Dirigido a:
Eduardo Parraguez
khipu

Enero
2019

INFORME TÉCNICO

Análisis de tráfico de datos

DOCUMENTO CONFIDENCIAL

https://nivel4.com

+56 2 2248 1368
Av Providencia 1208
Oficina 1204
Santiago, Chile.

1 Control de versiones

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

Fecha	Autor	Versión	Comentarios
10-01-2019	Kevin Möller	1.0	Creación del documento
15-01-2019	Kevin Möller	1.0	Documentación

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.

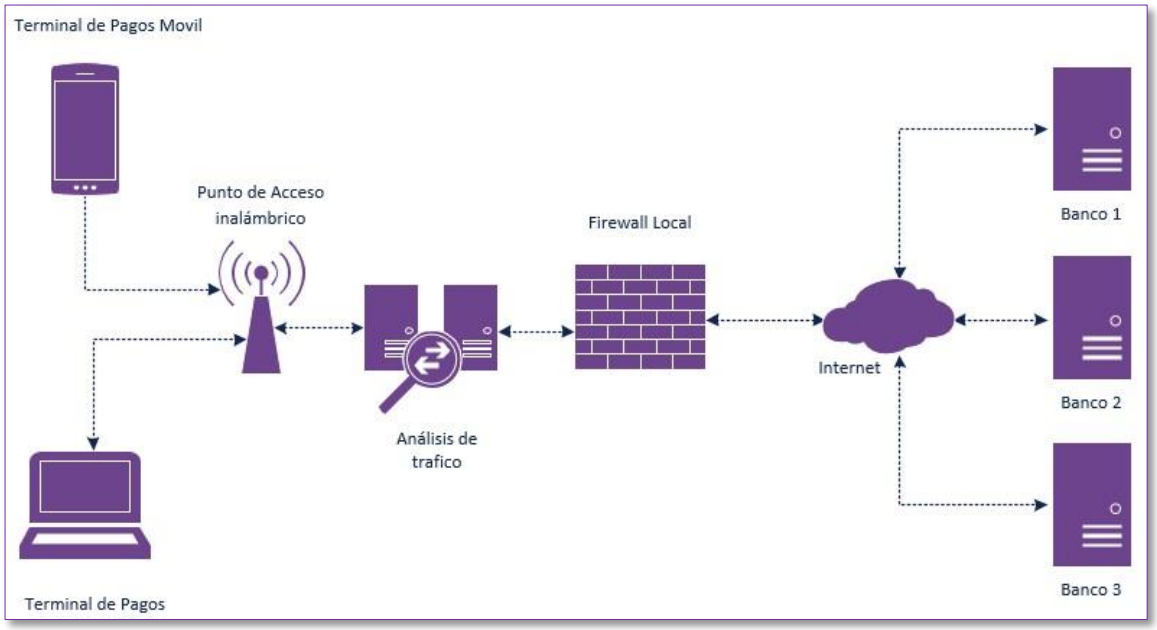
Esta revisión incluye la versión del terminal de pagos disponible para IOS y Android.

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 al terminal de pago de 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 siguiente diagrama:



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 **iOS y Android** tanto en su versión

como en su HASH.

Plataforma	Versión	SHA256SUM
Android	**6.8.1**	ca1e21d7bb85da81221c2eed04824b3e4ee90731b651e9be7b93f67c612e2bcb
iOS	**6.29**	0b6b1dc2c7ba0e9f41b47998abddc9dc45fb82c975c4564d7b11675f2dd4697a
Linux i386	1.17.1922.1	f5533662c3cbce75ecc9d6fdf9632ffb189941533f4992ef0ed8aaf82e6b1b1
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. 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 “Ripley”

APK

202	27.702671	192.168.1.66	200.54.56.74	TLSv1.2	280 Client Hello
203	27.705684	200.54.56.74	192.168.1.66	TLSv1.2	1514 Server Hello
204	27.705777	200.54.56.74	192.168.1.66	TCP	1514 443 → 51625 [ACK] Seq=1449 Ack=215 Win=4380 Len=1448 TSval=1368800880 TSecr=360001 [TCP segment of a reassembled PDU]
205	27.705830	200.54.56.74	192.168.1.66	TLSv1.2	332 Certificate, Server Hello Done
206	27.707025	192.168.1.66	200.54.56.74	TCP	66 51625 → 443 [ACK] Seq=215 Ack=1449 Win=65535 Len=0 TSval=360002 TSecr=1368800880
207	27.707074	192.168.1.66	200.54.56.74	TCP	66 51625 → 443 [ACK] Seq=215 Ack=2897 Win=65535 Len=0 TSval=360002 TSecr=1368800880
208	27.711081	192.168.1.66	200.54.56.74	TCP	66 51625 → 443 [ACK] Seq=215 Ack=3163 Win=65535 Len=0 TSval=360002 TSecr=1368800880
209	27.711134	192.168.1.66	192.168.1.1	DNS	87 Standard query 0x2c4d A safebrowsing.googleapis.com
210	27.711164	192.168.1.66	200.54.56.74	TLSv1.2	384 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
211	27.711344	192.168.1.1	192.168.1.66	DNS	103 Standard query response 0x2c4d A safebrowsing.googleapis.com A 64.233.190.95
212	27.713341	200.54.56.74	192.168.1.66	TCP	66 443 → 51625 [ACK] Seq=3163 Ack=533 Win=4912 Len=0 TSval=1368800888 TSecr=360002
213	27.714731	200.54.56.74	192.168.1.66	TLSv1.2	72 Change Cipher Spec
214	27.714820	200.54.56.74	192.168.1.66	TLSv1.2	111 Encrypted Handshake Message

6.2 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Chile Empresas”

APK

4362	216.127343	192.168.1.66	45.60.4.56	TLSv1.2	285	Client Hello
4363	216.179115	45.60.4.56	192.168.1.66	TCP	66	443 → 45003 [ACK] Seq=1 Ack=220 Win=30080 Len=0 TSval=1106890631 TSecr=378844
4364	216.179286	45.60.4.56	192.168.1.66	TLSv1.2	1514	Server Hello
4365	216.179356	45.60.4.56	192.168.1.66	TCP	1514	443 → 45003 [ACK] Seq=1449 Ack=220 Win=30080 Len=1448 TSval=1106890631 TSecr=378844 [TCP segment of a reassembled PDU]
4366	216.179403	45.60.4.56	192.168.1.66	TLSv1.2	1266	Certificate [TCP segment of a reassembled PDU]
4367	216.180361	45.60.4.56	192.168.1.66	TLSv1.2	823	Certificate Status, Server Key Exchange, Server Hello Done
4368	216.181302	192.168.1.66	45.60.4.56	TCP	66	45003 → 443 [ACK] Seq=220 Ack=1449 Win=90624 Len=0 TSval=378849 TSecr=1106890631
4369	216.181429	192.168.1.66	45.60.4.56	TCP	66	45003 → 443 [ACK] Seq=220 Ack=2897 Win=93440 Len=0 TSval=378849 TSecr=1106890631
4370	216.181644	192.168.1.66	45.60.4.56	TCP	66	45003 → 443 [ACK] Seq=220 Ack=4097 Win=96512 Len=0 TSval=378849 TSecr=1106890631
4372	216.183895	192.168.1.66	45.60.4.56	TCP	66	45003 → 443 [ACK] Seq=220 Ack=4854 Win=99328 Len=0 TSval=378850 TSecr=1106890631
4373	216.187390	192.168.1.66	45.60.4.56	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
4374	216.244068	45.60.4.56	192.168.1.66	TLSv1.2	324	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
4379	216.304278	192.168.1.66	45.60.4.56	TLSv1.2	545	Application Data

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

APK

7598	295.256186	192.168.1.66	96.17.19.110	TLSv1.2	274	Client Hello
7599	295.257810	96.17.19.110	192.168.1.66	TCP	66	443 → 48108 [ACK] Seq=1 Ack=209 Win=30080 Len=0 TSval=208789273 TSecr=386757
7600	295.258318	96.17.19.110	192.168.1.66	TLSv1.2	1514	Server Hello
7601	295.258402	96.17.19.110	192.168.1.66	TCP	1514	443 → 48108 [ACK] Seq=1449 Ack=209 Win=30080 Len=1448 TSval=208789273 TSecr=386757 [TCP segment of a reassembled PDU]
7602	295.258457	96.17.19.110	192.168.1.66	TLSv1.2	1266	Certificate [TCP segment of a reassembled PDU]
7603	295.259604	192.168.1.66	96.17.19.110	TCP	66	48108 → 443 [ACK] Seq=209 Ack=1449 Win=90624 Len=0 TSval=386757 TSecr=208789273
7604	295.259726	96.17.19.110	192.168.1.66	TLSv1.2	1514	Certificate Status [TCP segment of a reassembled PDU]
7605	295.259847	192.168.1.66	96.17.19.110	TCP	66	48108 → 443 [ACK] Seq=209 Ack=2897 Win=93440 Len=0 TSval=386757 TSecr=208789273
7606	295.260556	192.168.1.66	96.17.19.110	TCP	66	48108 → 443 [ACK] Seq=209 Ack=4097 Win=96512 Len=0 TSval=386757 TSecr=208789273
7607	295.260846	192.168.1.66	96.17.19.110	TCP	66	48108 → 443 [ACK] Seq=209 Ack=5545 Win=99328 Len=0 TSval=386757 TSecr=208789275
7608	295.261495	96.17.19.110	192.168.1.66	TLSv1.2	335	Server Key Exchange, Server Hello Done
7609	295.262363	192.168.1.66	96.17.19.110	TCP	66	48108 → 443 [ACK] Seq=209 Ack=5814 Win=99328 Len=0 TSval=386758 TSecr=208789277
7610	295.265880	192.168.1.66	96.17.19.110	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
7611	295.267992	96.17.19.110	192.168.1.66	TLSv1.2	324	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
7612	295.307645	192.168.1.66	96.17.19.110	TLSv1.2	743	Application Data

Tráfico DNS

APK

	Time	Source	Destination	Protocol	Length	Info
2320	31.766465	192.168.1.66	192.168.1.1	DNS	84	Standard query 0x142b A www.google-analytics.com
2321	31.766769	192.168.1.1	192.168.1.66	DNS	227	Standard query response 0x142b A www.google-analytics.com CNAME www-google-analytics.l.google.com A 64.233.190.113 A 64.233.190.139 A 64.233.190.100 A 64.233.190.138 A 64
2326	31.800279	192.168.1.66	192.168.1.1	DNS	80	Standard query 0x1edd A connect.facebook.net
2327	31.801651	192.168.1.1	192.168.1.66	DNS	128	Standard query response 0x1edd A connect.facebook.net CNAME scontent.xx.fbcdn.net A 179.60.193.20
2569	32.721880	192.168.1.66	192.168.1.1	DNS	76	Standard query 0x19d6 A www.facebook.com
2570	32.723384	192.168.1.1	192.168.1.66	DNS	121	Standard query response 0x19d6 A www.facebook.com CNAME star-mini.c10r.facebook.com A 179.60.193.35
2710	33.107361	192.168.1.66	192.168.1.1	DNS	83	Standard query 0x4373 A stats.g.doubleclick.net
2711	33.107673	192.168.1.1	192.168.1.66	DNS	184	Standard query response 0x4373 A stats.g.doubleclick.net CNAME stats.l.doubleclick.net A 64.233.186.156 A 64.233.186.157 A 64.233.186.155 A 64.233.186.154
2771	33.491002	192.168.1.66	192.168.1.1	DNS	73	Standard query 0x02e2 A www.google.cl
2772	33.491230	192.168.1.1	192.168.1.66	DNS	89	Standard query 0x02e2 A www.google.cl A 64.233.190.94
2800	33.704541	192.168.1.66	192.168.1.1	DNS	79	Standard query 0x1615 A cdn.appdynamics.com
2801	33.707436	192.168.1.1	192.168.1.66	DNS	143	Standard query response 0x1615 A cdn.appdynamics.com A 52.84.180.154 A 52.84.180.150 A 52.84.180.167 A 52.84.180.11
2859	35.115160	192.168.1.66	192.168.1.1	DNS	83	Standard query 0x2485 A col.eum-appdynamics.com
2860	35.121255	192.168.1.1	192.168.1.66	DNS	211	Standard query response 0x2485 A col.eum-appdynamics.com A 34.197.20.226 A 34.225.58.230 A 34.203.183.99 A 34.205.208.184 A 34.225.236.159 A 34.200.114.102 A 34.232.156.4
3371	91.427574	192.168.1.66	192.168.1.1	DNS	83	Standard query 0x597d A miportal.bancoripley.cl
3372	91.429484	192.168.1.1	192.168.1.66	DNS	99	Standard query response 0x597d A miportal.bancoripley.cl A 200.54.56.74
3419	91.635515	192.168.1.60	192.168.1.1	DNS	81	Standard query 0x719b A bancoripley.letsta.lk
3420	91.637421	192.168.1.1	192.168.1.66	DNS	190	Standard query response 0x719b A bancoripley.letsta.lk CNAME productionappload balancer-376843974.us-west-1.elb.amazonaws.com A 52.9.77.94 A 52.9.59.69
3461	92.785281	192.168.1.66	192.168.1.1	DNS	84	Standard query 0x0fa1 A www.googletagmanager.com
3462	92.785345	192.168.1.66	192.168.1.1	DNS	84	Standard query 0x546a A ssl.google-analytics.com
3463	92.787836	192.168.1.1	192.168.1.66	DNS	144	Standard query response 0x0fa1 A www.googletagmanager.com CNAME www-googletagmanager.l.google.com A 172.217.192.97
3464	92.787134	192.168.1.1	192.168.1.66	DNS	144	Standard query response 0x546a A ssl.google-analytics.com CNAME ssl-google-analytics.l.google.com A 172.217.162.40
3503	93.206207	192.168.1.66	192.168.1.1	DNS	77	Standard query 0x377f A cdn.mouseflow.com
3504	93.207954	192.168.1.1	192.168.1.66	DNS	135	Standard query response 0x377f A cdn.mouseflow.com CNAME rec.mouseflowaps.netdna-cdn.com A 23.111.9.38
3510	93.238757	192.168.1.66	192.168.1.1	DNS	80	Standard query 0x2beb A connect.facebook.net
3511	93.239858	192.168.1.1	192.168.1.66	DNS	128	Standard query response 0x2beb A connect.facebook.net CNAME scontent.xx.fbcdn.net A 179.60.193.20
3561	93.704859	192.168.1.66	192.168.1.1	DNS	76	Standard query 0x3c64 A www.facebook.com
3562	93.706574	192.168.1.1	192.168.1.66	DNS	121	Standard query response 0x3c64 A www.facebook.com CNAME star-mini.c10r.facebook.com A 179.60.193.35
3676	94.336514	192.168.1.66	192.168.1.1	DNS	79	Standard query 0x0609 A cdn.appdynamics.com
3677	94.337478	192.168.1.1	192.168.1.66	DNS	143	Standard query response 0x0609 A cdn.appdynamics.com A 52.84.180.154 A 52.84.180.11 A 52.84.180.167 A 52.84.180.150
3689	95.503627	192.168.1.66	192.168.1.1	DNS	83	Standard query 0x1142 A col.eum-appdynamics.com
3690	95.506160	192.168.1.1	192.168.1.66	DNS	211	Standard query response 0x1142 A col.eum-appdynamics.com A 52.3.12.93 A 52.22.51.176 A 52.45.107.246 A 52.205.157.65 A 52.202.147.27 A 52.44.195.191 A 52.205.158.81 A 35.
3886	104.030838	192.168.1.66	192.168.1.1	DNS	89	Standard query 0x6490 A cgedappmovqacentrality.cge.cl
3887	104.037124	192.168.1.1	192.168.1.66	DNS	147	Standard query response 0x6490 A cgedappmovqacentrality.cge.cl CNAME cgedappmovqacentrality.gslb.cge.cl A 186.148.34.32
4055	198.289270	192.168.1.66	192.168.1.1	DNS	78	Standard query 0x9b51 A graph.facebook.com
4056	198.291181	192.168.1.1	192.168.1.66	DNS	136	Standard query response 0x9b51 A graph.facebook.com CNAME api.facebook.com CNAME star.c10r.facebook.com A 179.60.193.16
4357	216.020758	192.168.1.66	192.168.1.1	DNS	88	Standard query 0xc814 A portalpersonas.bancochile.cl
4358	216.022656	192.168.1.1	192.168.1.66	DNS	140	Standard query response 0xc814 A portalpersonas.bancochile.cl CNAME prn2kam.x.incapdns.net A 45.60.4.56
4434	217.313893	192.168.1.66	192.168.1.1	DNS	79	Standard query 0xb2fc A login.bancochile.cl
4435	217.315937	192.168.1.1	192.168.1.66	DNS	131	Standard query response 0xb2fc A login.bancochile.cl CNAME x3hfncr.x.incapdns.net A 45.60.4.56
4923	219.067751	192.168.1.66	192.168.1.1	DNS	87	Standard query 0x9fe3 A imagepersonas.bancochile.cl
4924	219.069396	192.168.1.1	192.168.1.66	DNS	215	Standard query response 0x9fe3 A imagepersonas.bancochile.cl CNAME imagepersonas-bancochile-cl-2048333488.us-east-1.elb.amazonaws.com A 54.235.129.1 A 174.129.237.97 A 54
4984	219.558076	192.168.1.66	192.168.1.1	DNS	86	Standard query 0xf0cb A mainpersonas.bancochile.cl
4985	219.560072	192.168.1.1	192.168.1.66	DNS	212	Standard query response 0xf0cb A mainpersonas.bancochile.cl CNAME mainpersonas-bancochile-cl-587264832.us-east-1.elb.amazonaws.com A 54.225.239.163 A 184.73.158.146 A 54.
5262	220.403267	192.168.1.66	192.168.1.1	DNS	87	Standard query 0xd2ec A notespersonas.bancochile.cl
5263	220.405232	192.168.1.1	192.168.1.66	DNS	214	Standard query response 0xd2ec A notespersonas.bancochile.cl CNAME notespersonas-bancochile-cl-581130394.us-east-1.elb.amazonaws.com A 54.243.193.159 A 54.243.187.113 A 1
5266	220.433526	192.168.1.66	192.168.1.1	DNS	87	Standard query 0x9272 A velocpersonas.bancochile.cl
5268	220.435046	192.168.1.1	192.168.1.66	DNS	214	Standard query response 0x9272 A velocpersonas.bancochile.cl CNAME velocpersonas-bancochile-cl-286709436.us-east-1.elb.amazonaws.com A 54.243.225.35 A 23.23.172.85 A 54.1
5715	224.048664	192.168.1.66	192.168.1.1	DNS	89	Standard query 0x9074 A cgedappmovqacentrality.cge.cl
5716	224.055544	192.168.1.1	192.168.1.66	DNS	147	Standard query response 0x9074 A cgedappmovqacentrality.cge.cl CNAME cgedappmovqacentrality.gslb.cge.cl A 186.148.34.32
7592	295.235285	192.168.1.66	192.168.1.1	DNS	77	Standard query 0x91b3 A www.scotiabank.cl
7594	295.237333	192.168.1.1	192.168.1.66	DNS	170	Standard query response 0x91b3 A www.scotiabank.cl CNAME www.scotiabank.cl.edgekey.net CNAME e10175.b.akamaiedge.net A 96.17.19.110

Tráfico HTTP

IPA

No se detectó trafico HTTP durante este periodo.

Otro Tráfico

IPA

	Time	Source	Destination	Protocol	Length	Info
2890	36.761292	Ubiquiti_c3:d5:9c	Motorola_13:87:7b	ARP	60	Who has 192.168.1.66? Tell 192.168.1.1
2891	36.884005	Motorola_13:87:7b	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.66 is at d0:f8:8c:13:87:7b
3368	89.070675	Ubiquiti_c3:d5:9c	Motorola_13:87:7b	ARP	60	Who has 192.168.1.66? Tell 192.168.1.1
3369	89.101165	Motorola_13:87:7b	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.66 is at d0:f8:8c:13:87:7b
4047	144.910045	Ubiquiti_c3:d5:9c	Motorola_13:87:7b	ARP	60	Who has 192.168.1.66? Tell 192.168.1.1
4048	145.097195	Motorola_13:87:7b	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.66 is at d0:f8:8c:13:87:7b
4135	203.299351	Ubiquiti_c3:d5:9c	Motorola_13:87:7b	ARP	60	Who has 192.168.1.66? Tell 192.168.1.1
4136	203.378184	Motorola_13:87:7b	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.66 is at d0:f8:8c:13:87:7b
6889	248.468823	Ubiquiti_c3:d5:9c	Motorola_13:87:7b	ARP	60	Who has 192.168.1.66? Tell 192.168.1.1
6890	248.517852	Motorola_13:87:7b	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.66 is at d0:f8:8c:13:87:7b
7590	295.198276	Ubiquiti_c3:d5:9c	Motorola_13:87:7b	ARP	60	Who has 192.168.1.66? Tell 192.168.1.1
7593	295.236503	Motorola_13:87:7b	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.66 is at d0:f8:8c:13:87:7b
8495	318.053477	Motorola_13:87:7b	Ubiquiti_c3:d5:9c	ARP	42	Who has 192.168.1.1? Tell 192.168.1.66
8496	318.053540	Ubiquiti_c3:d5:9c	Motorola_13:87:7b	ARP	60	192.168.1.1 is at f0:9f:c2:c3:d5:9c

6.4 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Ripley”

IPA

5107	158.025466	192.168.1.52	200.54.56.74	TLSv1.2	299 Client Hello
5108	158.029472	200.54.56.74	192.168.1.52	TLSv1.2	1514 Server Hello
5109	158.029533	200.54.56.74	192.168.1.52	TCP	1514 443 → 63512 [ACK] Seq=1449 Ack=234 Win=4380 Len=1448 TSval=1373464066 TSecr=679033276 [TCP segment of a reassembled PDU]
5110	158.029565	200.54.56.74	192.168.1.52	TLSv1.2	332 Certificate, Server Hello Done
5112	158.164446	192.168.1.52	200.54.56.74	TCP	66 63512 → 443 [ACK] Seq=234 Ack=2897 Win=65535 Len=0 TSval=679033402 TSecr=1373464066
5113	158.799515	192.168.1.52	200.54.56.74	TCP	66 63512 → 443 [ACK] Seq=234 Ack=3163 Win=65535 Len=0 TSval=679033997 TSecr=1373464066
5116	158.811445	192.168.1.52	200.54.56.74	TLSv1.2	384 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
5117	158.814566	200.54.56.74	192.168.1.52	TCP	66 443 → 63512 [ACK] Seq=3163 Ack=552 Win=4931 Len=0 TSval=1373464851 TSecr=679034024
5118	158.815872	200.54.56.74	192.168.1.52	TLSv1.2	72 Change Cipher Spec
5119	158.815897	200.54.56.74	192.168.1.52	TLSv1.2	111 Encrypted Handshake Message
5121	159.204764	192.168.1.52	200.54.56.74	TCP	66 63512 → 443 [ACK] Seq=552 Ack=3169 Win=65535 Len=0 TSval=679034448 TSecr=1373464852
5122	159.204799	192.168.1.52	200.54.56.74	TCP	66 63512 → 443 [ACK] Seq=552 Ack=3214 Win=65535 Len=0 TSval=679034448 TSecr=1373464852
5125	159.205185	192.168.1.52	200.54.56.74	TLSv1.2	467 Application Data

6.5 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Chile Empresas”

IPA

7038	264.551041	192.168.1.52	45.60.4.56	TLSv1.2	304 Client Hello
7039	264.603519	45.60.4.56	192.168.1.52	TCP	66 443 → 63534 [ACK] Seq=1 Ack=239 Win=30080 Len=0 TSval=1108035953 TSecr=679139604
7040	264.603832	45.60.4.56	192.168.1.52	TLSv1.2	1514 Server Hello
7041	264.603893	45.60.4.56	192.168.1.52	TCP	1514 443 → 63534 [ACK] Seq=1449 Ack=239 Win=30080 Len=1448 TSval=1108035953 TSecr=679139604 [TCP segment of a reassembled PDU]
7042	264.603923	45.60.4.56	192.168.1.52	TLSv1.2	1266 Certificate [TCP segment of a reassembled PDU]
7043	264.604701	45.60.4.56	192.168.1.52	TLSv1.2	864 Certificate Status, Server Key Exchange, Server Hello Done
7044	264.734223	192.168.1.52	45.60.4.56	TCP	66 63534 → 443 [ACK] Seq=239 Ack=2897 Win=129536 Len=0 TSval=679139821 TSecr=1108035953
7045	264.734257	192.168.1.52	45.60.4.56	TCP	66 63534 → 443 [ACK] Seq=239 Ack=4097 Win=128384 Len=0 TSval=679139821 TSecr=1108035953
7046	264.734296	192.168.1.52	45.60.4.56	TCP	66 63534 → 443 [ACK] Seq=239 Ack=4895 Win=127616 Len=0 TSval=679139821 TSecr=1108035953
7047	264.734321	192.168.1.52	45.60.4.56	TCP	66 [TCP Window Update] 63534 → 443 [ACK] Seq=239 Ack=4895 Win=131072 Len=0 TSval=679139822 TSecr=1108035953
7048	264.808383	192.168.1.52	45.60.4.56	TLSv1.2	228 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
7049	264.862056	45.60.4.56	192.168.1.52	TLSv1.2	117 Change Cipher Spec, Encrypted Handshake Message
7050	265.450869	192.168.1.52	45.60.4.56	TCP	66 63534 → 443 [ACK] Seq=401 Ack=4946 Win=130944 Len=0 TSval=679140547 TSecr=1108036018
7051	265.452159	192.168.1.52	45.60.4.56	TLSv1.2	448 Application Data

6.6 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Scotiabank”

IPA

10211	357.769591	192.168.1.52	96.17.19.110	TLSv1.2	293 Client Hello
10212	357.771179	96.17.19.110	192.168.1.52	TCP	66 443 → 63567 [ACK] Seq=1 Ack=228 Win=30080 Len=0 TSval=213384652 TSecr=679232497
10213	357.771730	96.17.19.110	192.168.1.52	TLSv1.2	1514 Server Hello
10214	357.771781	96.17.19.110	192.168.1.52	TCP	1514 443 → 63567 [ACK] Seq=1449 Ack=228 Win=30080 Len=1448 TSval=213384652 TSecr=679232497 [TCP segment of a reassembled PDU]
10215	357.771812	96.17.19.110	192.168.1.52	TLSv1.2	1266 Certificate [TCP segment of a reassembled PDU]
10216	357.772542	96.17.19.110	192.168.1.52	TLSv1.2	1514 Certificate Status [TCP segment of a reassembled PDU]
10217	358.021273	192.168.1.52	96.17.19.110	TCP	66 63567 → 443 [ACK] Seq=228 Ack=2897 Win=128768 Len=0 TSval=679232819 TSecr=213384652
10218	358.021307	192.168.1.52	96.17.19.110	TCP	66 63567 → 443 [ACK] Seq=228 Ack=4097 Win=127616 Len=0 TSval=679232819 TSecr=213384652
10219	358.021373	192.168.1.52	96.17.19.110	TCP	66 [TCP Window Update] 63567 → 443 [ACK] Seq=228 Ack=4097 Win=131072 Len=0 TSval=679232819 TSecr=213384652
10220	358.023199	96.17.19.110	192.168.1.52	TLSv1.2	363 Server Key Exchange, Server Hello Done
10221	358.123683	192.168.1.52	96.17.19.110	TCP	66 63567 → 443 [ACK] Seq=228 Ack=5545 Win=131072 Len=0 TSval=679232920 TSecr=213384653
10222	358.195231	192.168.1.52	96.17.19.110	TCP	66 63567 → 443 [ACK] Seq=228 Ack=5842 Win=130688 Len=0 TSval=679232980 TSecr=213384904
10223	358.195267	192.168.1.52	96.17.19.110	TLSv1.2	192 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10224	358.199227	96.17.19.110	192.168.1.52	TLSv1.2	117 Change Cipher Spec, Encrypted Handshake Message

Tráfico DNS

IPA

	Time	Source	Destination	Protocol	Length	Info
5244	164.252904	192.168.1.52	192.168.1.1	DNS	83	Standard query 0xc845 A www-google-analytics.l.google.com
5245	164.253311	192.168.1.1	192.168.1.52	DNS	189	Standard query response 0xc845 A www-google-analytics.l.google.com A 172.217.192.139 A 172.217.192.102 A 172.217.192.138 A 172.217.192.113 A 172.217.192.101 A 172.217.192
5363	167.453602	192.168.1.52	192.168.1.1	DNS	74	Standard query 0x2133 A www.google.com
5364	167.456653	192.168.1.1	192.168.1.52	DNS	170	Standard query response 0x2133 A www.google.com A 64.233.186.105 A 64.233.186.147 A 64.233.186.99 A 64.233.186.104 A 64.233.186.106 A 64.233.186.103
5419	181.309655	192.168.1.52	192.168.1.1	DNS	83	Standard query 0x9677 A col.eum-appdynamics.com
5420	181.314112	192.168.1.1	192.168.1.52	DNS	211	Standard query response 0x9677 A col.eum-appdynamics.com A 34.197.20.226 A 34.199.172.226 A 34.200.114.102 A 34.198.36.67 A 34.198.78.42 A 34.233.86.134 A 34.205.208.184
5579	228.241223	192.168.1.52	192.168.1.1	DNS	79	Standard query 0xd282 A app-measurement.com
5580	228.243372	192.168.1.1	192.168.1.52	DNS	175	Standard query response 0xd282 A app-measurement.com A 64.233.190.102 A 64.233.190.113 A 64.233.190.138 A 64.233.190.101 A 64.233.190.100 A 64.233.190.139
5791	236.225432	192.168.1.52	192.168.1.1	DNS	94	Standard query 0xd8e2 A p9-buy.itunes-apple.com.akadns.net
5792	236.250715	192.168.1.1	192.168.1.52	DNS	110	Standard query response 0xd8e2 A p9-buy.itunes-apple.com.akadns.net A 17.173.66.103
5830	237.231938	192.168.1.52	192.168.1.1	DNS	94	Standard query 0xd8e2 A p9-buy.itunes-apple.com.akadns.net
5831	237.232154	192.168.1.1	192.168.1.52	DNS	110	Standard query response 0xd8e2 A p9-buy.itunes-apple.com.akadns.net A 17.173.66.103
7009	263.241013	192.168.1.52	192.168.1.1	DNS	88	Standard query 0x7589 A portalpersonas.bancochile.cl
7010	263.244609	192.168.1.1	192.168.1.52	DNS	140	Standard query response 0x7589 A portalpersonas.bancochile.cl CNAME prn2kam.x.incapdns.net A 45.60.4.56
7193	269.938800	192.168.1.52	192.168.1.1	DNS	79	Standard query 0xbec6 A login.bancochile.cl
7194	269.934185	192.168.1.1	192.168.1.52	DNS	131	Standard query response 0xbec6 A login.bancochile.cl CNAME x3hfncr.x.incapdns.net A 45.60.4.56
7297	277.182476	192.168.1.52	192.168.1.1	DNS	126	Standard query 0x586b A imagepersonas-bancochile-cl-2048333488.us-east-1.elb.amazonaws.com
7298	277.184130	192.168.1.1	192.168.1.52	DNS	174	Standard query response 0x586b A imagepersonas-bancochile-cl-2048333488.us-east-1.elb.amazonaws.com A 174.129.237.97 A 54.235.129.1 A 54.197.248.88
7299	277.193856	192.168.1.52	192.168.1.1	DNS	93	Standard query 0x41ca A www-googletagmanager.l.google.com
7301	277.194961	192.168.1.1	192.168.1.52	DNS	109	Standard query response 0x41ca A www-googletagmanager.l.google.com A 172.217.192.97
7314	277.262550	192.168.1.52	192.168.1.1	DNS	124	Standard query 0x01de A mainpersonas-bancochile-cl-587264832.us-east-1.elb.amazonaws.com
7317	277.264216	192.168.1.1	192.168.1.52	DNS	172	Standard query response 0x01de A mainpersonas-bancochile-cl-587264832.us-east-1.elb.amazonaws.com A 54.225.239.163 A 184.73.158.146 A 54.225.222.156
7907	281.929301	192.168.1.52	192.168.1.1	DNS	83	Standard query 0x9abe A stats.l.doubleclick.net
7910	281.932235	192.168.1.1	192.168.1.52	DNS	147	Standard query response 0x9abe A stats.l.doubleclick.net A 64.233.186.156 A 64.233.186.155 A 64.233.186.157 A 64.233.186.154
7953	282.888353	192.168.1.52	192.168.1.1	DNS	125	Standard query 0xb5b8 A notespersonas-bancochile-cl-581130394.us-east-1.elb.amazonaws.com
7954	282.888383	192.168.1.52	192.168.1.1	DNS	125	Standard query 0xc56e A velocpersonas-bancochile-cl-286709436.us-east-1.elb.amazonaws.com
7955	282.892432	192.168.1.1	192.168.1.52	DNS	173	Standard query response 0xb5b8 A notespersonas-bancochile-cl-581130394.us-east-1.elb.amazonaws.com A 54.243.187.113 A 54.243.193.159 A 184.73.222.160
7966	282.894805	192.168.1.1	192.168.1.52	DNS	173	Standard query response 0xc56e A velocpersonas-bancochile-cl-286709436.us-east-1.elb.amazonaws.com A 54.243.225.35 A 54.197.253.50 A 23.23.172.85
7998	283.895058	192.168.1.52	192.168.1.1	DNS	125	Standard query 0xc56e A velocpersonas-bancochile-cl-286709436.us-east-1.elb.amazonaws.com
7999	283.895328	192.168.1.1	192.168.1.52	DNS	173	Standard query response 0xc56e A velocpersonas-bancochile-cl-286709436.us-east-1.elb.amazonaws.com A 23.23.172.85 A 54.197.253.50 A 54.243.225.35
8121	285.055946	192.168.1.52	192.168.1.1	DNS	76	Standard query 0xcee0 A gs-loc.apple.com
8122	285.059634	192.168.1.1	192.168.1.52	DNS	177	Standard query response 0xcee0 A gs-loc.apple.com CNAME gs-loc-nev.ls-apple.com.akadns.net CNAME gs-loc.ls-apple.com.akadns.net A 17.134.127.79 A 17.134.127.97
8279	286.906755	192.168.1.52	192.168.1.1	DNS	73	Standard query 0x4b7e A www.google.cl
8280	286.907034	192.168.1.1	192.168.1.52	DNS	89	Standard query response 0x4b7e A www.google.cl A 64.233.190.94
8736	297.653699	192.168.1.52	192.168.1.1	DNS	82	Standard query 0x8179 A x3hfncr.x.incapdns.net
8737	297.655247	192.168.1.1	192.168.1.52	DNS	98	Standard query response 0x8179 A x3hfncr.x.incapdns.net A 45.60.4.56
8968	311.562895	192.168.1.52	192.168.1.1	DNS	82	Standard query 0xd244 A prn2kam.x.incapdns.net
8969	311.564634	192.168.1.1	192.168.1.52	DNS	98	Standard query response 0xd244 A prn2kam.x.incapdns.net A 45.60.4.56
9083	316.945124	192.168.1.52	192.168.1.1	DNS	126	Standard query 0x43be A imagepersonas-bancochile-cl-2048333488.us-east-1.elb.amazonaws.com
9084	316.948187	192.168.1.1	192.168.1.52	DNS	174	Standard query response 0x43be A imagepersonas-bancochile-cl-2048333488.us-east-1.elb.amazonaws.com A 174.129.237.97 A 54.235.129.1 A 54.197.248.88
9125	317.949860	192.168.1.52	192.168.1.1	DNS	126	Standard query 0x43be A imagepersonas-bancochile-cl-2048333488.us-east-1.elb.amazonaws.com
9126	317.949999	192.168.1.1	192.168.1.52	DNS	174	Standard query response 0x43be A imagepersonas-bancochile-cl-2048333488.us-east-1.elb.amazonaws.com A 54.197.248.88 A 54.235.129.1 A 174.129.237.97
9483	322.758036	192.168.1.52	192.168.1.1	DNS	124	Standard query 0x5bb0 A mainpersonas-bancochile-cl-587264832.us-east-1.elb.amazonaws.com
9487	322.751318	192.168.1.1	192.168.1.52	DNS	172	Standard query response 0x5bb0 A mainpersonas-bancochile-cl-587264832.us-east-1.elb.amazonaws.com A 54.225.222.156 A 54.225.239.163 A 184.73.158.146
9519	323.762670	192.168.1.52	192.168.1.1	DNS	124	Standard query 0x5bb0 A mainpersonas-bancochile-cl-587264832.us-east-1.elb.amazonaws.com
9520	323.762904	192.168.1.1	192.168.1.52	DNS	172	Standard query response 0x5bb0 A mainpersonas-bancochile-cl-587264832.us-east-1.elb.amazonaws.com A 184.73.158.146 A 54.225.239.163 A 54.225.222.156
9682	331.309142	192.168.1.52	192.168.1.1	DNS	82	Standard query 0x0f89 A x3hfncr.x.incapdns.net
9684	331.310760	192.168.1.1	192.168.1.52	DNS	98	Standard query response 0x0f89 A x3hfncr.x.incapdns.net A 45.60.4.56
0194	355.185348	192.168.1.52	192.168.1.1	DNS	77	Standard query 0x2d65 A www.scotiabank.cl
0195	355.187098	192.168.1.1	192.168.1.52	DNS	170	Standard query response 0x2d65 A www.scotiabank.cl CNAME www.scotiabank.cl.edgekey.net CNAME e10175.b.akamaiedge.net A 96.17.19.110
0200	356.192556	192.168.1.52	192.168.1.1	DNS	77	Standard query 0x2d65 A www.scotiabank.cl
0201	356.192827	192.168.1.1	192.168.1.52	DNS	173	Standard query response 0x2d65 A www.scotiabank.cl CNAME www.scotiabank.cl.edgekey.net CNAME e10175.b.akamaiedge.net A 96.17.19.110
0238	360.474120	192.168.1.52	192.168.1.1	DNS	93	Standard query 0x8a91 A www-googletagmanager.l.google.com
0243	360.475916	192.168.1.1	192.168.1.52	DNS	109	Standard query response 0x8a91 A www-googletagmanager.l.google.com A 172.217.192.97

Tráfico HTTP

IPA

No se detectó trafico HTTP durante este periodo.

Otro Tráfico

IPA

	Time	Source	Destination	Protocol	Length	Info
29	2.788018	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	Who has 192.168.1.1? Tell 192.168.1.52
30	2.788112	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	192.168.1.1 is at f0:9f:c2:c3:d5:9c
1067	24.357465	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	Who has 192.168.1.52? Tell 192.168.1.1
1074	24.443371	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.52 is at 98:9e:63:6b:d1:af
3649	71.016913	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	Who has 192.168.1.52? Tell 192.168.1.1
3650	71.079940	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.52 is at 98:9e:63:6b:d1:af
4871	92.676796	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	Who has 192.168.1.1? Tell 192.168.1.52
4872	92.676886	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	192.168.1.1 is at f0:9f:c2:c3:d5:9c
4952	104.156480	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	Who has 192.168.1.52? Tell 192.168.1.1
4953	104.256760	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.52 is at 98:9e:63:6b:d1:af
5195	162.905760	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	Who has 192.168.1.52? Tell 192.168.1.1
5196	163.050039	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.52 is at 98:9e:63:6b:d1:af
5443	182.721423	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	Who has 192.168.1.1? Tell 192.168.1.52
5444	182.721489	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	192.168.1.1 is at f0:9f:c2:c3:d5:9c
5481	195.655386	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	Who has 192.168.1.52? Tell 192.168.1.1
5482	195.871519	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.52 is at 98:9e:63:6b:d1:af
5673	232.384902	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	Who has 192.168.1.52? Tell 192.168.1.1
5679	232.422185	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.52 is at 98:9e:63:6b:d1:af
7078	268.254469	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	Who has 192.168.1.52? Tell 192.168.1.1
7079	269.254448	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	Who has 192.168.1.52? Tell 192.168.1.1
7080	269.281478	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.52 is at 98:9e:63:6b:d1:af
7081	269.304441	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.52 is at 98:9e:63:6b:d1:af
7133	272.661096	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	Who has 192.168.1.1? Tell 192.168.1.52
7134	272.661318	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	192.168.1.1 is at f0:9f:c2:c3:d5:9c
8835	301.284054	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	Who has 192.168.1.52? Tell 192.168.1.1
8836	301.374974	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.52 is at 98:9e:63:6b:d1:af
9849	333.153670	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	Who has 192.168.1.52? Tell 192.168.1.1
9850	333.211800	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.52 is at 98:9e:63:6b:d1:af
10370	362.652427	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	Who has 192.168.1.1? Tell 192.168.1.52
10371	362.652486	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	192.168.1.1 is at f0:9f:c2:c3:d5:9c
10851	368.563250	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	Who has 192.168.1.52? Tell 192.168.1.1
10868	369.413466	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.52 is at 98:9e:63:6b:d1:af
13801	404.742784	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	Who has 192.168.1.52? Tell 192.168.1.1
13835	404.829445	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.52 is at 98:9e:63:6b:d1:af
15610	442.822310	Ubiquiti_c3:d5:9c	Apple_6b:d1:af	ARP	60	Who has 192.168.1.52? Tell 192.168.1.1
15611	442.848983	Apple_6b:d1:af	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.52 is at 98:9e:63:6b:d1:af

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.

7.1 APK

Origen	Destino	Tipo de Tráfico	Descripción
192.168.1.56	50.22.89.18	TLSv1.2	khipu
192.168.1. 66	200.54.56.74	TLSv1.2	Banco Ripley
192.168.1. 66	45.60.4.56	TLSv1.2	Banco Chile
192.168.1. 66	96.17.19.110	TLSv1.2	Banco Scotiabank

7.2 IPA

Origen	Destino	Tipo de Tráfico	Descripción
192.168.1.56	50.22.89.18	TLSv1.2	khipu
192.168.1. 52	200.54.56.74	TLSv1.2	Banco Ripley
192.168.1. 52	45.60.4.56	TLSv1.2	Banco Chile
192.168.1. 52	96.17.19.110	TLSv1.2	Banco Scotiabank

8 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

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

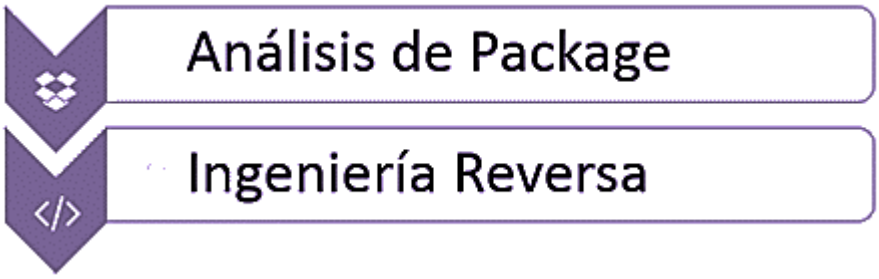
Se detectaron 2 vulnerabilidades en la implementación de SSL/TLS del sitio khipu.com las que afectan la confidencialidad de la información, sin embargo, estas vulnerabilidades tienen un alto grado de dificultad de explotación y se requieren condiciones especiales para su correcta explotación.

9 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

10 Ethical Hacking Mobile

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 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.

11 Análisis APK

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

Nombre	com.khipu.android-6.8.1.apk
SHA256	a1e21d7bb85da81221c2eed04824b3e4ee90731b651e9be7b93f67c612e2bcb
Tamaño	7.48 MB
Tipo	.apk
URLs Interesantes	4
IPs encontradas	0
Emails encontrados	0

URLs detectadas

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

Direcciones de correo detectados

No se encontraron direcciones IP en el análisis.

Direcciones de correo detectados

No se encontraron direcciones de correo en el análisis.

12 Análisis IPA

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

Nombre	khipu6.24.ipa
SHA256	0b6b1dc2c7ba0e9f41b47998abddc9dc45fb82c975c4564d7b11675f2dd4697a
Tamaño	14.7 MB
Tipo	.ipa
URLs Interesantes	0
IPs encontradas	0
Emails encontrados	0

URLs detectadas

No se encontraron URLs en el análisis.

Direcciones de correo detectados

No se encontraron direcciones IP en el análisis.

Direcciones de correo detectados

No se encontraron direcciones.

13 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 el archivo .ipa y el archivo .apk correspondiente a IOS Y Android. En este periodo se analizó la .ipa y la .apk debido a un cambio en su hash y versión.

IPA		APK	
Motor	**Estado**	**Motor**	**Estado**
Ad-Aware	✓	**Ad-Aware**	✓
AegisLab	✓	**AegisLab**	✓
AhnLab-V3	✓	**AhnLab-V3**	✓
Alibaba	✓	**Alibaba**	✓
ALYac	✓	**ALYac**	✓
Antiy-AVL	✓	**Antiy-AVL**	✓
Arcabit	✓	**Arcabit**	✓
Avast	✓	**Avast**	✓
Avast-Mobile	✓	**Avast-Mobile**	✓
AVG	✓	**AVG**	✓
Avira (no cloud)	✓	**Avira (no cloud)**	✓
AVware	✓	**AVware**	✓
Babable	✓	**Babable**	✓

Baidu	✓	**Baidu**	✓
BitDefender	✓	**BitDefender**	✓
Bkav	✓	**Bkav**	✓
CAT-QuickHeal	✓	**CAT-QuickHeal**	✓
ClamAV	✓	**ClamAV**	✓
CMC	✓	**CMC**	✓
Comodo	✓	**Comodo**	✓
Cyren	✓	**Cyren**	✓
DrWeb	✓	**DrWeb**	✓
Emsisoft	✓	**Emsisoft**	✓
ESET-NOD32	✓	**ESET-NOD32**	✓
F-Prot	✓	**F-Prot**	✓
F-Secure	✓	**F-Secure**	✓
Fortinet	✓	**Fortinet**	✓
GData	✓	**GData**	✓
Ikarus	✓	**Ikarus**	✓
Jiangmin	✓	**Jiangmin**	✓
K7AntiVirus	✓	**K7AntiVirus**	✓
K7GW	✓	**K7GW**	✓

Kaspersky	✓	**Kaspersky**	✓
Kingsoft	✓	**Kingsoft**	✓
Malwarebytes	✓	**Malwarebytes**	✓
MAX	✓	**MAX**	✓
McAfee	✓	**McAfee**	✓
McAfee-GW-Edition	✓	**McAfee-GW-Edition**	✓
Microsoft	✓	**Microsoft**	✓
eScan	✓	**eScan**	✓
NANO-Antivirus	✓	**NANO-Antivirus**	✓
Panda	✓	**Panda**	✓
Qihoo-360	✓	**Qihoo-360**	✓
Rising	✓	**Rising**	✓
Sophos AV	✓	**Sophos AV**	✓
SUPERAntiSpyware	✓	**SUPERAntiSpyware**	✓
Symantec	✓	**Symantec**	✓
TACHYON	✓	**Symantec Mobile Insight**	✓
Tencent	✓	**TACHYON**	✓
TheHacker	✓	**Tencent**	✓
VBA32	✓	**TheHacker**	✓
VIPRE	✓	**TrendMicro**	✓

ViRobot	✓	**TrendMicro-House-Call**	✓
Yandex	✓	**Trustlook**	✓
Zillya	✓	**VBA32**	✓
ZoneAlarm by Check Point	✓	**VIPRE**	✓
Zoner	✓	**ViRobot**	✓
		Yandex	✓
		Zillya	✓
		ZoneAlarm by Check Point	✓
		Zoner	✓

14 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/

15 Anexos

#	Archivo	SHA256SUM
1	APK20190115.pcap	b8a704ed9beeb8acc4009c48b20f74480b1d1d6cac276bc733c392dc0e657e1f
2	IOS20190115.pcap	aac003677825e819fdfce9ac7b882e481efb2046b7157d0890b83a42ab84be75