Dirigido a:
Eduardo Parraguez
khipu

JULIO
2019

INFORME TÉCNICO

Análisis de Tráfico de Datos Junio 2019

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
15-07-2019	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. khipu no almacena ni envía claves ni contraseñas a sus servidores o a terceros.

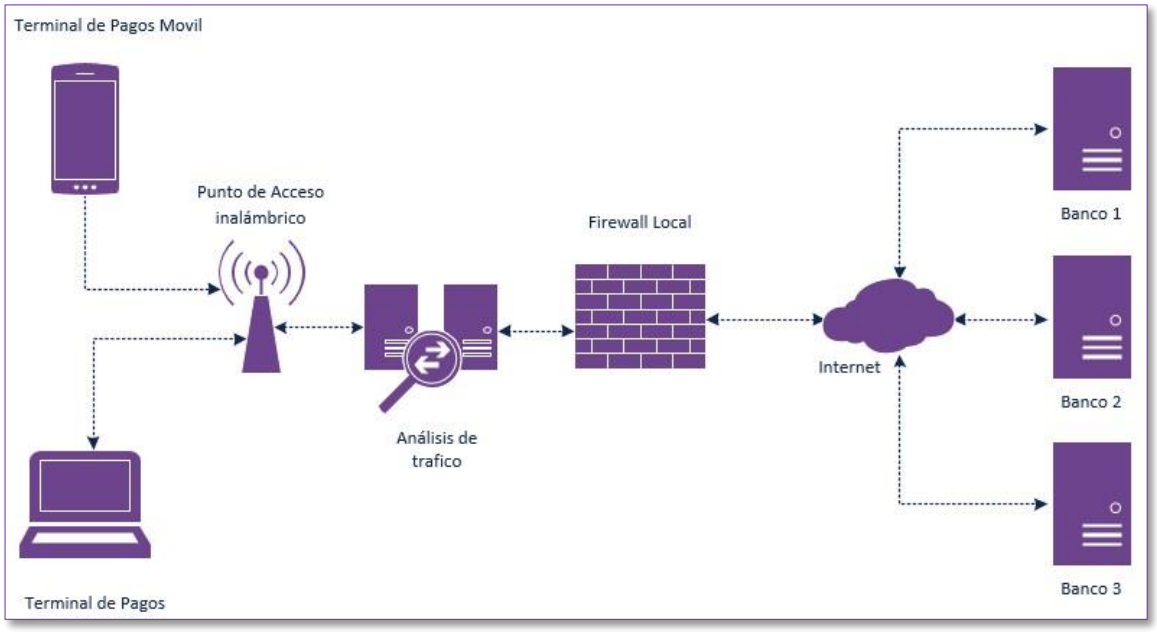
El presente análisis consiste en el monitoreo y análisis de todo el tráfico que genera la aplicación para las distintas plataformas, con el fin de detectar conexiones sospechosas. La revisión incluye la versión del terminal de pagos disponible para iOS y Android.

3 Objetivo

El análisis se realiza mensualmente, en un día y hora definida por Nivel4 sin que khipu conozca previamente esta información y tiene por objetivo certificar que la empresa 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 con el siguiente diagrama:



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

5 Ámbito

Para el actual período correspondiente al mes de Junio se registraron cambios para las aplicaciones de **iOS y Android** tanto en su versión como en su HASH. Las versiones de escritorio de la aplicación han sido descontinuadas en las últimas versiones de Firefox, Chrome y MacOS debido a esto no fueron analizadas durante este periodo.

Plataforma	Versión	SHA256SUM
Android	7.1.17	61e3a5d9ead9eb38121636e0945e0edd3a3ed79b9708b349827549b2560f7806
iOS	7.3	af2511d4bc212640f9dd47e4c4fa991f7048ba57aa41b0566c47916292f9cea9

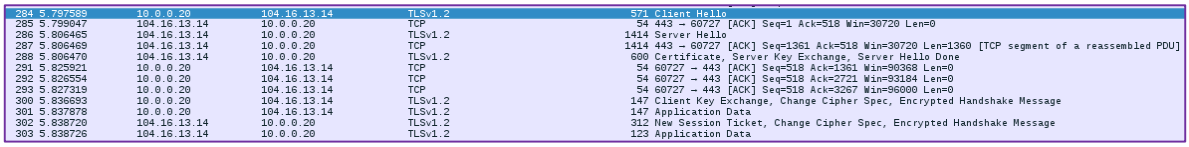
6 Análisis de tráfico de datos

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 “BCI”

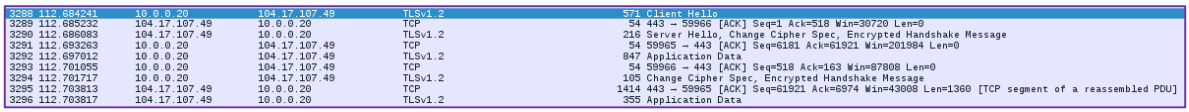
APK



284	5.797589	10.0.0.20	104.16.13.14	TLSv1.2	571 Client Hello
285	5.799047	104.16.13.14	10.0.0.20	TCP	54 443 → 60727 [ACK] Seq=1 Ack=518 Win=30720 Len=0
286	5.806465	104.16.13.14	10.0.0.20	TLSv1.2	1414 Server Hello
287	5.806469	104.16.13.14	10.0.0.20	TCP	1414 443 → 60727 [ACK] Seq=1361 Ack=518 Win=30720 Len=1360 [TCP segment of a reassembled PDU]
288	5.806470	104.16.13.14	10.0.0.20	TLSv1.2	600 Certificate, Server Key Exchange, Server Hello Done
291	5.825921	10.0.0.20	104.16.13.14	TCP	54 60727 → 443 [ACK] Seq=518 Ack=1361 Win=90368 Len=0
292	5.826554	10.0.0.20	104.16.13.14	TCP	54 60727 → 443 [ACK] Seq=518 Ack=2721 Win=93184 Len=0
293	5.827319	10.0.0.20	104.16.13.14	TCP	54 60727 → 443 [ACK] Seq=518 Ack=3267 Win=96000 Len=0
300	5.836693	10.0.0.20	104.16.13.14	TLSv1.2	147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
301	5.837878	10.0.0.20	104.16.13.14	TLSv1.2	147 Application Data
302	5.838720	104.16.13.14	10.0.0.20	TLSv1.2	312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
303	5.838726	104.16.13.14	10.0.0.20	TLSv1.2	123 Application Data

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

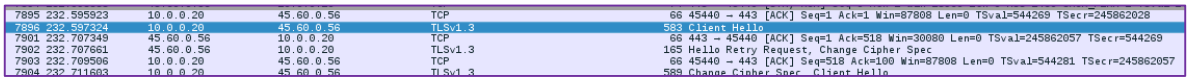
APK



3288	112.684241	10.0.0.20	104.17.107.49	TLSv1.2	571 Client Hello
3289	112.685232	104.17.107.49	10.0.0.20	TCP	54 443 → 59966 [ACK] Seq=1 Ack=518 Win=30720 Len=0
3290	112.686083	104.17.107.49	10.0.0.20	TLSv1.2	216 Server Hello, Change Cipher Spec, Encrypted Handshake Message
3291	112.693263	10.0.0.20	104.17.107.49	TCP	54 59965 → 443 [ACK] Seq=6181 Ack=61921 Win=201984 Len=0
3292	112.697012	10.0.0.20	104.17.107.49	TLSv1.2	847 Application Data
3293	112.701055	10.0.0.20	104.17.107.49	TCP	54 59966 → 443 [ACK] Seq=518 Ack=163 Win=87808 Len=0
3294	112.701717	10.0.0.20	104.17.107.49	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
3295	112.703813	104.17.107.49	10.0.0.20	TCP	1414 443 → 59965 [ACK] Seq=61921 Ack=6974 Win=43008 Len=1360 [TCP segment of a reassembled PDU]
3296	112.703817	104.17.107.49	10.0.0.20	TLSv1.2	355 Application Data

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

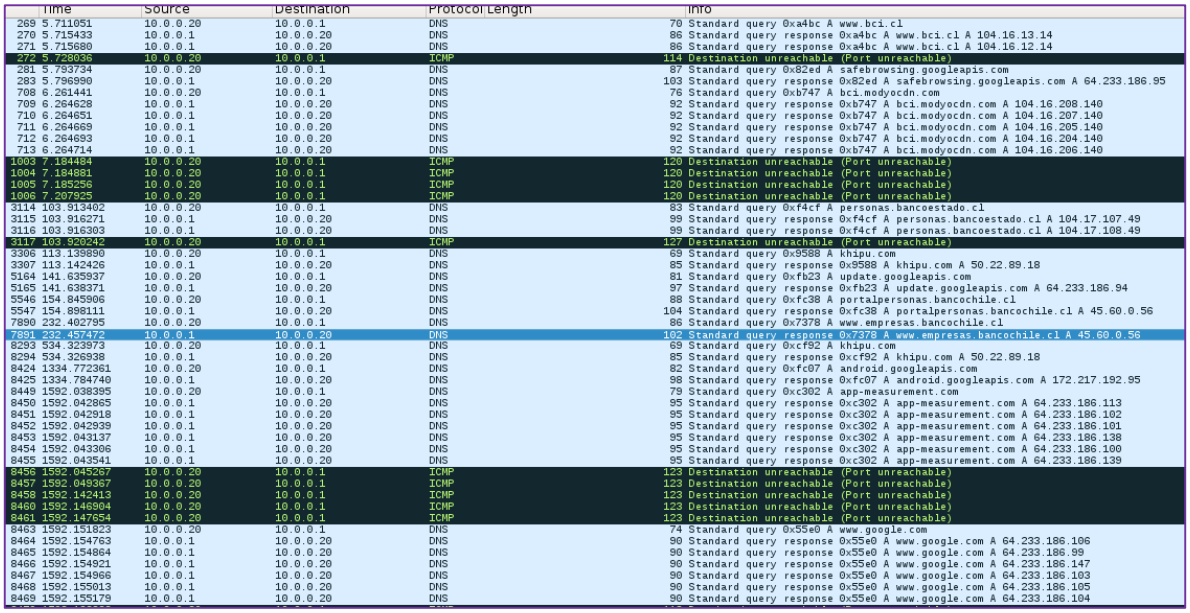
APK



7895	232.595923	10.0.0.20	45.60.0.56	TCP	66 45440 → 443 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSval=544269 TSecr=245862028
7896	232.597324	10.0.0.20	45.60.0.56	TLSv1.3	583 Client Hello
7901	232.707349	45.60.0.56	10.0.0.20	TCP	66 443 → 45440 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=245862057 TSecr=544269
7902	232.707661	45.60.0.56	10.0.0.20	TLSv1.3	165 Hello Retry Request, Change Cipher Spec
7903	232.709506	10.0.0.20	45.60.0.56	TCP	66 45440 → 443 [ACK] Seq=518 Ack=100 Win=87808 Len=0 TSval=544281 TSecr=245862057
7904	232.711603	10.0.0.20	45.60.0.56	TLSv1.3	589 Change Cipher Spec, Client Hello

Tráfico DNS

APK



No.	Time	Source	Destination	Protocol	Length	Info
269	5.711051	10.0.0.20	10.0.0.1	DNS	70	Standard query 0xa4bc A www.bci.cl
270	5.715433	10.0.0.1	10.0.0.20	DNS	86	Standard query response 0xa4bc A www.bci.cl A 104.16.13.14
271	5.715680	10.0.0.1	10.0.0.20	DNS	86	Standard query response 0xa4bc A www.bci.cl A 104.16.12.14
272	5.728036	10.0.0.20	10.0.0.1	ICMP	114	Destination unreachable (Port unreachable)
281	5.793734	10.0.0.20	10.0.0.1	DNS	87	Standard query 0x82ed A safebrowsing.googleapis.com
283	5.796990	10.0.0.1	10.0.0.20	DNS	103	Standard query response 0x82ed A safebrowsing.googleapis.com A 64.233.186.95
708	6.261441	10.0.0.20	10.0.0.1	DNS	76	Standard query 0xb747 A bci.modyocdn.com
709	6.264628	10.0.0.1	10.0.0.20	DNS	92	Standard query response 0xb747 A bci.modyocdn.com A 104.16.208.140
710	6.264651	10.0.0.1	10.0.0.20	DNS	92	Standard query response 0xb747 A bci.modyocdn.com A 104.16.207.140
711	6.264669	10.0.0.1	10.0.0.20	DNS	92	Standard query response 0xb747 A bci.modyocdn.com A 104.16.205.140
712	6.264693	10.0.0.1	10.0.0.20	DNS	92	Standard query response 0xb747 A bci.modyocdn.com A 104.16.204.140
713	6.264714	10.0.0.1	10.0.0.20	DNS	92	Standard query response 0xb747 A bci.modyocdn.com A 104.16.206.140
1003	7.184454	10.0.0.20	10.0.0.1	ICMP	120	Destination unreachable (Port unreachable)
1004	7.184881	10.0.0.20	10.0.0.1	ICMP	120	Destination unreachable (Port unreachable)
1005	7.185256	10.0.0.20	10.0.0.1	ICMP	120	Destination unreachable (Port unreachable)
1006	7.207925	10.0.0.20	10.0.0.1	ICMP	120	Destination unreachable (Port unreachable)
3114	103.913402	10.0.0.20	10.0.0.1	DNS	83	Standard query 0xf4cf A personas.bancoestado.cl
3115	103.916271	10.0.0.1	10.0.0.20	DNS	99	Standard query response 0xf4cf A personas.bancoestado.cl A 104.17.107.49
3116	103.916303	10.0.0.1	10.0.0.20	DNS	99	Standard query response 0xf4cf A personas.bancoestado.cl A 104.17.108.49
3117	103.920242	10.0.0.20	10.0.0.1	ICMP	127	Destination unreachable (Port unreachable)
3306	113.139890	10.0.0.20	10.0.0.1	DNS	69	Standard query 0x9588 A khipu.com
3307	113.142426	10.0.0.1	10.0.0.20	DNS	85	Standard query response 0x9588 A khipu.com A 50.22.89.18
5164	141.635937	10.0.0.20	10.0.0.1	DNS	81	Standard query 0xfb23 A update.googleapis.com
5165	141.638371	10.0.0.1	10.0.0.20	DNS	97	Standard query response 0xfb23 A update.googleapis.com A 64.233.186.94
5546	154.845906	10.0.0.20	10.0.0.1	DNS	88	Standard query 0xfc38 A portalpersonas.bancochile.cl
5547	154.898111	10.0.0.1	10.0.0.20	DNS	104	Standard query response 0xfc38 A portalpersonas.bancochile.cl A 45.60.0.56
7890	232.402795	10.0.0.20	10.0.0.1	DNS	86	Standard query 0x7378 A www.empresas.bancochile.cl
7891	232.457472	10.0.0.1	10.0.0.20	DNS	102	Standard query response 0x7378 A www.empresas.bancochile.cl A 45.60.0.56
8293	534.323973	10.0.0.20	10.0.0.1	DNS	69	Standard query 0xcf92 A khipu.com
8294	534.326938	10.0.0.1	10.0.0.20	DNS	85	Standard query response 0xcf92 A khipu.com A 50.22.89.18
8424	1334.772361	10.0.0.20	10.0.0.1	DNS	82	Standard query 0xfc07 A android.googleapis.com
8425	1334.784740	10.0.0.1	10.0.0.20	DNS	98	Standard query response 0xfc07 A android.googleapis.com A 172.217.192.95
8449	1592.038395	10.0.0.20	10.0.0.1	DNS	79	Standard query 0xc302 A app-measurement.com
8450	1592.042865	10.0.0.1	10.0.0.20	DNS	95	Standard query response 0xc302 A app-measurement.com A 64.233.186.113
8451	1592.042918	10.0.0.1	10.0.0.20	DNS	95	Standard query response 0xc302 A app-measurement.com A 64.233.186.102
8452	1592.042939	10.0.0.1	10.0.0.20	DNS	95	Standard query response 0xc302 A app-measurement.com A 64.233.186.101
8453	1592.043137	10.0.0.1	10.0.0.20	DNS	95	Standard query response 0xc302 A app-measurement.com A 64.233.186.138
8454	1592.043306	10.0.0.1	10.0.0.20	DNS	95	Standard query response 0xc302 A app-measurement.com A 64.233.186.100
8455	1592.043541	10.0.0.1	10.0.0.20	DNS	95	Standard query response 0xc302 A app-measurement.com A 64.233.186.139
8456	1592.045267	10.0.0.20	10.0.0.1	ICMP	123	Destination unreachable (Port unreachable)
8457	1592.049367	10.0.0.20	10.0.0.1	ICMP	123	Destination unreachable (Port unreachable)
8458	1592.142413	10.0.0.20	10.0.0.1	ICMP	123	Destination unreachable (Port unreachable)
8460	1592.146904	10.0.0.20	10.0.0.1	ICMP	123	Destination unreachable (Port unreachable)
8461	1592.147654	10.0.0.20	10.0.0.1	ICMP	123	Destination unreachable (Port unreachable)
8463	1592.151823	10.0.0.20	10.0.0.1	DNS	74	Standard query 0x55e0 A www.google.com
8464	1592.154763	10.0.0.1	10.0.0.20	DNS	90	Standard query response 0x55e0 A www.google.com A 64.233.186.106
8465	1592.154864	10.0.0.1	10.0.0.20	DNS	90	Standard query response 0x55e0 A www.google.com A 64.233.186.99
8466	1592.154921	10.0.0.1	10.0.0.20	DNS	90	Standard query response 0x55e0 A www.google.com A 64.233.186.147
8467	1592.154966	10.0.0.1	10.0.0.20	DNS	90	Standard query response 0x55e0 A www.google.com A 64.233.186.103
8468	1592.155013	10.0.0.1	10.0.0.20	DNS	90	Standard query response 0x55e0 A www.google.com A 64.233.186.105
8469	1592.155179	10.0.0.1	10.0.0.20	DNS	90	Standard query response 0x55e0 A www.google.com A 64.233.186.104

Tráfico HTTP

APK

No se detectó tráfico HTTP durante este periodo.

Otro Tráfico

APK

	Time	Source	Destination	Protocol	Length	Info
1935	9.236969	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
1938	9.266570	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
2500	42.516975	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
2501	42.647746	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
2660	76.052968	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
2661	76.241279	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
3265	105.236995	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
3266	105.313694	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
4533	132.884990	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
4534	132.967460	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
5569	167.956988	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
5570	168.087977	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
6134	200.981008	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
6135	200.983354	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
7815	230.420968	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
7816	230.423503	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
7924	267.796987	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
7925	267.928833	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
7956	294.420974	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
7957	294.553643	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
7997	327.956992	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
7998	328.038990	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
8219	387.031055	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 Who has 10.0.0.1? Tell 10.0.0.20
8220	387.031065	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 10.0.0.1 is at bc:f6:85:21:26:0b
8221	387.092970	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
8222	387.212921	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
8264	431.762292	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 Who has 10.0.0.1? Tell 10.0.0.20
8265	431.762302	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 10.0.0.1 is at bc:f6:85:21:26:0b
8266	432.660979	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
8267	432.797524	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
8277	455.752442	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 Who has 10.0.0.1? Tell 10.0.0.20
8278	455.752452	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 10.0.0.1 is at bc:f6:85:21:26:0b
8281	508.547637	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 Who has 10.0.0.1? Tell 10.0.0.20
8282	508.547647	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 10.0.0.1 is at bc:f6:85:21:26:0b
8359	539.412983	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
8360	539.499812	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
8367	600.781536	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 Who has 10.0.0.1? Tell 10.0.0.20
8368	600.781545	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 10.0.0.1 is at bc:f6:85:21:26:0b
8369	600.852988	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
8370	600.855086	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
8408	679.700989	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
8409	679.788446	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
8414	789.524999	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
8415	789.781834	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
8418	906.361079	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 Who has 10.0.0.1? Tell 10.0.0.20
8419	906.361095	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 10.0.0.1 is at bc:f6:85:21:26:0b
8443	1339.668973	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
8444	1339.872832	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b
8447	1580.308987	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP		42 Who has 10.0.0.20? Tell 10.0.0.1
8448	1580.518225	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP		42 10.0.0.20 is at d0:f8:8c:13:87:7b

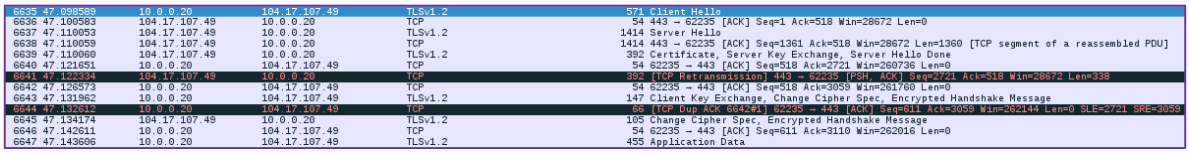
6.4 Tráfico TLS (seguro) entre el terminal de pagos y Banco “BCI”

IPA

437 9.537933	10.0.0.20	104.16.13.14	TLSv1.2	571 Client Hello
438 9.538767	10.0.0.20	104.16.13.14	TCP	54 62191 → 443 [ACK] Seq=1422 Ack=92797 Win=261248 Len=0
439 9.539374	10.0.0.20	64.233.186.97	TCP	66 62198 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0 TSval=373833848 TSecr=2052035774
440 9.539797	104.16.13.14	10.0.0.20	TCP	54 443 → 62197 [ACK] Seq=1 Ack=518 Win=30720 Len=0
441 9.540410	10.0.0.20	64.233.186.97	TLSv1.3	583 Client Hello
442 9.540911	104.16.13.14	10.0.0.20	TLSv1.2	201 Server Hello, Change Cipher Spec, Encrypted Handshake Message

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

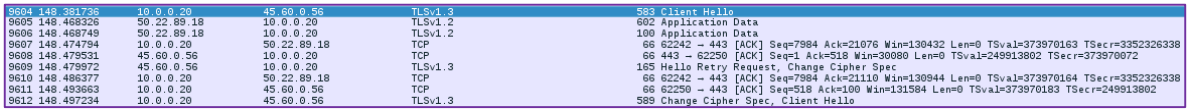
IPA



6635 47.098589	10.0.0.20	104.17.107.49	TLSv1.2	571 Client Hello
6636 47.100583	104.17.107.49	10.0.0.20	TCP	54 443 → 62235 [ACK] Seq=1 Ack=518 Win=28672 Len=0
6637 47.110053	104.17.107.49	10.0.0.20	TLSv1.2	1414 Server Hello
6638 47.110059	104.17.107.49	10.0.0.20	TCP	1414 443 → 62235 [ACK] Seq=1361 Ack=518 Win=28672 Len=1360 [TCP segment of a reassembled PDU]
6639 47.110060	104.17.107.49	10.0.0.20	TLSv1.2	392 Certificate, Server Key Exchange, Server Hello Done
6640 47.121651	10.0.0.20	104.17.107.49	TCP	54 62235 → 443 [ACK] Seq=518 Ack=2721 Win=260736 Len=0
6641 47.122334	104.17.107.49	10.0.0.20	TCP	392 [TCP Retransmission] 443 → 62235 [PSH, ACK] Seq=2721 Ack=518 Win=28672 Len=338
6642 47.126573	10.0.0.20	104.17.107.49	TCP	54 62235 → 443 [ACK] Seq=518 Ack=3059 Win=261760 Len=0
6643 47.131962	10.0.0.20	104.17.107.49	TLSv1.2	147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
6644 47.132412	10.0.0.20	104.17.107.49	TCP	66 [TCP Dup ACK 6642#1] 62235 → 443 [ACK] Seq=611 Ack=3059 Win=262144 Len=0 SLE=2721 SRE=3059
6645 47.134174	104.17.107.49	10.0.0.20	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
6646 47.142611	10.0.0.20	104.17.107.49	TCP	54 62235 → 443 [ACK] Seq=611 Ack=3110 Win=262016 Len=0
6647 47.143606	10.0.0.20	104.17.107.49	TLSv1.2	455 Application Data

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

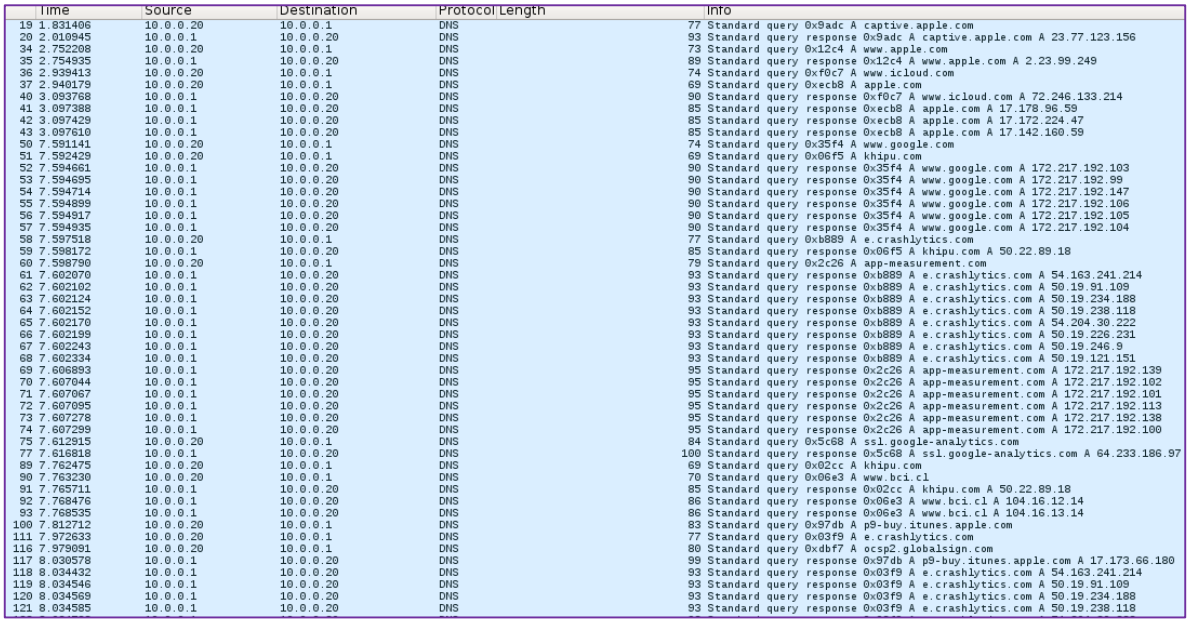
IPA



9604 148.381736	10.0.0.20	45.60.0.56	TLSv1.3	583 Client Hello
9605 148.468326	50.22.89.18	10.0.0.20	TLSv1.2	602 Application Data
9606 148.468749	50.22.89.18	10.0.0.20	TLSv1.2	100 Application Data
9607 148.474794	10.0.0.20	50.22.89.18	TCP	66 62242 → 443 [ACK] Seq=7984 Ack=21076 Win=130432 Len=0 TSval=373970163 TSecr=3352326338
9608 148.479531	45.60.0.56	10.0.0.20	TCP	66 443 → 62250 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=249913802 TSecr=373970072
9609 148.479972	45.60.0.56	10.0.0.20	TLSv1.3	165 Hello Retry Request, Change Cipher Spec
9610 148.486377	10.0.0.20	50.22.89.18	TCP	66 62242 → 443 [ACK] Seq=7984 Ack=21110 Win=130944 Len=0 TSval=373970164 TSecr=3352326338
9611 148.493663	10.0.0.20	45.60.0.56	TCP	66 62250 → 443 [ACK] Seq=518 Ack=100 Win=131584 Len=0 TSval=373970183 TSecr=249913802
9612 148.497234	10.0.0.20	45.60.0.56	TLSv1.3	589 Change Cipher Spec, Client Hello

Tráfico DNS

IPA



	Time	Source	Destination	Protocol	Length	Info
19	1.831406	10.0.0.20	10.0.0.1	DNS	77	Standard query 0x9adc A captive.apple.com
20	2.010945	10.0.0.1	10.0.0.20	DNS	93	Standard query response 0x9adc A captive.apple.com A 23.77.123.156
34	2.752208	10.0.0.20	10.0.0.1	DNS	73	Standard query 0x12c4 A www.apple.com
35	2.754935	10.0.0.1	10.0.0.20	DNS	89	Standard query response 0x12c4 A www.apple.com A 2.23.99.249
36	2.939413	10.0.0.20	10.0.0.1	DNS	74	Standard query 0xf0c7 A www.icloud.com
37	2.940179	10.0.0.20	10.0.0.1	DNS	69	Standard query 0xecb8 A apple.com
40	3.093768	10.0.0.1	10.0.0.20	DNS	90	Standard query response 0xf0c7 A www.icloud.com A 72.246.133.214
41	3.097388	10.0.0.1	10.0.0.20	DNS	85	Standard query response 0xecb8 A apple.com A 17.178.96.59
42	3.097429	10.0.0.1	10.0.0.20	DNS	85	Standard query response 0xecb8 A apple.com A 17.172.224.47
43	3.097610	10.0.0.1	10.0.0.20	DNS	85	Standard query response 0xecb8 A apple.com A 17.142.160.59
50	7.591141	10.0.0.20	10.0.0.1	DNS	74	Standard query 0x35f4 A www.google.com
51	7.592429	10.0.0.20	10.0.0.1	DNS	69	Standard query 0x06f5 A khipu.com
52	7.594661	10.0.0.1	10.0.0.20	DNS	90	Standard query response 0x35f4 A www.google.com A 172.217.192.103
53	7.594695	10.0.0.1	10.0.0.20	DNS	90	Standard query response 0x35f4 A www.google.com A 172.217.192.99
54	7.594714	10.0.0.1	10.0.0.20	DNS	90	Standard query response 0x35f4 A www.google.com A 172.217.192.147
55	7.594899	10.0.0.1	10.0.0.20	DNS	90	Standard query response 0x35f4 A www.google.com A 172.217.192.106
56	7.594917	10.0.0.1	10.0.0.20	DNS	90	Standard query response 0x35f4 A www.google.com A 172.217.192.105
57	7.594935	10.0.0.1	10.0.0.20	DNS	90	Standard query response 0x35f4 A www.google.com A 172.217.192.104
58	7.597518	10.0.0.20	10.0.0.1	DNS	77	Standard query 0xb889 A e.crashlytics.com
59	7.598172	10.0.0.1	10.0.0.20	DNS	85	Standard query response 0x06f5 A khipu.com A 50.22.89.18
60	7.598790	10.0.0.20	10.0.0.1	DNS	79	Standard query 0x2c26 A app-measurement.com
61	7.602070	10.0.0.1	10.0.0.20	DNS	93	Standard query response 0xb889 A e.crashlytics.com A 54.163.241.214
62	7.602102	10.0.0.1	10.0.0.20	DNS	93	Standard query response 0xb889 A e.crashlytics.com A 50.19.91.109
63	7.602124	10.0.0.1	10.0.0.20	DNS	93	Standard query response 0xb889 A e.crashlytics.com A 50.19.234.188
64	7.602152	10.0.0.1	10.0.0.20	DNS	93	Standard query response 0xb889 A e.crashlytics.com A 50.19.238.118
65	7.602170	10.0.0.1	10.0.0.20	DNS	93	Standard query response 0xb889 A e.crashlytics.com A 54.204.30.222
66	7.602199	10.0.0.1	10.0.0.20	DNS	93	Standard query response 0xb889 A e.crashlytics.com A 50.19.226.231
67	7.602243	10.0.0.1	10.0.0.20	DNS	93	Standard query response 0xb889 A e.crashlytics.com A 50.19.246.9
68	7.602334	10.0.0.1	10.0.0.20	DNS	93	Standard query response 0xb889 A e.crashlytics.com A 50.19.121.151
69	7.606893	10.0.0.1	10.0.0.20	DNS	95	Standard query response 0x2c26 A app-measurement.com A 172.217.192.139
70	7.607044	10.0.0.1	10.0.0.20	DNS	95	Standard query response 0x2c26 A app-measurement.com A 172.217.192.102
71	7.607067	10.0.0.1	10.0.0.20	DNS	95	Standard query response 0x2c26 A app-measurement.com A 172.217.192.101
72	7.607095	10.0.0.1	10.0.0.20	DNS	95	Standard query response 0x2c26 A app-measurement.com A 172.217.192.113
73	7.607278	10.0.0.1	10.0.0.20	DNS	95	Standard query response 0x2c26 A app-measurement.com A 172.217.192.138
74	7.607299	10.0.0.1	10.0.0.20	DNS	95	Standard query response 0x2c26 A app-measurement.com A 172.217.192.100
75	7.612915	10.0.0.20	10.0.0.1	DNS	84	Standard query 0x5c68 A ssl.google-analytics.com
77	7.616818	10.0.0.1	10.0.0.20	DNS	100	Standard query response 0x5c68 A ssl.google-analytics.com A 64.233.186.97
89	7.762475	10.0.0.20	10.0.0.1	DNS	69	Standard query 0x02cc A khipu.com
90	7.763230	10.0.0.20	10.0.0.1	DNS	70	Standard query 0x06e3 A www.bci.cl
91	7.765711	10.0.0.1	10.0.0.20	DNS	85	Standard query response 0x02cc A khipu.com A 50.22.89.18
92	7.768476	10.0.0.1	10.0.0.20	DNS	86	Standard query response 0x06e3 A www.bci.cl A 104.16.12.14
93	7.768535	10.0.0.1	10.0.0.20	DNS	86	Standard query response 0x06e3 A www.bci.cl A 104.16.13.14
100	7.812712	10.0.0.20	10.0.0.1	DNS	83	Standard query 0x97db A p9-buy.itunes.apple.com
111	7.972633	10.0.0.20	10.0.0.1	DNS	77	Standard query 0x03f9 A e.crashlytics.com
116	7.979091	10.0.0.20	10.0.0.1	DNS	80	Standard query 0xdbf7 A ocsp2.globalsign.com
117	8.030578	10.0.0.1	10.0.0.20	DNS	99	Standard query response 0x97db A p9-buy.itunes.apple.com A 17.173.66.180
118	8.034432	10.0.0.1	10.0.0.20	DNS	93	Standard query response 0x03f9 A e.crashlytics.com A 54.163.241.214
119	8.034546	10.0.0.1	10.0.0.20	DNS	93	Standard query response 0x03f9 A e.crashlytics.com A 50.19.91.109
120	8.034569	10.0.0.1	10.0.0.20	DNS	93	Standard query response 0x03f9 A e.crashlytics.com A 50.19.234.188
121	8.034585	10.0.0.1	10.0.0.20	DNS	93	Standard query response 0x03f9 A e.crashlytics.com A 50.19.238.118

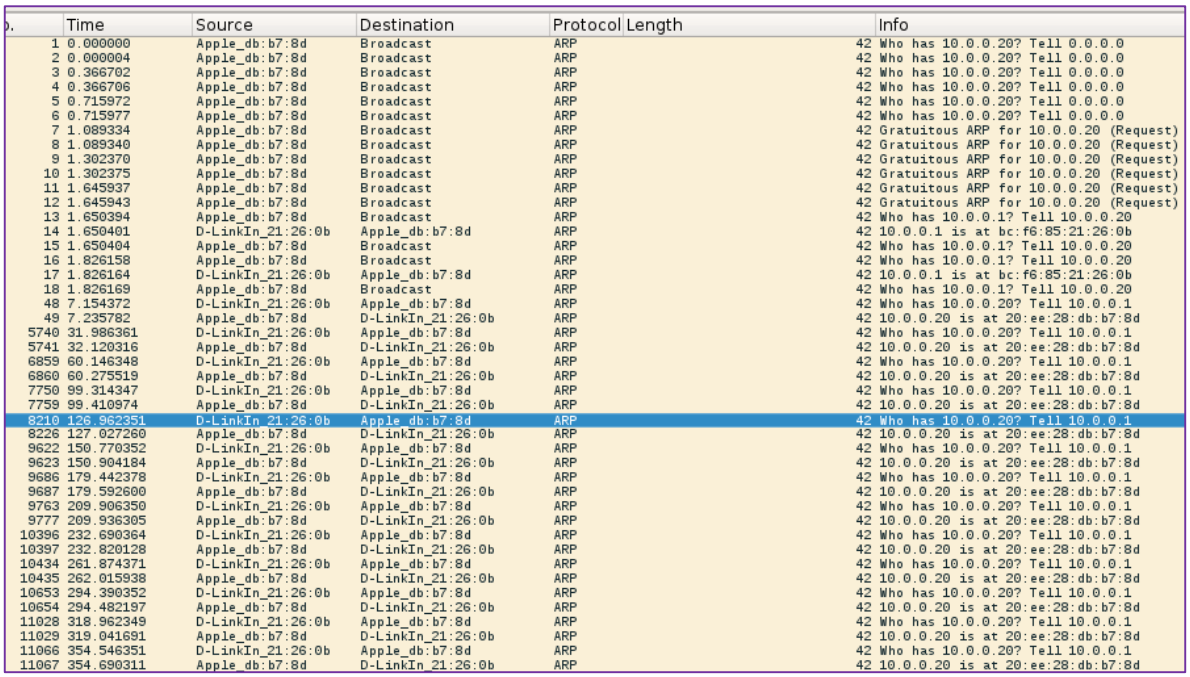
Tráfico HTTP

IPA

No se detectó tráfico HTTP durante este período.

Otro Tráfico

IPA



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Apple_db:b7:8d	Broadcast	ARP	42	Who has 10.0.0.20? Tell 0.0.0.0
2	0.000004	Apple_db:b7:8d	Broadcast	ARP	42	Who has 10.0.0.20? Tell 0.0.0.0
3	0.366702	Apple_db:b7:8d	Broadcast	ARP	42	Who has 10.0.0.20? Tell 0.0.0.0
4	0.366706	Apple_db:b7:8d	Broadcast	ARP	42	Who has 10.0.0.20? Tell 0.0.0.0
5	0.715972	Apple_db:b7:8d	Broadcast	ARP	42	Who has 10.0.0.20? Tell 0.0.0.0
6	0.715977	Apple_db:b7:8d	Broadcast	ARP	42	Who has 10.0.0.20? Tell 0.0.0.0
7	1.089334	Apple_db:b7:8d	Broadcast	ARP	42	Gratuitous ARP for 10.0.0.20 (Request)
8	1.089340	Apple_db:b7:8d	Broadcast	ARP	42	Gratuitous ARP for 10.0.0.20 (Request)
9	1.302370	Apple_db:b7:8d	Broadcast	ARP	42	Gratuitous ARP for 10.0.0.20 (Request)
10	1.302375	Apple_db:b7:8d	Broadcast	ARP	42	Gratuitous ARP for 10.0.0.20 (Request)
11	1.645937	Apple_db:b7:8d	Broadcast	ARP	42	Gratuitous ARP for 10.0.0.20 (Request)
12	1.645943	Apple_db:b7:8d	Broadcast	ARP	42	Gratuitous ARP for 10.0.0.20 (Request)
13	1.650394	Apple_db:b7:8d	Broadcast	ARP	42	Who has 10.0.0.1? Tell 10.0.0.20
14	1.650401	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	10.0.0.1 is at bc:f6:85:21:26:0b
15	1.650404	Apple_db:b7:8d	Broadcast	ARP	42	Who has 10.0.0.1? Tell 10.0.0.20
16	1.826158	Apple_db:b7:8d	Broadcast	ARP	42	Who has 10.0.0.1? Tell 10.0.0.20
17	1.826164	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	10.0.0.1 is at bc:f6:85:21:26:0b
18	1.826169	Apple_db:b7:8d	Broadcast	ARP	42	Who has 10.0.0.1? Tell 10.0.0.20
48	7.154372	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
49	7.235782	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at 20:ee:28:db:b7:8d
5740	31.986361	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
5741	32.120316	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at 20:ee:28:db:b7:8d
6859	60.146348	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
6860	60.275519	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at 20:ee:28:db:b7:8d
7750	99.314347	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
7759	99.410974	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at 20:ee:28:db:b7:8d
8210	126.962351	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
8226	127.027260	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at 20:ee:28:db:b7:8d
9622	150.770352	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
9623	150.904184	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at 20:ee:28:db:b7:8d
9686	179.442378	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
9687	179.592600	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at 20:ee:28:db:b7:8d
9763	209.906350	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
9777	209.936305	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at 20:ee:28:db:b7:8d
10396	232.690364	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
10397	232.820128	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at 20:ee:28:db:b7:8d
10434	261.874371	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
10435	262.015938	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at 20:ee:28:db:b7:8d
10653	294.390352	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
10654	294.482197	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at 20:ee:28:db:b7:8d
11028	318.962349	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
11029	319.041691	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at 20:ee:28:db:b7:8d
11066	354.546351	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
11067	354.690311	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at 20:ee:28:db:b7:8d

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
10.0.0. 20	104.16.13.14	TLSv1.2	Banco BCI
10.0.0. 20	104.17.07.49	TLSv1.2	Banco Estado
10.0.0. 20	45.60.0.56	TLSv1.3	Banco Chile

7.2 IPA

Origen	Destino	Tipo de Tráfico	Descripción
192.168.1.56	50.22.89.18	TLSv1.2	khipu
10.0.0. 21	104.16.13.14	TLSv1.2	Banco BCI
10.0.0. 21	104.17.07.49	TLSv1.2	Banco Estado
10.0.0. 21	45.60.0.56	TLSv1.3	Banco Chile

8 Análisis SSL

El siguiente análisis tiene como objetivo determinar el nivel de seguridad en la implementación de SSL/TLS, se ejecutaron 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
Ticketbleed	(CVE-2016-9244)	✓	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	✗	Potencialmente Vulnerable
LUCKY13	CVE-2013-0169	✗	Potencialmente Vulnerable
RC4	CVE-2013-2566 CVE-2015-2808	✓	No vulnerable

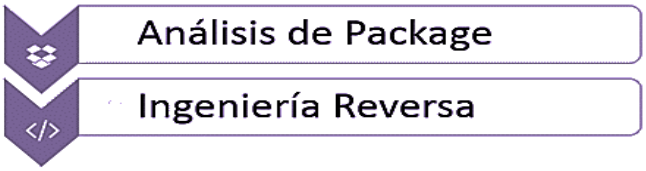
Se detectaron 2 vulnerabilidades en la implementación de SSL/TLS del sitio khipu.com las que afectan la confidencialidad de la información, sin embargo, estas vulnerabilidades tienen un alto grado de dificultad de explotación y se requieren condiciones especiales para su concreción.

9 Referencias

Nombre	Link de referencia
Heartbleed	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
Ticketbleed	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9244
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/cvenamcgi?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 descompiladas 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.apk
SHA256	61e3a5d9ead9eb38121636e0945e0edd3a3ed79b9708b349827549b2560f7806
Tamaño	8.13 MB
Tipo	.apk
URLs de interés	0
IPs encontradas	0
Emails encontrados	0

URLs detectadas

1. https://Khipu.com/
2. https://Khipu.com/app/2.0/

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	khipu7.1.ipa
SHA256	6c4deb1d10608c7b53260f5d3187f7a59aa4cac98493acd58d8bbaaf93ad82f2
Tamaño	16.12 MB
Tipo	.ipa
URLs de interés	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 realizó un análisis utilizando distintos motores de antivirus, lo cual permite la detección de virus, gusanos, troyanos y todo tipo de malware que contengan los archivos *.ipa (iOS) y el archivo *.apk (Android). En esta ocasión ambos fueron analizados debido a cambios 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)**	✓

IPA		APK	
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	✓

IPA		APK	
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	✓

IPA		APK	
Rising	✓	Rising	✓
Sophos AV	✓	Sophos AV	✓
SUPERAntiSpywar e	✓	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	✓

IPA		APK	
		Yandex	✓
		Zillya	✓
		ZoneAlarm by Check Point	✓
		Zoner	✓

14 Vulnerabilidades declaradas

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

En este período 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. Si bien 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 utilizan 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 correspondiente al tráfico de datos de cada aplicación

#	Archivo	SHA256SUM
1	APK20190611.pcap	8621436b1910921bb2d40f91bab54c5f520b263e15a7bdb8dc5b024fc7fd120e
2	IOS20190611pcap	91dd68d21df1110d966c5c8b53e4ab8cef79fe9bde80a4d987c1e753be470a86