NIVEL

Cliente:

Eduardo Parraguez

khipu

Marzo

2018

INFORME TÉCNICO

Análisis de tráfico de datos aplicación khipu

DOCUMENTO CONFIDENCIAL

https://nivel4.com

+56 2 2248 1368

Av Providencia 1208/ Of. 1204

Santiago. Chile.

1 Control de versiones

El siguiente cuadro muestra el historial de cambios sobre el presente documento.

Fecha	Autor	Versión	Comentarios
05-03-2018	Guillermo Zabra	1.0	Creación del documento
08-03-2018	Kevin Möller	2.0	Confección final del documento

Tabla de contenido

2 Introducción

La aplicación khipu permite a personas y empresas, pagar y cobrar, usando sus cuentas corrientes o cuentas vista del banco, de manera fácil y segura.

El terminal de pago de khipu es un navegador web especializado en pagos, por lo que, valida el correcto uso de las páginas de los bancos, forma parte de un sistema que genera comprobantes de pago firmados electrónicamente, es reconocido por los principales antivirus del mundo y se instala desde fuentes oficiales de cada plataforma.

Adicionalmente, khipu no almacena ni envía claves u contraseñas a sus servidores o a terceros.

El análisis consiste en el monitoreo y análisis de todo el tráfico que genera la aplicación para las distintas plataformas, con el fin de detectar conexiones sospechosas.

Esta revisión incluye las versiones del terminal de pagos disponible para Windows, OSX, Linux, iOS y Android.

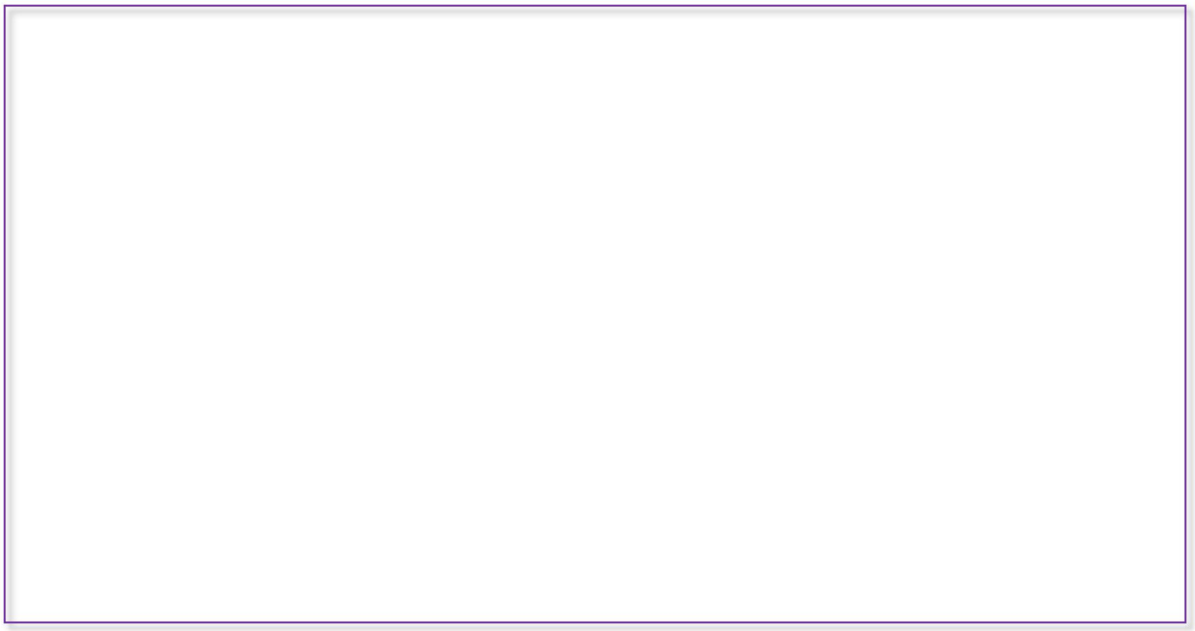
3 Objetivo

El presente análisis se realiza mensualmente, en un día y hora definida por Nivel 4 sin que khipu conozca esta información de antemano y tiene por objetivo certificar que khipu no recibe las claves bancarias de sus usuarios ni las comparte con terceros.

Adicionalmente, se realiza un Ethical Hacking a los terminales de pago móviles en IOS y Android.

4 Metodología

La metodología utilizada para la realización de este análisis de tráfico de red se basa en la utilización de un equipo que captura este tráfico entre el terminal de pagos y los bancos, de acuerdo al diagrama a continuación:



Esta u otras metodologías pueden ser realizadas por cualquier organización o persona natural que así lo requiera.

5 Ámbito

Para el actual periodo se registraron cambios para las aplicaciones de **Android,** y en el caso de **iOS** durante este periodo solo fue posible ver un cambio en su **HASH.**

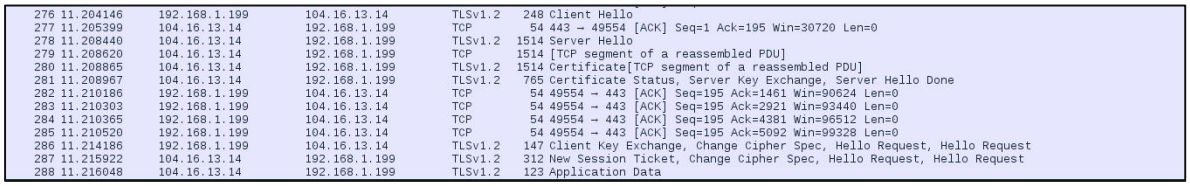
Plataforma	Versión	SHA256SUM
Android	**6.6.31**	**08f86f67118ed597440dd7306f250c0e61a4349f823b4b5aae5b533be17935b2**
iOS	**6.22**	**1fab5d1b4b5a1de2003e8a4b2a63e4c760c45b9a82398ae2238f4a7d65e70e24**
Linux i386	1.17.1922.1	f5533662c3cabce75ecc9d6fdf9632ffb189941533f4992ef0ed8aaf82e6b1b1
Linux x64	1.17.1922.1	9321ae02910a9dfcd8801ca24c11a43e707a62e8b579bcb4a10d79e0e77c908f
OSX	1.17.1922.1	637f66c0b5c4d04f2291ffc71ee85643980ee3e1e6c171f1caeb3430ff16a577
Windows	1.17.1922.1	e610e91976939e06ee53797db22f97f584c3063ae311ab8fab68a5f81faf071e

6 Análisis de tráfico de datos

Todo el tráfico analizado entre el terminal de pagos y los bancos se estableció mediante un **canal seguro** de comunicación. Finalmente, el resto del tráfico corresponde a consultas **DNS** y tráfico propio de una red local, como **NTP**, **NETBIOS**, **ARP**, entre otros.

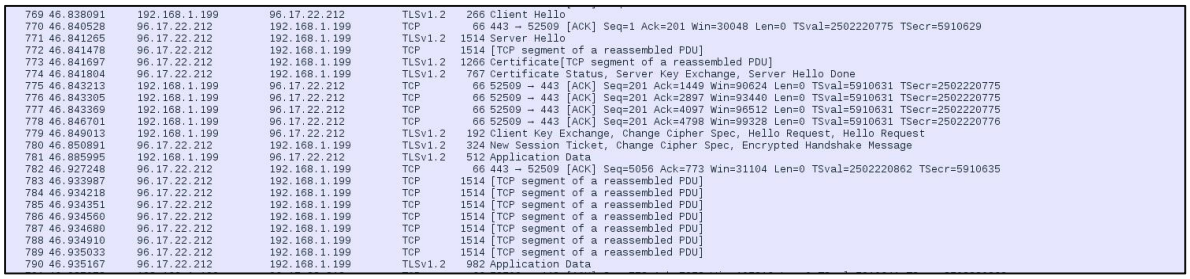
En los siguientes puntos se detalla el tráfico detectado durante el uso de la aplicación evidenciando que las transacciones se realizan de forma segura y no se almacenan datos de usuario como, por ejemplo, claves del banco.

6.1 Tráfico TLS (seguro) entre el terminal de pagos y Banco BCI



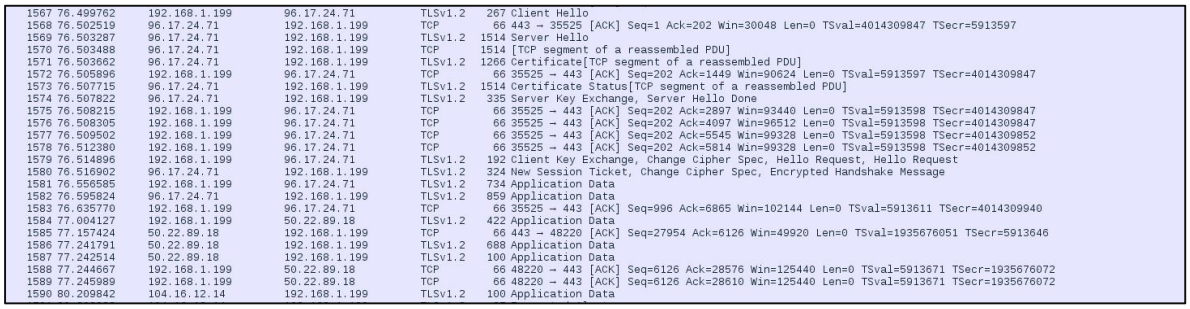
276	11.204146	192.168.1.199	104.16.13.14	TLSv1.2	248 Client Hello
277	11.205399	104.16.13.14	192.168.1.199	TCP	54 443 → 49554 [ACK] Seq=1 Ack=195 Win=30720 Len=0
278	11.208440	104.16.13.14	192.168.1.199	TLSv1.2	1514 Server Hello
279	11.208620	104.16.13.14	192.168.1.199	TCP	1514 [TCP segment of a reassembled PDU]
280	11.208865	104.16.13.14	192.168.1.199	TLSv1.2	1514 Certificate[TCP segment of a reassembled PDU]
281	11.208967	104.16.13.14	192.168.1.199	TLSv1.2	765 Certificate Status, Server Key Exchange, Server Hello Done
282	11.210186	192.168.1.199	104.16.13.14	TCP	54 49554 → 443 [ACK] Seq=195 Ack=1461 Win=90624 Len=0
283	11.210303	192.168.1.199	104.16.13.14	TCP	54 49554 → 443 [ACK] Seq=195 Ack=2921 Win=93440 Len=0
284	11.210365	192.168.1.199	104.16.13.14	TCP	54 49554 → 443 [ACK] Seq=195 Ack=4381 Win=96512 Len=0
285	11.210520	192.168.1.199	104.16.13.14	TCP	54 49554 → 443 [ACK] Seq=195 Ack=5092 Win=99328 Len=0
286	11.214186	192.168.1.199	104.16.13.14	TLSv1.2	147 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
287	11.215922	104.16.13.14	192.168.1.199	TLSv1.2	312 New Session Ticket, Change Cipher Spec, Hello Request, Hello Request
288	11.216048	104.16.13.14	192.168.1.199	TLSv1.2	123 Application Data

6.2 Tráfico TLS (seguro) entre el terminal de pagos y Banco Santander



769	46.838091	192.168.1.199	96.17.22.212	TLSv1.2	266 Client Hello
770	46.840528	96.17.22.212	192.168.1.199	TCP	66 443 → 52509 [ACK] Seq=1 Ack=201 Win=30048 Len=0 TSval=2502220775 TSecr=5910629
771	46.841265	96.17.22.212	192.168.1.199	TLSv1.2	1514 Server Hello
772	46.841478	96.17.22.212	192.168.1.199	TCP	1514 [TCP segment of a reassembled PDU]
773	46.841697	96.17.22.212	192.168.1.199	TLSv1.2	1266 Certificate[TCP segment of a reassembled PDU]
774	46.841804	96.17.22.212	192.168.1.199	TLSv1.2	767 Certificate Status, Server Key Exchange, Server Hello Done
775	46.843213	192.168.1.199	96.17.22.212	TCP	66 52509 → 443 [ACK] Seq=201 Ack=1449 Win=90624 Len=0 TSval=5910631 TSecr=2502220775
776	46.843305	192.168.1.199	96.17.22.212	TCP	66 52509 → 443 [ACK] Seq=201 Ack=2897 Win=93440 Len=0 TSval=5910631 TSecr=2502220775
777	46.843369	192.168.1.199	96.17.22.212	TCP	66 52509 → 443 [ACK] Seq=201 Ack=4097 Win=96512 Len=0 TSval=5910631 TSecr=2502220775
778	46.846701	192.168.1.199	96.17.22.212	TCP	66 52509 → 443 [ACK] Seq=201 Ack=4798 Win=99328 Len=0 TSval=5910631 TSecr=2502220776
779	46.849013	192.168.1.199	96.17.22.212	TLSv1.2	192 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
780	46.850891	96.17.22.212	192.168.1.199	TLSv1.2	324 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
781	46.885995	192.168.1.199	96.17.22.212	TLSv1.2	512 Application Data
782	46.927248	96.17.22.212	192.168.1.199	TCP	66 443 → 52509 [ACK] Seq=5056 Ack=773 Win=31104 Len=0 TSval=2502220862 TSecr=5910635
783	46.933987	96.17.22.212	192.168.1.199	TCP	1514 [TCP segment of a reassembled PDU]
784	46.934218	96.17.22.212	192.168.1.199	TCP	1514 [TCP segment of a reassembled PDU]
785	46.934351	96.17.22.212	192.168.1.199	TCP	1514 [TCP segment of a reassembled PDU]
786	46.934560	96.17.22.212	192.168.1.199	TCP	1514 [TCP segment of a reassembled PDU]
787	46.934680	96.17.22.212	192.168.1.199	TCP	1514 [TCP segment of a reassembled PDU]
788	46.934910	96.17.22.212	192.168.1.199	TCP	1514 [TCP segment of a reassembled PDU]
789	46.935033	96.17.22.212	192.168.1.199	TCP	1514 [TCP segment of a reassembled PDU]
790	46.935167	96.17.22.212	192.168.1.199	TLSv1.2	982 Application Data

6.3 Tráfico TLS (seguro) entre el terminal de pagos y Banco Scotiabank



1567	76.499762	192.168.1.199	96.17.24.71	TLSv1.2	267 Client Hello
1568	76.502519	96.17.24.71	192.168.1.199	TCP	66 443 → 35525 [ACK] Seq=1 Ack=202 Win=30048 Len=0 TSval=4014309847 TSecr=5913597
1569	76.503287	96.17.24.71	192.168.1.199	TLSv1.2	1514 Server Hello
1570	76.503488	96.17.24.71	192.168.1.199	TCP	1514 [TCP segment of a reassembled PDU]
1571	76.503562	96.17.24.71	192.168.1.199	TLSv1.2	1266 Certificate[TCP segment of a reassembled PDU]
1572	76.505896	192.168.1.199	96.17.24.71	TCP	66 35525 → 443 [ACK] Seq=202 Ack=1449 Win=90624 Len=0 TSval=5913597 TSecr=4014309847
1573	76.507715	96.17.24.71	192.168.1.199	TLSv1.2	1514 Certificate Status[TCP segment of a reassembled PDU]
1574	76.507822	96.17.24.71	192.168.1.199	TLSv1.2	335 Server Key Exchange, Server Hello Done
1575	76.508215	192.168.1.199	96.17.24.71	TCP	66 35525 → 443 [ACK] Seq=202 Ack=2897 Win=93440 Len=0 TSval=5913598 TSecr=4014309847
1576	76.508305	192.168.1.199	96.17.24.71	TCP	66 35525 → 443 [ACK] Seq=202 Ack=4097 Win=96512 Len=0 TSval=5913598 TSecr=4014309847
1577	76.509502	192.168.1.199	96.17.24.71	TCP	66 35525 → 443 [ACK] Seq=202 Ack=5545 Win=99328 Len=0 TSval=5913598 TSecr=4014309852
1578	76.512380	192.168.1.199	96.17.24.71	TCP	66 35525 → 443 [ACK] Seq=202 Ack=5814 Win=99328 Len=0 TSval=5913598 TSecr=4014309852
1579	76.514896	192.168.1.199	96.17.24.71	TLSv1.2	192 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
1580	76.516902	96.17.24.71	192.168.1.199	TLSv1.2	324 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1581	76.556585	192.168.1.199	96.17.24.71	TLSv1.2	734 Application Data
1582	76.595824	96.17.24.71	192.168.1.199	TLSv1.2	859 Application Data
1583	76.635770	192.168.1.199	96.17.24.71	TCP	66 35525 → 443 [ACK] Seq=996 Ack=6865 Win=102144 Len=0 TSval=5913611 TSecr=4014309940
1584	77.004127	192.168.1.199	50.22.89.18	TLSv1.2	422 Application Data
1585	77.157424	50.22.89.18	192.168.1.199	TCP	66 443 → 48220 [ACK] Seq=27954 Ack=6126 Win=49920 Len=0 TSval=1935676051 TSecr=5913646
1586	77.241791	50.22.89.18	192.168.1.199	TLSv1.2	688 Application Data
1587	77.242514	50.22.89.18	192.168.1.199	TLSv1.2	100 Application Data
1588	77.244667	192.168.1.199	50.22.89.18	TCP	66 48220 → 443 [ACK] Seq=6126 Ack=28576 Win=125440 Len=0 TSval=5913671 TSecr=1935676072
1589	77.245989	192.168.1.199	50.22.89.18	TCP	66 48220 → 443 [ACK] Seq=6126 Ack=28610 Win=125440 Len=0 TSval=5913671 TSecr=1935676072
1590	80.209842	104.16.12.14	192.168.1.199	TLSv1.2	100 Application Data

https://nivel4.com

+56 2 2248 1368

6.4 Tráfico DNS

No.	Time	Source	Destination	Protocol	Length	Info
266	11.039391	192.168.1.199	192.168.1.1	DNS	70	Standard query 0xec92 A www.bci.cl
272	11.178803	192.168.1.1	192.168.1.199	DNS	145	Standard query response 0xec92 A www.bci.cl CNAME www.bci.cl.cdn.cloudflare.net A 104.16.13.14 A 104.16.12.14

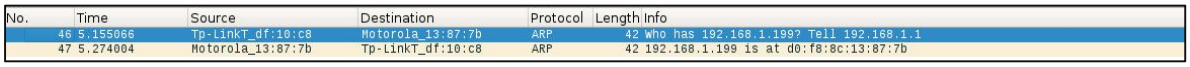
No.	Time	Source	Destination	Protocc	Length	Info
266	11.039391	192.168.1.199	192.168.1.1	DNS	70	Standard query 0xec92 A www.bci.cl
272	11.178803	192.168.1.1	192.168.1.199	DNS	145	Standard query response 0xec92 A www.bci.cl CNAME www.bci.cl.cdn.cloudflare.net A 104.16.13.14 A 104.16.12.14
358	11.426808	192.168.1.199	192.168.1.1	DNS	76	Standard query 0xcb54 A bci.modyocdn.com
359	11.568983	192.168.1.1	192.168.1.199	DNS	156	Standard query response 0xcb54 A bci.modyocdn.com A 104.16.204.140 A 104.16.205.140 A 104.16.208.140 A 104.16.206.140 A 104.16.207.140
360	11.659125	192.168.1.199	192.168.1.1	DNS	76	Standard query 0xe291 A www.facebook.com
361	11.661721	192.168.1.1	192.168.1.199	DNS	121	Standard query response 0xe291 A www.facebook.com CNAME star-mini.c10r.facebook.com A 31.13.69.228
366	11.854219	192.168.1.199	192.168.1.1	DNS	80	Standard query 0xdeac A connect.facebook.net
377	11.992850	192.168.1.1	192.168.1.199	DNS	128	Standard query response 0xdeac A connect.facebook.net CNAME scontent.xx.fbcdn.net A 179.60.193.20
764	46.654329	192.168.1.199	192.168.1.1	DNS	76	Standard query 0xa5df A www.santander.cl

No.	Time	Source	Destination	Protocol	Length	Info
1562	75.593982	192.168.1.199	192.168.1.1	DNS	77	Standard query 0x923c A www.scotiabank.cl
1563	75.733299	192.168.1.1	192.168.1.199	DNS	170	Standard query response 0x923c A www.scotiabank.cl CNAME www.scotiabank.cl.edgekey.net CNAME e10175.b.akamaiedge.net A 96.17.24.71

6.5 Tráfico HTTP

Durante este periodo no se fue posible detectar tráfico HTTP.

6.6 Otro Tráfico



No.	Time	Source	Destination	Protocol	Length	Info
46	5.155066	Tp-LinkT_df:10:c8	Motorola_13:87:7b	ARP	42	Who has 192.168.1.199? Tell 192.168.1.1
47	5.274004	Motorola_13:87:7b	Tp-LinkT_df:10:c8	ARP	42	192.168.1.199 is at d0:f8:8c:13:87:7b

https://nivel4.com

+56 2 2248 1368

6.7 Análisis del terminal de pagos

Como se puede ver en las siguientes tablas el tráfico que se genera al utilizar la aplicación de khipu, solo se realiza con servidores confiables mediante canales seguros.

6.7.1 Android

Origen	Destino	Tipo de Tráfico	Descripción
192.168.1.199	50.22.89.18	TLSv1.2	Khipu
192.168.1.199	104.16.13.14	TLSv1.2	Banco BCI
192.168.1.199	96.17.22.212	TLSv1.2	Banco Santander
192.168.1.199	96.17.24.71	TLSv1.2	Banco Scotiabank

7 Análisis SSL

El siguiente análisis tiene como objetivo determinar el nivel de seguridad en la implementación de SSL/TLS, se realizarán pruebas para determinar si se ve afectado por las vulnerabilidades conocidas hasta el momento.

7.1 khipu.com – 50.22.89.18 puerto 443

Vulnerabilidad	Identificador	Estado	Observaciones
Heartbleed	CVE-2014-0160	✓	No vulnerable
CCS	CVE-2014-0224	✓	No vulnerable
ROBOT	CVE-2017-17382	✓	No vulnerable
Secure Renegotiation	CVE-2009-3555	✓	No vulnerable
Secure Client-Initiated Renegotiation	CVE-2011-1473	✓	No vulnerable
CRIME	CVE-2012-4929	✓	No vulnerable
BREACH	CVE-2013-3587	✓	No vulnerable
POODLE	CVE-2014-3566	✓	No vulnerable
TLS_FALLBACK_SCSV	RFC 7507	✓	No vulnerable
SWEET32	CVE-2016-2183	✓	No vulnerable
FREAK	CVE-2015-0204	✓	No vulnerable
DROWN	CVE-2016-0703	✓	No vulnerable
LOGJAM	CVE-2015-4000	✓	No vulnerable

BEAST	CVE-2011-3389	✗	Vulnerable
LUCKY13	CVE-2013-0169	✗	Vulnerable
RC4	CVE-2013-2566 CVE-2015-2808	✓	No vulnerable

Se detectaron 2 vulnerabilidades en la implementación de SSL/TLS del sitio khipu.com las que afectan la confidencialidad de la información, sin embargo, estas vulnerabilidades tienen un alto grado de dificultad de explotación y se requieren condiciones especiales para su correcta explotación.

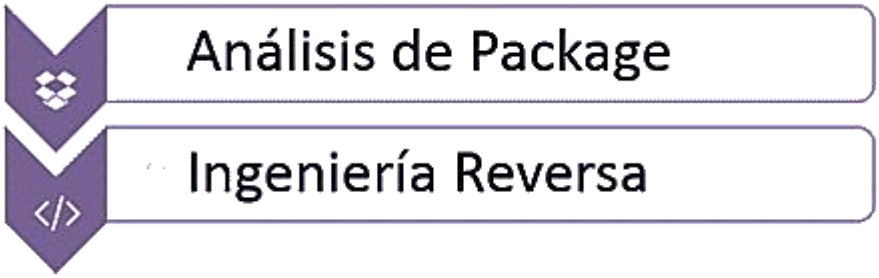
7.2 Referencias

Nombre	Link de referencia
Heartbleed	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
ROBOT	https://robotattack.org/
BREACH	http://breachattack.com/
POODLE	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555
FREAK	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204
Logjam	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
BEAST	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3389
RC4	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2566
SLOTH	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7575
DROWN	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0800
Padding Oracle	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2107

SWEET32	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2183
LUCKY13	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0169

8 Ethical Hacking Mobile

8.1 Procesos automatizados y verificación manual



Desempaquetado
Decompilación
Análisis de integridad
Análisis de metadatos
Análisis de strings
Búsqueda con expresiones regulares
Análisis en VirusTotal (malware)

Análisis de Package: Se analiza de forma estática el paquete compilado para los distintos sistemas operativos. En caso de Android se analiza el archivo APK y en el caso de iOS (para iPhone) el archivo IPA. Estos paquetes son sometidos a distintos tipos de análisis que verifican su integridad y seguridad.

Ingeniería Reversa: Durante este proceso las aplicaciones son decompiladas con el fin de realizar un análisis de código. Este tipo de análisis permite detectar malas prácticas de desarrollo, fugas de información mediante el código fuente, como direcciones IP, usuarios, claves. Además, permite conocer internamente los distintos componentes que utiliza la aplicación.

8.2 Análisis APK

El resultado del análisis para la aplicación móvil es el siguiente:

Nombre	com.khipu.android-6.6.31.apk
SHA256	08f86f67118ed597440dd7306f250c0e61a4349f823b4b5aae5b533be17935b2
Tamaño	6.76 MB
Tipo	Android
URLs Interesantes	6
IPs encontradas	0
Emails encontrados	0

8.2.1 URLs detectadas

1. https://khipu.com/payment/simplified/
2. https://khipu.com/payment/show/
3. https://khipu.com/payment/end/
4. https://khipu.com/cerebro/
5. https://khipu.com/app/2.0/automaton
6. https//khipi.com/zendesk/support

La cuarta URL tiene un formulario de autenticación al cual se le realizó un ataque de fuerza bruta con un diccionario simple de 2.000.000 de palabras, sin embargo, no se logró obtener ninguna credencial para acceder al sistema. Se recomienda agregar un método de protección para prevenir ataques de fuerza bruta sobre el formulario.

8.2.2 Direcciones IPs detectadas

No se encontraron direcciones IP en el análisis.

8.2.3 Emails detectados

No se encontraron direcciones de correo electrónico en el análisis.

8.2.4 URL detectadas

No se encontraron URL en el análisis

8.2.5 Direcciones IPs detectadas

No se encontraron direcciones IP en el análisis

8.2.6 Direcciones de correo detectados

No se encontraron direcciones de correo en el análisis

8.3 Análisis de Malware

Se hizo un análisis utilizando distintos motores de antivirus, lo que permite la detección de virus, gusanos, troyanos y todo tipo de malware que contengan los archivos .ipa y .apk correspondiente a iOS y Android respectivamente. En este periodo solo analizamos la apk de android debido a su cambio de versión.

Android	
Motor	**Estado**
Ad-Aware	✓
AegisLab	✓
AhnLab-V3	✓
Alibaba	✓

ALYac	✓
Antiy-AVL	✓
Arcabit	✓
Avast	✓
Avast Mobile Security	✓
AVG	✓
Avira	✓
AVware	✓
Baidu	✓
BitDefender	✓
Bkav	✓
CAT-QuickHeal	✓
ClamAV	✓
CMC	✓
Comodo	✓
Cyren	✓
Emsisoft	✓
eScan	✓
ESET-NOD32	✓

F-Prot	✓
F-Secure	✓
Fortinet	✓
GData	✓
Ikarus	✓
Jiangmin	✓
K7AntiVirus	✓
K7GW	✓
Kaspersky	✓
Kingsoft	✓
Malwarebytes	✓
MAX	✓
McAfee	✓
McAfee-GW-Edition	✓
Microsoft	✓
NANO-Antivirus	✓
nProtect	✓
Panda	✓
Qihoo-360	✓

Rising	✓
Sophos AV	✓
SUPERAntiSpyware	✓
Symantec	✓
Symantec Mobile Insight	✓
Tencent	✓
TheHacker	✓
TrendMicro	✓
TrendMicro-HouseCall	✓
Trustlook	✓
VBA32	✓
VIPRE	✓
ViRobot	✓
Webroot	✓
WhiteArmor	✓
Yandex	✓
Zillya	✓
ZoneAlarm	✓
Zoner	✓

9 Vulnerabilidades declaradas

A continuación, se listan las vulnerabilidades declaradas por terceros que puedan comprometer la seguridad de la aplicación y khipu.com.

En este periodo de análisis se encontraron 2 vulnerabilidades que afectan a la implementación de SSL/TLS, la primera de ellas es **BEAST** (CVE-2011-3389), esta vulnerabilidad afecta a la versión 1 de TLS, esta vulnerabilidad se encuentra mitigada al soportar la versión 1.1 y 1.2 de TLS, para corregirla correctamente, se debe desactivar el soporte para TLS 1.

La segunda vulnerabilidad es **LUCKY13** (CVE-2013-0169) esta afecta a las implementaciones de TLS que utilicen el modo de cifrado CBC (Cipher-Block-Chaining), por lo cual la mitigación es deshabilitar los cifrados que utilicen estos métodos y siempre tener la última versión estable de OpenSSL.

Referencias

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
http://www.isg.rhul.ac.uk/tls/
https://raymii.org/s/tutorials/Strong_SSL_Security_On_nginx.html
https://cipherli.st/

10 Anexos

#	Archivo	SHA256SUM
1	khipuandroid05032018.cap	59cd2070041f5f17957cb0538bc011fbeda128c4bdbacd51eb63e9e0f1929703