Personales y en el Gobierno Autónomo Municipal de La Paz.
Email: bfrancachs@gmail.com. ORCID ID: https://orcid.org/0000-0002-2792-8808.