Cliente:

khipu

Febrero

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
08-02-2018	Kevin Moller	1.0	Creación del documento

https://nivel4.com

+56 2 2248 1368

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.

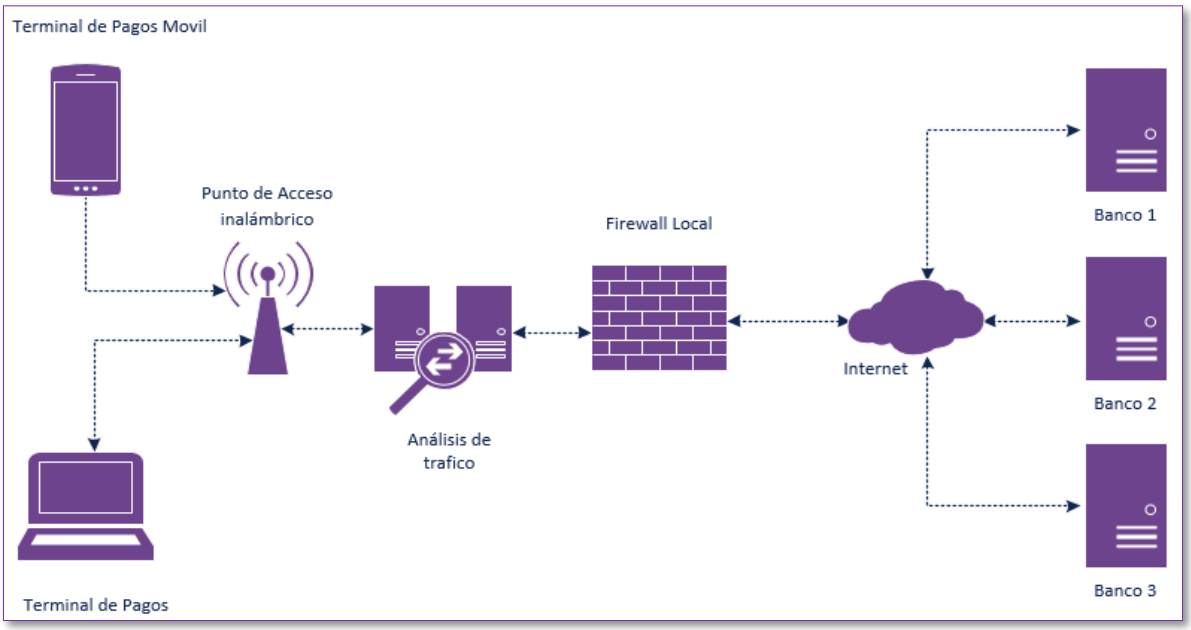
3 Objetivo

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.

https://nivel4.com

+56 2 2248 1368

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.**

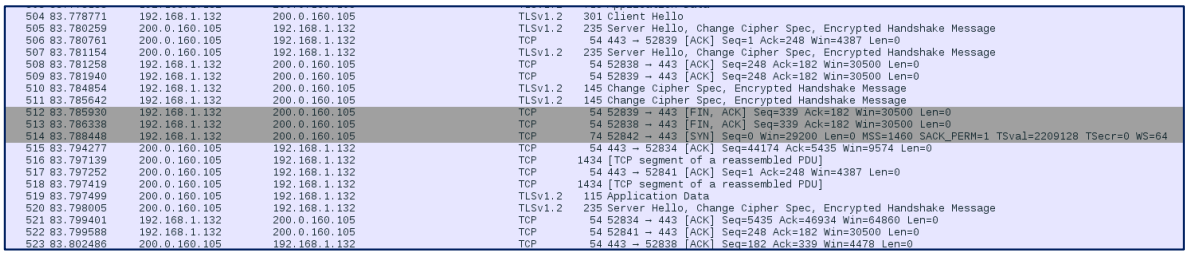
Plataforma	Versión	SHA256SUM
Android	**6.6.29**	**9cb37cf3002f677d835a2806od67d3787caaec6c87b639b4a2d47ff937c001cd**
iOS	6.21	**30115e25e3ddb9aa43bb7dab02efoba2d49ddfe7d207f3c9b0b48098c16788e2**
Linux i386	1.17.1922.1	f5533662c3ca-bce75ecc9d6fdf9632ffb189941533f4992efoed8aaf82e6b1b1
Linux x64	1.17.1922.1	9321ae02910a9dfcd8801ca24c11a43e707a62e8b579bcb4a10d79e0e77c908f
OSX	1.17.1922.1	637f66c0b5c4d04f2291ffc71ee8564398oee3e1e6c171f1caeb3430ff16a577
Windows	1.17.1922.1	e610e91976939e06ee53797db22f97f584c3063ae311ab8fab68a5f81fafo71e

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. Si bien se detectó tráfico no seguro (http) este corresponde a la validación del estado de los certificados SSL de algunos sitios, mediante OCSP y no durante la interacción con algún banco, en ningún caso se enviaron credenciales de usuario o datos de relacionados con las transacciones realizadas con el terminal de pagos al momento de realizar las pruebas. Finalmente, el resto del tráfico corresponde a consultas **DNS** y tráfico propio de una red local, como **NTP**, **NETBIOS**, **ARP**, entre otros.

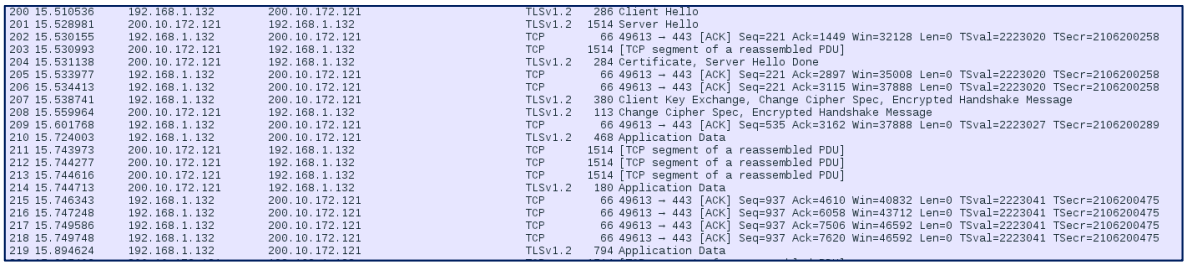
En los siguientes puntos se detalla el tráfico detectado durante el uso de la aplicación evidenciando que las transacciones se realizan de forma segura y no se almacenan datos de usuario como, por ejemplo, claves del banco.

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



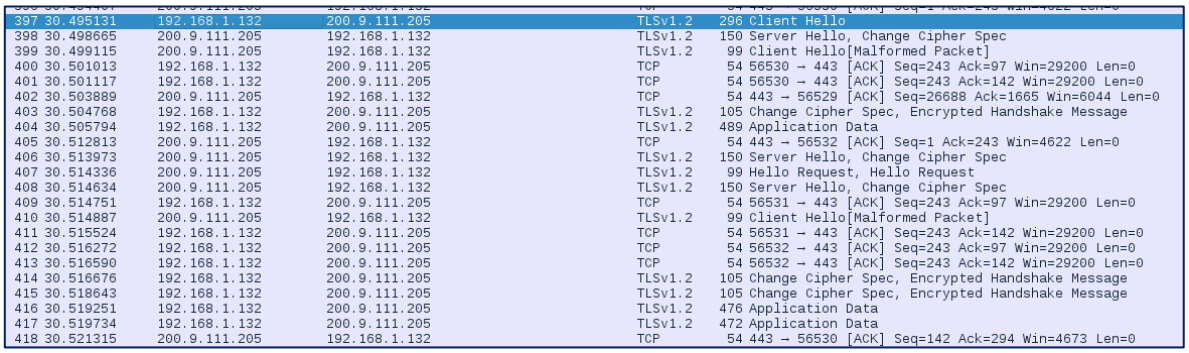
504	83.778771	192.168.1.132	200.0.160.105	TLSv1.2	301 Client Hello
505	83.780259	200.0.160.105	192.168.1.132	TLSv1.2	235 Server Hello, Change Cipher Spec, Encrypted Handshake Message
506	83.780761	200.0.160.105	192.168.1.132	TCP	54 443 → 52839 [ACK] Seq=1 Ack=248 Win=4387 Len=0
507	83.781154	200.0.160.105	192.168.1.132	TLSv1.2	235 Server Hello, Change Cipher Spec, Encrypted Handshake Message
508	83.781258	192.168.1.132	200.0.160.105	TCP	54 52838 → 443 [ACK] Seq=248 Ack=182 Win=30500 Len=0
509	83.781940	192.168.1.132	200.0.160.105	TCP	54 52839 → 443 [ACK] Seq=248 Ack=182 Win=30500 Len=0
510	83.784854	192.168.1.132	200.0.160.105	TLSv1.2	145 Change Cipher Spec, Encrypted Handshake Message
511	83.785642	192.168.1.132	200.0.160.105	TLSv1.2	145 Change Cipher Spec, Encrypted Handshake Message
512	83.785930	192.168.1.132	200.0.160.105	TCP	54 52839 → 443 [FIN, ACK] Seq=339 Ack=182 Win=30500 Len=0
513	83.786338	192.168.1.132	200.0.160.105	TCP	54 52838 → 443 [FIN, ACK] Seq=339 Ack=182 Win=30500 Len=0
514	83.788448	192.168.1.132	200.0.160.105	TCP	74 52842 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2209128 TSecr=0 WS=64
515	83.794277	200.0.160.105	192.168.1.132	TCP	54 443 → 52834 [ACK] Seq=44174 Ack=5435 Win=9574 Len=0
516	83.797139	200.0.160.105	192.168.1.132	TCP	1434 [TCP segment of a reassembled PDU]
517	83.797252	200.0.160.105	192.168.1.132	TCP	54 443 → 52841 [ACK] Seq=1 Ack=248 Win=4387 Len=0
518	83.797419	200.0.160.105	192.168.1.132	TCP	1434 [TCP segment of a reassembled PDU]
519	83.797499	200.0.160.105	192.168.1.132	TLSv1.2	115 Application Data
520	83.798005	200.0.160.105	192.168.1.132	TLSv1.2	235 Server Hello, Change Cipher Spec, Encrypted Handshake Message
521	83.799401	192.168.1.132	200.0.160.105	TCP	54 52834 → 443 [ACK] Seq=5435 Ack=46934 Win=64860 Len=0
522	83.799588	192.168.1.132	200.0.160.105	TCP	54 52841 → 443 [ACK] Seq=248 Ack=182 Win=30500 Len=0
523	83.802486	200.0.160.105	192.168.1.132	TCP	54 443 → 52838 [ACK] Seq=182 Ack=339 Win=4478 Len=0

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



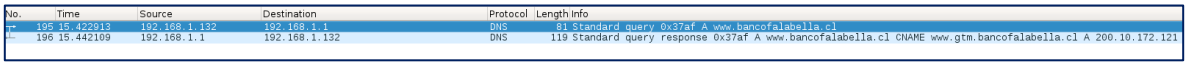
200	15.510536	192.168.1.132	200.10.172.121	TLSv1.2	286 Client Hello
201	15.528981	200.10.172.121	192.168.1.132	TLSv1.2	1514 Server Hello
202	15.530155	192.168.1.132	200.10.172.121	TCP	66 49613 → 443 [ACK] Seq=221 Ack=1449 Win=32128 Len=0 TSval=2223020 TSecr=2106200258
203	15.530993	200.10.172.121	192.168.1.132	TCP	1514 [TCP segment of a reassembled PDU]
204	15.531138	200.10.172.121	192.168.1.132	TLSv1.2	284 Certificate, Server Hello Done
205	15.533977	192.168.1.132	200.10.172.121	TCP	66 49613 → 443 [ACK] Seq=221 Ack=2897 Win=35008 Len=0 TSval=2223020 TSecr=2106200258
206	15.534413	192.168.1.132	200.10.172.121	TCP	66 49613 → 443 [ACK] Seq=221 Ack=3115 Win=37888 Len=0 TSval=2223020 TSecr=2106200258
207	15.538741	192.168.1.132	200.10.172.121	TLSv1.2	380 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
208	15.559964	200.10.172.121	192.168.1.132	TLSv1.2	113 Change Cipher Spec, Encrypted Handshake Message
209	15.601768	192.168.1.132	200.10.172.121	TCP	66 49613 → 443 [ACK] Seq=535 Ack=3162 Win=37888 Len=0 TSval=2223027 TSecr=2106200289
210	15.724003	192.168.1.132	200.10.172.121	TLSv1.2	468 Application Data
211	15.743973	200.10.172.121	192.168.1.132	TCP	1514 [TCP segment of a reassembled PDU]
212	15.744277	200.10.172.121	192.168.1.132	TCP	1514 [TCP segment of a reassembled PDU]
213	15.744616	200.10.172.121	192.168.1.132	TCP	1514 [TCP segment of a reassembled PDU]
214	15.744713	200.10.172.121	192.168.1.132	TLSv1.2	180 Application Data
215	15.746343	192.168.1.132	200.10.172.121	TCP	66 49613 → 443 [ACK] Seq=937 Ack=4610 Win=40832 Len=0 TSval=2223041 TSecr=2106200475
216	15.747248	192.168.1.132	200.10.172.121	TCP	66 49613 → 443 [ACK] Seq=937 Ack=6058 Win=43712 Len=0 TSval=2223041 TSecr=2106200475
217	15.749586	192.168.1.132	200.10.172.121	TCP	66 49613 → 443 [ACK] Seq=937 Ack=7506 Win=46592 Len=0 TSval=2223041 TSecr=2106200475
218	15.749748	192.168.1.132	200.10.172.121	TCP	66 49613 → 443 [ACK] Seq=937 Ack=7620 Win=46592 Len=0 TSval=2223041 TSecr=2106200475
219	15.894624	192.168.1.132	200.10.172.121	TLSv1.2	794 Application Data

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

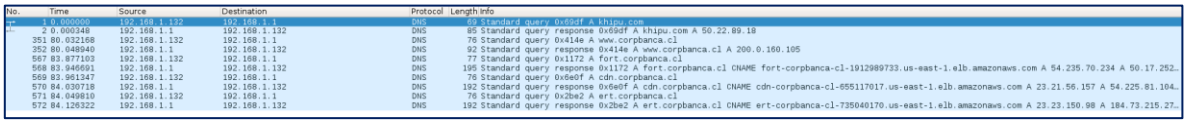


397	30.495131	192.168.1.132	200.9.111.205	TLSv1.2	296 Client Hello
398	30.498665	200.9.111.205	192.168.1.132	TLSv1.2	150 Server Hello, Change Cipher Spec
399	30.499115	200.9.111.205	192.168.1.132	TLSv1.2	99 Client Hello[Malformed Packet]
400	30.501013	192.168.1.132	200.9.111.205	TCP	54 56530 → 443 [ACK] Seq=243 Ack=97 Win=29200 Len=0
401	30.501117	192.168.1.132	200.9.111.205	TCP	54 56530 → 443 [ACK] Seq=243 Ack=142 Win=29200 Len=0
402	30.503889	200.9.111.205	192.168.1.132	TCP	54 443 → 56529 [ACK] Seq=26688 Ack=1665 Win=6044 Len=0
403	30.504768	192.168.1.132	200.9.111.205	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
404	30.505794	192.168.1.132	200.9.111.205	TLSv1.2	489 Application Data
405	30.512813	200.9.111.205	192.168.1.132	TCP	54 443 → 56532 [ACK] Seq=1 Ack=243 Win=4622 Len=0
406	30.513973	200.9.111.205	192.168.1.132	TLSv1.2	150 Server Hello, Change Cipher Spec
407	30.514336	200.9.111.205	192.168.1.132	TLSv1.2	99 Hello Request, Hello Request
408	30.514634	200.9.111.205	192.168.1.132	TLSv1.2	150 Server Hello, Change Cipher Spec
409	30.514751	192.168.1.132	200.9.111.205	TCP	54 56531 → 443 [ACK] Seq=243 Ack=97 Win=29200 Len=0
410	30.514887	200.9.111.205	192.168.1.132	TLSv1.2	99 Client Hello[Malformed Packet]
411	30.515524	192.168.1.132	200.9.111.205	TCP	54 56531 → 443 [ACK] Seq=243 Ack=142 Win=29200 Len=0
412	30.516272	192.168.1.132	200.9.111.205	TCP	54 56532 → 443 [ACK] Seq=243 Ack=97 Win=29200 Len=0
413	30.516590	192.168.1.132	200.9.111.205	TCP	54 56532 → 443 [ACK] Seq=243 Ack=142 Win=29200 Len=0
414	30.516676	192.168.1.132	200.9.111.205	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
415	30.518643	192.168.1.132	200.9.111.205	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
416	30.519251	192.168.1.132	200.9.111.205	TLSv1.2	476 Application Data
417	30.519734	192.168.1.132	200.9.111.205	TLSv1.2	472 Application Data
418	30.521315	200.9.111.205	192.168.1.132	TCP	54 443 → 56530 [ACK] Seq=142 Ack=294 Win=4673 Len=0

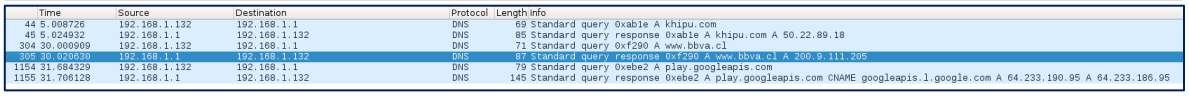
6.4 Tráfico DNS



No.	Time	Source	Destination	Protocol	Length	Info
195	15.422913	192.168.1.132	192.168.1.1	DNS	81	Standard query 0x37af A www.bancofalabella.cl
196	15.442109	192.168.1.1	192.168.1.132	DNS	119	Standard query response 0x37af A www.bancofalabella.cl CNAME www.gtm.bancofalabella.cl A 200.10.172.121



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.132	192.168.1.1	DNS	69	Standard query 0x69df A khipu.com
2	0.000348	192.168.1.1	192.168.1.132	DNS	85	Standard query response 0x69df A khipu.com A 50.22.89.18
351	80.032168	192.168.1.132	192.168.1.1	DNS	76	Standard query 0x414e A www.corpbanca.cl
352	80.048940	192.168.1.1	192.168.1.132	DNS	92	Standard query response 0x414e A www.corpbanca.cl A 200.0.160.105
567	83.877103	192.168.1.132	192.168.1.1	DNS	77	Standard query 0x1172 A fort.corpbanca.cl
568	83.946691	192.168.1.1	192.168.1.132	DNS	195	Standard query response 0x1172 A fort.corpbanca.cl CNAME fort-corpbanca-cl-1912989733.us-east-1.elb.amazonaws.com A 54.235.70.234 A 50.17.252…
569	83.961347	192.168.1.132	192.168.1.1	DNS	76	Standard query 0x6e0f A cdn.corpbanca.cl
570	84.030718	192.168.1.1	192.168.1.132	DNS	192	Standard query response 0x6e0f A cdn.corpbanca.cl CNAME cdn-corpbanca-cl-655117017.us-east-1.elb.amazonaws.com A 23.21.56.157 A 54.225.81.104…
571	84.049810	192.168.1.132	192.168.1.1	DNS	76	Standard query 0x2be2 A ert.corpbanca.cl
572	84.126322	192.168.1.1	192.168.1.132	DNS	192	Standard query response 0x2be2 A ert.corpbanca.cl CNAME ert-corpbanca-cl-735040170.us-east-1.elb.amazonaws.com A 23.23.150.98 A 184.73.215.27…

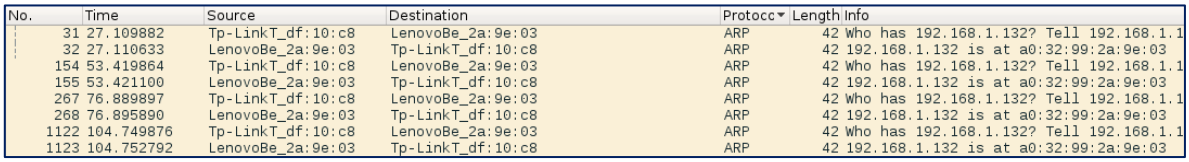


	Time	Source	Destination	Protocol	Length	Info
44	5.008726	192.168.1.132	192.168.1.1	DNS	69	Standard query 0xab1e A khipu.com
45	5.024932	192.168.1.1	192.168.1.132	DNS	85	Standard query response 0xab1e A khipu.com A 50.22.89.18
304	30.000909	192.168.1.132	192.168.1.1	DNS	71	Standard query 0xf290 A www.bbva.cl
305	30.020530	192.168.1.1	192.168.1.132	DNS	87	Standard query response 0xf290 A www.bbva.cl A 200.9.111.205
1154	31.684329	192.168.1.132	192.168.1.1	DNS	79	Standard query 0xebe2 A play.googleapis.com
1155	31.706128	192.168.1.1	192.168.1.132	DNS	145	Standard query response 0xebe2 A play.googleapis.com CNAME googleapis.l.google.com A 64.233.190.95 A 64.233.186.95

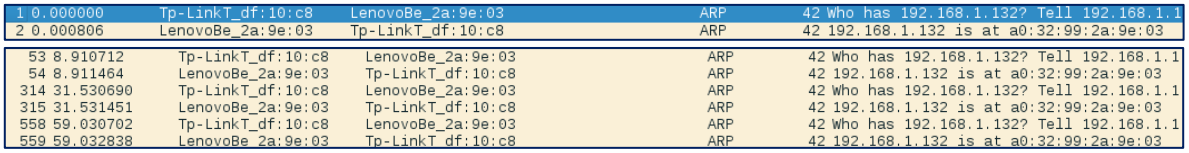
6.5 Tráfico HTTP

Durante este periodo no se fue posible detectar tráfico HTTP.

6.6 Otro Tráfico



No.	Time	Source	Destination	Protocc	Length	Info
31	27.109882	Tp-LinkT_df:10:c8	LenovoBe_2a:9e:03	ARP	42	Who has 192.168.1.132? Tell 192.168.1.1
32	27.110633	LenovoBe_2a:9e:03	Tp-LinkT_df:10:c8	ARP	42	192.168.1.132 is at a0:32:99:2a:9e:03
154	53.419864	Tp-LinkT_df:10:c8	LenovoBe_2a:9e:03	ARP	42	Who has 192.168.1.132? Tell 192.168.1.1
155	53.421100	LenovoBe_2a:9e:03	Tp-LinkT_df:10:c8	ARP	42	192.168.1.132 is at a0:32:99:2a:9e:03
267	76.889897	Tp-LinkT_df:10:c8	LenovoBe_2a:9e:03	ARP	42	Who has 192.168.1.132? Tell 192.168.1.1
268	76.895890	LenovoBe_2a:9e:03	Tp-LinkT_df:10:c8	ARP	42	192.168.1.132 is at a0:32:99:2a:9e:03
1122	104.749876	Tp-LinkT_df:10:c8	LenovoBe_2a:9e:03	ARP	42	Who has 192.168.1.132? Tell 192.168.1.1
1123	104.752792	LenovoBe_2a:9e:03	Tp-LinkT_df:10:c8	ARP	42	192.168.1.132 is at a0:32:99:2a:9e:03



1	0.000000	Tp-LinkT_df:10:c8	LenovoBe_2a:9e:03	ARP	42	Who has 192.168.1.132? Tell 192.168.1.1
2	0.000806	LenovoBe_2a:9e:03	Tp-LinkT_df:10:c8	ARP	42	192.168.1.132 is at a0:32:99:2a:9e:03

53	8.910712	Tp-LinkT_df:10:c8	LenovoBe_2a:9e:03	ARP	42	Who has 192.168.1.132? Tell 192.168.1.1
54	8.911464	LenovoBe_2a:9e:03	Tp-LinkT_df:10:c8	ARP	42	192.168.1.132 is at a0:32:99:2a:9e:03
314	31.530690	Tp-LinkT_df:10:c8	LenovoBe_2a:9e:03	ARP	42	Who has 192.168.1.132? Tell 192.168.1.1
315	31.531451	LenovoBe_2a:9e:03	Tp-LinkT_df:10:c8	ARP	42	192.168.1.132 is at a0:32:99:2a:9e:03
558	59.030702	Tp-LinkT_df:10:c8	LenovoBe_2a:9e:03	ARP	42	Who has 192.168.1.132? Tell 192.168.1.1
559	59.032838	LenovoBe_2a:9e:03	Tp-LinkT_df:10:c8	ARP	42	192.168.1.132 is at a0:32:99:2a:9e:03

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
192.168.1.132	50.22.89.18	TLSv1.2	khipu
192.168.1.132	200.0.160.105	TLSv1.2	Banco Corpbanca
192.168.1.132	200.10.172.121	TLSv1.2	Banco Falabella
192.168.1.132	200.9.111.205	TLSv1.2	Banco BBVA

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.

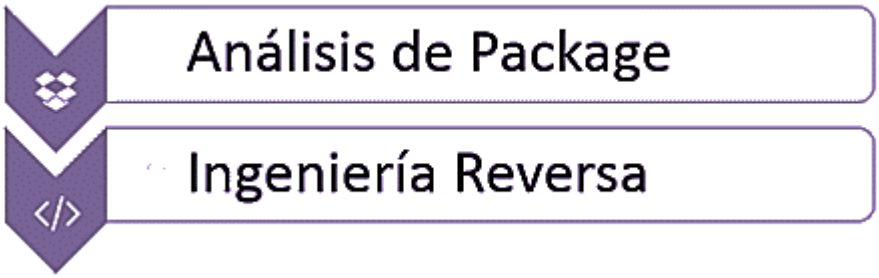
7.2 Referencias

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_2017-12-06.apk
SHA256	a525f51ce2e52782d33a5967a61bcc5d9f87139f49f4192d7a28abdc2dda5571
Tamaño	6.8 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 version.

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	AndroidCorpbanca20180208.cap	775ba6357b349b6cd7099cc72b9ed3ea7c74dcb57090643d98133a806261ea88
2	AndroidFalabella20180208.cap	3ae5da1903319081afd6afc0de58656750810f165cec969597f1090ccfe6b718
	AndroidBBVA20180208.cap	679490521e705ab61bb80056f8fa80b0494f0bfd71042efb1cb8436eea91da71