Dirigido a:
Eduardo Parraguez
khipu

NOVIEMBRE
2019

INFORME TÉCNICO

Análisis de Tráfico de Datos noviembre 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
26-12-2019	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 u contraseñas a sus servidores o a terceros.

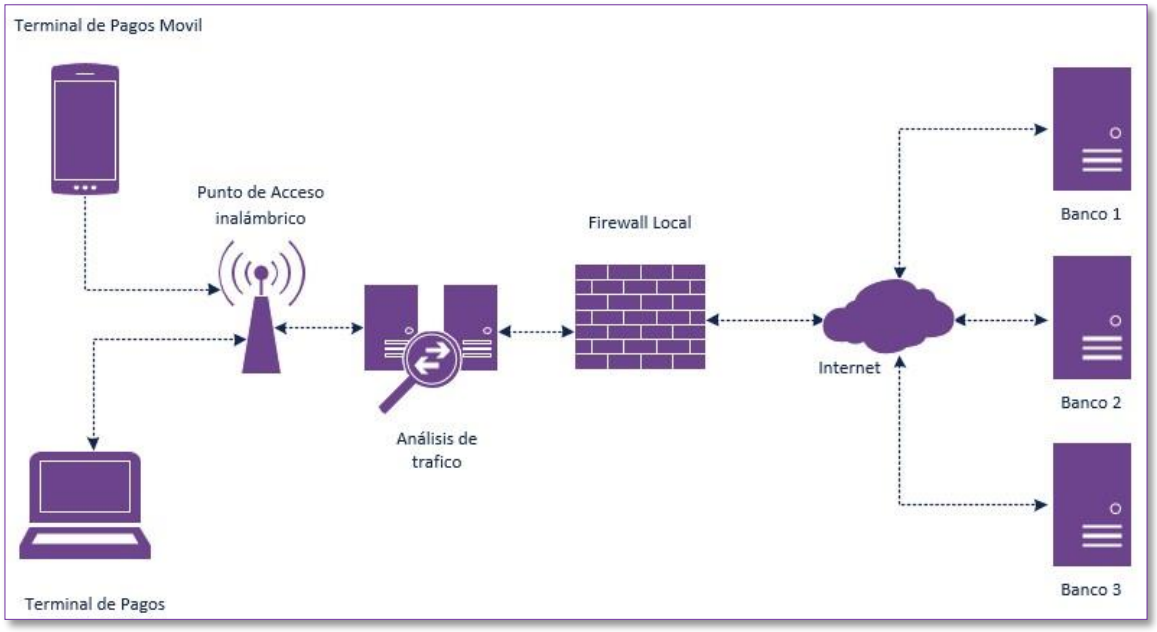
El presente análisis consiste en el monitoreo y análisis de todo el tráfico que genera la aplicación para las distintas plataformas, con el fin de detectar conexiones sospechosas. La revisión incluye la versión del terminal de pagos disponible para IOS y Android.

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 se registraron cambios para las aplicaciones de **iOS y Android** tanto en su versión como en su HASH.

Plataforma	Versión	SHA256SUM
Android	**7.5.2 - Ultima actualización 10/12/2019**	
iOS	**7.1.5 - Ultima actualización 05/12/2019**	**6ea87c85620c60a7f8675be6fc0fac47bd142ed84bcb6de83ca16d5b27d98a91**

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.

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

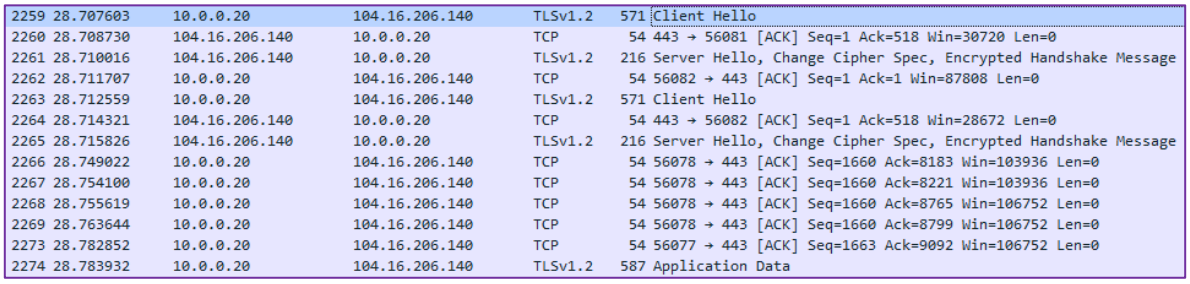
Origen	Destino	Tipo de Tráfico	Descripción
10.0.0.20	52.116.25.250	TLSv1.2	khipu
10.0.0.20	104.16.206.140	TLSv1.2	Banco BCI
10.0.0.20	200.11.88.142	TLSv1.2	Banco ITAU
10.0.0.20	169.63.198.82	TLSv1.2	Banco Estado

7.2 IPA

Origen	Destino	Tipo de Tráfico	Descripción
10.0.0.21	52.116.25.250	TLSv1.2	khipu
10.0.0.21	104.16.206.140	TLSv1.2	Banco BCI
10.0.0.21	200.54.67.183	TLSv1.2	Banco ITAU
10.0.0.21	52.116.25.250	TLSv1.2	Banco Estado

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

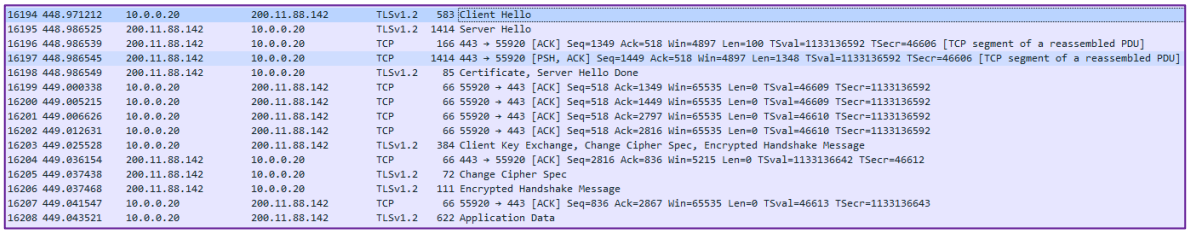
APK



2259	28.707603	10.0.0.20	104.16.206.140	TLSv1.2	571 Client Hello
2260	28.708730	104.16.206.140	10.0.0.20	TCP	54 443 → 56081 [ACK] Seq=1 Ack=518 Win=30720 Len=0
2261	28.710016	104.16.206.140	10.0.0.20	TLSv1.2	216 Server Hello, Change Cipher Spec, Encrypted Handshake Message
2262	28.711707	10.0.0.20	104.16.206.140	TCP	54 56082 → 443 [ACK] Seq=1 Ack=1 Win=87808 Len=0
2263	28.712559	10.0.0.20	104.16.206.140	TLSv1.2	571 Client Hello
2264	28.714321	104.16.206.140	10.0.0.20	TCP	54 443 → 56082 [ACK] Seq=1 Ack=518 Win=28672 Len=0
2265	28.715826	104.16.206.140	10.0.0.20	TLSv1.2	216 Server Hello, Change Cipher Spec, Encrypted Handshake Message
2266	28.749022	10.0.0.20	104.16.206.140	TCP	54 56078 → 443 [ACK] Seq=1660 Ack=8183 Win=103936 Len=0
2267	28.754100	10.0.0.20	104.16.206.140	TCP	54 56078 → 443 [ACK] Seq=1660 Ack=8221 Win=103936 Len=0
2268	28.755619	10.0.0.20	104.16.206.140	TCP	54 56078 → 443 [ACK] Seq=1660 Ack=8765 Win=106752 Len=0
2269	28.763644	10.0.0.20	104.16.206.140	TCP	54 56078 → 443 [ACK] Seq=1660 Ack=8799 Win=106752 Len=0
2273	28.782852	10.0.0.20	104.16.206.140	TCP	54 56077 → 443 [ACK] Seq=1663 Ack=9092 Win=106752 Len=0
2274	28.783932	10.0.0.20	104.16.206.140	TLSv1.2	587 Application Data

7.4 Tráfico TLS (seguro) entre el terminal de pagos y Banco “ITAU”

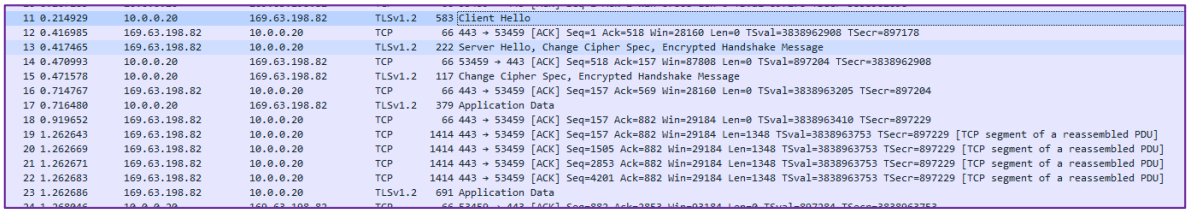
APK



16194	448.971212	10.0.0.20	200.11.88.142	TLSv1.2	583 Client Hello
16195	448.986525	200.11.88.142	10.0.0.20	TLSv1.2	1414 Server Hello
16196	448.986539	200.11.88.142	10.0.0.20	TCP	166 443 → 55920 [ACK] Seq=1349 Ack=518 Win=4897 Len=100 TSval=1133136592 TSecr=46606 [TCP segment of a reassembled PDU]
16197	448.986545	200.11.88.142	10.0.0.20	TCP	1414 443 → 55920 [PSH, ACK] Seq=1449 Ack=518 Win=4897 Len=1348 TSval=1133136592 TSecr=46606 [TCP segment of a reassembled PDU]
16198	448.986549	200.11.88.142	10.0.0.20	TLSv1.2	85 Certificate, Server Hello Done
16199	449.000338	10.0.0.20	200.11.88.142	TCP	66 55920 → 443 [ACK] Seq=518 Ack=1349 Win=65535 Len=0 TSval=46609 TSecr=1133136592
16200	449.005215	10.0.0.20	200.11.88.142	TCP	66 55920 → 443 [ACK] Seq=518 Ack=1449 Win=65535 Len=0 TSval=46609 TSecr=1133136592
16201	449.006626	10.0.0.20	200.11.88.142	TCP	66 55920 → 443 [ACK] Seq=518 Ack=2797 Win=65535 Len=0 TSval=46610 TSecr=1133136592
16202	449.012631	10.0.0.20	200.11.88.142	TCP	66 55920 → 443 [ACK] Seq=518 Ack=2816 Win=65535 Len=0 TSval=46610 TSecr=1133136592
16203	449.025528	10.0.0.20	200.11.88.142	TLSv1.2	384 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
16204	449.036154	200.11.88.142	10.0.0.20	TCP	66 443 → 55920 [ACK] Seq=2816 Ack=836 Win=5215 Len=0 TSval=1133136642 TSecr=46612
16205	449.037438	200.11.88.142	10.0.0.20	TLSv1.2	72 Change Cipher Spec
16206	449.037468	200.11.88.142	10.0.0.20	TLSv1.2	111 Encrypted Handshake Message
16207	449.041547	10.0.0.20	200.11.88.142	TCP	66 55920 → 443 [ACK] Seq=836 Ack=2867 Win=65535 Len=0 TSval=46613 TSecr=1133136643
16208	449.043521	10.0.0.20	200.11.88.142	TLSv1.2	622 Application Data

7.5 Tráfico TLS (seguro) entre el terminal de pagos y Banco “ESTADO”

APK



11	0.214929	10.0.0.20	169.63.198.82	TLSv1.2	583 Client Hello
12	0.416985	169.63.198.82	10.0.0.20	TCP	66 443 → 53459 [ACK] Seq=1 Ack=518 Win=28160 Len=0 TSval=3838962908 TSecr=897178
13	0.417465	169.63.198.82	10.0.0.20	TLSv1.2	222 Server Hello, Change Cipher Spec, Encrypted Handshake Message
14	0.470993	10.0.0.20	169.63.198.82	TCP	66 53459 → 443 [ACK] Seq=518 Ack=157 Win=87808 Len=0 TSval=897204 TSecr=3838962908
15	0.471578	10.0.0.20	169.63.198.82	TLSv1.2	117 Change Cipher Spec, Encrypted Handshake Message
16	0.714767	169.63.198.82	10.0.0.20	TCP	66 443 → 53459 [ACK] Seq=157 Ack=569 Win=28160 Len=0 TSval=3838963205 TSecr=897204
17	0.716480	10.0.0.20	169.63.198.82	TLSv1.2	379 Application Data
18	0.919652	169.63.198.82	10.0.0.20	TCP	66 443 → 53459 [ACK] Seq=157 Ack=882 Win=29184 Len=0 TSval=3838963410 TSecr=897229
19	1.262643	169.63.198.82	10.0.0.20	TCP	1414 443 → 53459 [ACK] Seq=157 Ack=882 Win=29184 Len=1348 TSval=3838963753 TSecr=897229 [TCP segment of a reassembled PDU]
20	1.262669	169.63.198.82	10.0.0.20	TCP	1414 443 → 53459 [ACK] Seq=1505 Ack=882 Win=29184 Len=1348 TSval=3838963753 TSecr=897229 [TCP segment of a reassembled PDU]
21	1.262671	169.63.198.82	10.0.0.20	TCP	1414 443 → 53459 [ACK] Seq=2853 Ack=882 Win=29184 Len=1348 TSval=3838963753 TSecr=897229 [TCP segment of a reassembled PDU]
22	1.262683	169.63.198.82	10.0.0.20	TCP	1414 443 → 53459 [ACK] Seq=4201 Ack=882 Win=29184 Len=1348 TSval=3838963753 TSecr=897229 [TCP segment of a reassembled PDU]
23	1.262686	169.63.198.82	10.0.0.20	TLSv1.2	691 Application Data

Tráfico DNS

APK

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.20	10.0.0.1	DNS	78	Standard query 0x7c1b A graph.facebook.com
2	0.045312	10.0.0.20	10.0.0.1	DNS	84	Standard query 0x1ccb A settings.crashlytics.com
3	0.125519	10.0.0.1	10.0.0.20	DNS	94	Standard query response 0x7c1b A graph.facebook.com A 157.240.204.17
4	0.129325	10.0.0.1	10.0.0.20	DNS	100	Standard query response 0x1ccb A settings.crashlytics.com A 64.233.186.94
77	0.974652	10.0.0.20	10.0.0.1	DNS	69	Standard query 0x79d3 A khipu.com
78	0.978794	10.0.0.1	10.0.0.20	DNS	85	Standard query response 0x79d3 A khipu.com A 169.63.198.82
79	0.978835	10.0.0.1	10.0.0.20	DNS	85	Standard query response 0x79d3 A khipu.com A 169.47.100.12
80	0.980391	10.0.0.1	10.0.0.20	DNS	85	Standard query response 0x79d3 A khipu.com A 52.116.25.250
81	0.980819	10.0.0.20	10.0.0.1	ICMP	113	Destination unreachable (Port unreachable)
82	0.983909	10.0.0.20	10.0.0.1	ICMP	113	Destination unreachable (Port unreachable)
93	1.198629	10.0.0.20	10.0.0.1	DNS	108	Standard query 0x13a5 A us-central1-appversions-911ee.cloudfunctions.net
94	1.204425	10.0.0.1	10.0.0.20	DNS	124	Standard query response 0x13a5 A us-central1-appversions-911ee.cloudfunctions.net A 172.217.192.102
95	1.204466	10.0.0.1	10.0.0.20	DNS	124	Standard query response 0x13a5 A us-central1-appversions-911ee.cloudfunctions.net A 172.217.192.139
96	1.204484	10.0.0.1	10.0.0.20	DNS	124	Standard query response 0x13a5 A us-central1-appversions-911ee.cloudfunctions.net A 172.217.192.138
97	1.204499	10.0.0.1	10.0.0.20	DNS	124	Standard query response 0x13a5 A us-central1-appversions-911ee.cloudfunctions.net A 172.217.192.100
98	1.204514	10.0.0.1	10.0.0.20	DNS	124	Standard query response 0x13a5 A us-central1-appversions-911ee.cloudfunctions.net A 172.217.192.113
99	1.204530	10.0.0.1	10.0.0.20	DNS	124	Standard query response 0x13a5 A us-central1-appversions-911ee.cloudfunctions.net A 172.217.192.101
100	1.208085	10.0.0.20	10.0.0.1	ICMP	152	Destination unreachable (Port unreachable)
101	1.209355	10.0.0.20	10.0.0.1	ICMP	152	Destination unreachable (Port unreachable)
103	1.211708	10.0.0.20	10.0.0.1	ICMP	152	Destination unreachable (Port unreachable)
104	1.212375	10.0.0.20	10.0.0.1	ICMP	152	Destination unreachable (Port unreachable)
1059	26.551242	10.0.0.20	10.0.0.1	DNS	70	Standard query 0x2791 A www.bci.cl
1060	26.555617	10.0.0.1	10.0.0.20	DNS	86	Standard query response 0x2791 A www.bci.cl A 104.16.12.14
1061	26.555658	10.0.0.1	10.0.0.20	DNS	86	Standard query response 0x2791 A www.bci.cl A 104.16.13.14
1062	26.557951	10.0.0.20	10.0.0.1	ICMP	114	Destination unreachable (Port unreachable)
1254	27.113496	10.0.0.20	10.0.0.1	DNS	76	Standard query 0x57e8 A bci.modyocdn.com
1255	27.118101	10.0.0.1	10.0.0.20	DNS	92	Standard query response 0x57e8 A bci.modyocdn.com A 104.16.206.140
1256	27.118866	10.0.0.1	10.0.0.20	DNS	92	Standard query response 0x57e8 A bci.modyocdn.com A 104.16.204.140
1257	27.118902	10.0.0.1	10.0.0.20	DNS	92	Standard query response 0x57e8 A bci.modyocdn.com A 104.16.205.140
1258	27.118958	10.0.0.1	10.0.0.20	DNS	92	Standard query response 0x57e8 A bci.modyocdn.com A 104.16.207.140
1259	27.118976	10.0.0.1	10.0.0.20	DNS	92	Standard query response 0x57e8 A bci.modyocdn.com A 104.16.208.140
1260	27.122422	10.0.0.20	10.0.0.1	ICMP	120	Destination unreachable (Port unreachable)
1269	27.124104	10.0.0.20	10.0.0.1	ICMP	120	Destination unreachable (Port unreachable)
1275	27.131530	10.0.0.20	10.0.0.1	ICMP	120	Destination unreachable (Port unreachable)
1276	27.134149	10.0.0.20	10.0.0.1	ICMP	120	Destination unreachable (Port unreachable)
1852	28.129800	10.0.0.20	10.0.0.1	DNS	80	Standard query 0x21a6 A cdnjs.cloudflare.com
1855	28.133112	10.0.0.1	10.0.0.20	DNS	96	Standard query response 0x21a6 A cdnjs.cloudflare.com A 104.17.65.4
1856	28.133147	10.0.0.1	10.0.0.20	DNS	96	Standard query response 0x21a6 A cdnjs.cloudflare.com A 104.17.64.4
2216	28.623959	10.0.0.20	10.0.0.1	ICMP	124	Destination unreachable (Port unreachable)
3453	30.623240	10.0.0.20	10.0.0.1	DNS	91	Standard query 0x31fa A wup-297715e5.us.v2.we-stats.com
3454	30.632009	10.0.0.1	10.0.0.20	DNS	107	Standard query response 0x31fa A wup-297715e5.us.v2.we-stats.com A 104.43.210.166
3688	33.096187	10.0.0.20	10.0.0.1	DNS	91	Standard query 0x6434 A log-297715e5.us.v2.we-stats.com
3689	33.100646	10.0.0.1	10.0.0.20	DNS	107	Standard query response 0x6434 A log-297715e5.us.v2.we-stats.com A 52.238.253.184
6175	121.067870	10.0.0.20	10.0.0.1	DNS	77	Standard query 0xf661 A e.crashlytics.com

Tráfico HTTP

APK

No se detectó tráfico HTTP durante el periodo de noviembre.

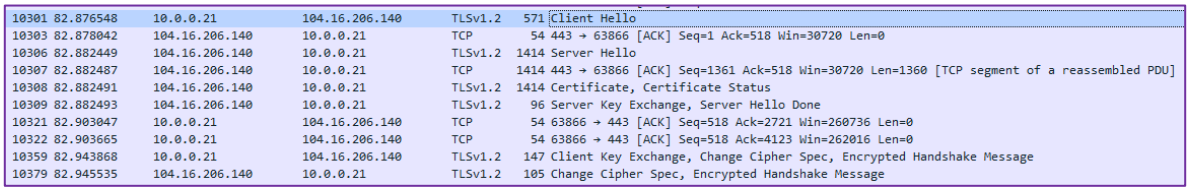
Otro Tráfico

APK

	Time	Source	Destination	Protocol	Length	Info
219	5.297007	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
220	5.458771	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at d0:f8:8c:13:87:7b
4005	34.225008	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
4239	34.758653	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at d0:f8:8c:13:87:7b
5748	60.853003	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
5749	60.858945	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at d0:f8:8c:13:87:7b
6041	87.729005	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
6042	87.888848	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at d0:f8:8c:13:87:7b
6150	115.377005	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
6151	115.539924	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at d0:f8:8c:13:87:7b
7066	141.489004	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
7067	141.491407	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at d0:f8:8c:13:87:7b
8088	158.653187	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8089	158.653198	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8092	159.631902	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8093	159.631914	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8123	160.631987	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8124	160.631998	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8180	162.014702	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8181	162.014711	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8182	163.032053	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8183	163.032064	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8187	164.031822	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8188	164.031850	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8209	165.185241	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8210	165.185270	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8211	166.200823	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8212	166.200834	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8216	167.202020	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8217	167.202031	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8526	176.625547	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8527	176.625573	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8528	177.620739	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8529	177.620753	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8533	178.617913	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
8534	178.617926	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
11897	205.191685	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
11898	205.191696	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
11906	206.201055	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
11907	206.201070	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
11912	207.200703	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
11913	207.200732	Motorola_13:87:7b	Broadcast	ARP	42	Who has 10.162.0.1? Tell 10.0.0.20
11984	245.685018	D-LinkIn_21:26:0b	Motorola_13:87:7b	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
11985	245.793776	Motorola_13:87:7b	D-LinkIn_21:26:0b	ARP	42	10.0.0.20 is at d0:f8:8c:13:87:7b

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

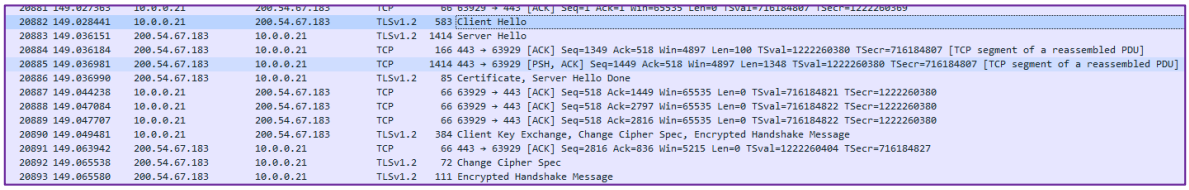
IPA



10301	82.876548	10.0.0.21	104.16.206.140	TLSv1.2	571 Client Hello
10303	82.878042	104.16.206.140	10.0.0.21	TCP	54 443 → 63866 [ACK] Seq=1 Ack=518 Win=30720 Len=0
10306	82.882449	104.16.206.140	10.0.0.21	TLSv1.2	1414 Server Hello
10307	82.882487	104.16.206.140	10.0.0.21	TCP	1414 443 → 63866 [ACK] Seq=1361 Ack=518 Win=30720 Len=1360 [TCP segment of a reassembled PDU]
10308	82.882491	104.16.206.140	10.0.0.21	TLSv1.2	1414 Certificate, Certificate Status
10309	82.882493	104.16.206.140	10.0.0.21	TLSv1.2	96 Server Key Exchange, Server Hello Done
10321	82.903047	10.0.0.21	104.16.206.140	TCP	54 63866 → 443 [ACK] Seq=518 Ack=2721 Win=260736 Len=0
10322	82.903665	10.0.0.21	104.16.206.140	TCP	54 63866 → 443 [ACK] Seq=518 Ack=4123 Win=262016 Len=0
10359	82.943868	10.0.0.21	104.16.206.140	TLSv1.2	147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10379	82.945535	104.16.206.140	10.0.0.21	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message

7.7 Tráfico TLS (seguro) entre el terminal de pagos y Banco “ITAU”

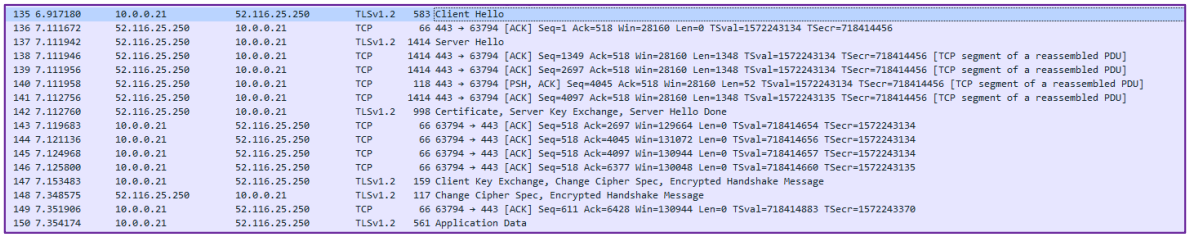
IPA



20881	149.027363	10.0.0.21	200.54.67.183	TCP	66 63929 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0 TSval=716184807 TSecr=1222260369
20882	149.028441	10.0.0.21	200.54.67.183	TLSv1.2	583 Client Hello
20883	149.036151	200.54.67.183	10.0.0.21	TLSv1.2	1414 Server Hello
20884	149.036184	200.54.67.183	10.0.0.21	TCP	166 443 → 63929 [ACK] Seq=1349 Ack=518 Win=4897 Len=100 TSval=1222260380 TSecr=716184807 [TCP segment of a reassembled PDU]
20885	149.036981	200.54.67.183	10.0.0.21	TCP	1414 443 → 63929 [PSH, ACK] Seq=1449 Ack=518 Win=4897 Len=1348 TSval=1222260380 TSecr=716184807 [TCP segment of a reassembled PDU]
20886	149.036990	200.54.67.183	10.0.0.21	TLSv1.2	85 Certificate, Server Hello Done
20887	149.044238	10.0.0.21	200.54.67.183	TCP	66 63929 → 443 [ACK] Seq=518 Ack=1449 Win=65535 Len=0 TSval=716184821 TSecr=1222260380
20888	149.047084	10.0.0.21	200.54.67.183	TCP	66 63929 → 443 [ACK] Seq=518 Ack=2797 Win=65535 Len=0 TSval=716184822 TSecr=1222260380
20889	149.047707	10.0.0.21	200.54.67.183	TCP	66 63929 → 443 [ACK] Seq=518 Ack=2816 Win=65535 Len=0 TSval=716184822 TSecr=1222260380
20890	149.049481	10.0.0.21	200.54.67.183	TLSv1.2	384 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
20891	149.063942	200.54.67.183	10.0.0.21	TCP	66 443 → 63929 [ACK] Seq=2816 Ack=836 Win=5215 Len=0 TSval=1222260404 TSecr=716184827
20892	149.065538	200.54.67.183	10.0.0.21	TLSv1.2	72 Change Cipher Spec
20893	149.065580	200.54.67.183	10.0.0.21	TLSv1.2	111 Encrypted Handshake Message

7.8 Tráfico TLS (seguro) entre el terminal de pagos y Banco “ESTADO”

IPA



135	6.917180	10.0.0.21	52.116.25.250	TLSv1.2	583 Client Hello
136	7.111672	52.116.25.250	10.0.0.21	TCP	66 443 → 63794 [ACK] Seq=1 Ack=518 Win=28160 Len=0 TSval=1572243134 TSecr=718414456
137	7.111942	52.116.25.250	10.0.0.21	TLSv1.2	1414 Server Hello
138	7.111946	52.116.25.250	10.0.0.21	TCP	1414 443 → 63794 [ACK] Seq=1349 Ack=518 Win=28160 Len=1348 TSval=1572243134 TSecr=718414456 [TCP segment of a reassembled PDU]
139	7.111956	52.116.25.250	10.0.0.21	TCP	1414 443 → 63794 [ACK] Seq=2697 Ack=518 Win=28160 Len=1348 TSval=1572243134 TSecr=718414456 [TCP segment of a reassembled PDU]
140	7.111958	52.116.25.250	10.0.0.21	TCP	118 443 → 63794 [PSH, ACK] Seq=4045 Ack=518 Win=28160 Len=52 TSval=1572243134 TSecr=718414456 [TCP segment of a reassembled PDU]
141	7.112756	52.116.25.250	10.0.0.21	TCP	1414 443 → 63794 [ACK] Seq=4097 Ack=518 Win=28160 Len=1348 TSval=1572243135 TSecr=718414456 [TCP segment of a reassembled PDU]
142	7.112760	52.116.25.250	10.0.0.21	TLSv1.2	998 Certificate, Server Key Exchange, Server Hello Done
143	7.119683	10.0.0.21	52.116.25.250	TCP	66 63794 → 443 [ACK] Seq=518 Ack=2697 Win=129664 Len=0 TSval=718414654 TSecr=1572243134
144	7.121136	10.0.0.21	52.116.25.250	TCP	66 63794 → 443 [ACK] Seq=518 Ack=4045 Win=131072 Len=0 TSval=718414656 TSecr=1572243134
145	7.124968	10.0.0.21	52.116.25.250	TCP	66 63794 → 443 [ACK] Seq=518 Ack=4097 Win=130944 Len=0 TSval=718414657 TSecr=1572243134
146	7.125800	10.0.0.21	52.116.25.250	TCP	66 63794 → 443 [ACK] Seq=518 Ack=6377 Win=130048 Len=0 TSval=718414660 TSecr=1572243135
147	7.153483	10.0.0.21	52.116.25.250	TLSv1.2	159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
148	7.348575	52.116.25.250	10.0.0.21	TLSv1.2	117 Change Cipher Spec, Encrypted Handshake Message
149	7.351906	10.0.0.21	52.116.25.250	TCP	66 63794 → 443 [ACK] Seq=611 Ack=6428 Win=130944 Len=0 TSval=718414883 TSecr=1572243370
150	7.354174	10.0.0.21	52.116.25.250	TLSv1.2	561 Application Data

Tráfico DNS

IPA

No.	Time	Source	Destination	Protocol	Length	Info
31075	429.160243	10.0.0.21	10.0.0.1	DNS	79	Standard query 0x16a8 A app-measurement.com
31077	429.164379	10.0.0.1	10.0.0.21	DNS	95	Standard query response 0x16a8 A app-measurement.com A 172.217.192.101
31078	429.164434	10.0.0.1	10.0.0.21	DNS	95	Standard query response 0x16a8 A app-measurement.com A 172.217.192.100
31079	429.164459	10.0.0.1	10.0.0.21	DNS	95	Standard query response 0x16a8 A app-measurement.com A 172.217.192.139
31080	429.164549	10.0.0.1	10.0.0.21	DNS	95	Standard query response 0x16a8 A app-measurement.com A 172.217.192.113
31081	429.164575	10.0.0.1	10.0.0.21	DNS	95	Standard query response 0x16a8 A app-measurement.com A 172.217.192.138
31082	429.164612	10.0.0.1	10.0.0.21	DNS	95	Standard query response 0x16a8 A app-measurement.com A 172.217.192.102
31325	430.381318	10.0.0.21	10.0.0.1	DNS	72	Standard query 0x8462 A xp.apple.com
31345	430.430955	10.0.0.1	10.0.0.21	DNS	88	Standard query response 0x8462 A xp.apple.com A 23.45.136.145
31854	434.332457	10.0.0.21	10.0.0.1	DNS	73	Standard query 0x16ff A www.apple.com
31855	434.340053	10.0.0.21	10.0.0.1	DNS	74	Standard query 0x9973 A www.icloud.com
31856	434.344765	10.0.0.21	10.0.0.1	DNS	69	Standard query 0x4d6f A apple.com
31857	434.384604	10.0.0.1	10.0.0.21	DNS	89	Standard query response 0x16ff A www.apple.com A 23.198.188.95
31858	434.515809	10.0.0.1	10.0.0.21	DNS	90	Standard query response 0x9973 A www.icloud.com A 23.3.249.130
31859	434.518413	10.0.0.1	10.0.0.21	DNS	85	Standard query response 0x4d6f A apple.com A 17.172.224.47
31860	434.518648	10.0.0.1	10.0.0.21	DNS	85	Standard query response 0x4d6f A apple.com A 17.178.96.59
31861	434.518688	10.0.0.1	10.0.0.21	DNS	85	Standard query response 0x4d6f A apple.com A 17.142.160.59
31866	443.770912	10.0.0.21	10.0.0.1	DNS	74	Standard query 0x77b4 A www.google.com
31867	443.774720	10.0.0.1	10.0.0.21	DNS	90	Standard query response 0x77b4 A www.google.com A 64.233.190.104
31868	443.774793	10.0.0.1	10.0.0.21	DNS	90	Standard query response 0x77b4 A www.google.com A 64.233.190.106
31869	443.774815	10.0.0.1	10.0.0.21	DNS	90	Standard query response 0x77b4 A www.google.com A 64.233.190.147
31870	443.774837	10.0.0.1	10.0.0.21	DNS	90	Standard query response 0x77b4 A www.google.com A 64.233.190.103
31871	443.774855	10.0.0.1	10.0.0.21	DNS	90	Standard query response 0x77b4 A www.google.com A 64.233.190.105
31872	443.774875	10.0.0.1	10.0.0.21	DNS	90	Standard query response 0x77b4 A www.google.com A 64.233.190.99
31879	444.656855	10.0.0.21	10.0.0.1	DNS	84	Standard query 0x9879 A ssl.google-analytics.com
31880	444.660444	10.0.0.1	10.0.0.21	DNS	100	Standard query response 0x9879 A ssl.google-analytics.com A 172.217.192.97
31881	444.717790	10.0.0.21	10.0.0.1	DNS	83	Standard query 0x0047 A p9-buy.itunes.apple.com
31882	444.855593	10.0.0.1	10.0.0.21	DNS	99	Standard query response 0x0047 A p9-buy.itunes.apple.com A 17.173.66.102
31948	449.634114	10.0.0.21	10.0.0.1	DNS	85	Standard query 0x088f A 44-courier.push.apple.com
31949	449.830798	10.0.0.1	10.0.0.21	DNS	101	Standard query response 0x088f A 44-courier.push.apple.com A 17.57.144.148
31950	449.832313	10.0.0.1	10.0.0.21	DNS	101	Standard query response 0x088f A 44-courier.push.apple.com A 17.57.144.150
31959	452.654983	10.0.0.21	10.0.0.1	DNS	74	Standard query 0xb060 A imap.gmail.com
31960	452.659499	10.0.0.1	10.0.0.21	DNS	90	Standard query response 0xb060 A imap.gmail.com A 64.233.190.109
31961	452.659624	10.0.0.1	10.0.0.21	DNS	90	Standard query response 0xb060 A imap.gmail.com A 64.233.190.108
32329	516.628179	10.0.0.21	10.0.0.1	DNS	80	Standard query 0x220d A gsp-ssl.ls.apple.com
32330	516.758590	10.0.0.1	10.0.0.21	DNS	96	Standard query response 0x220d A gsp-ssl.ls.apple.com A 17.249.146.18
32375	532.816548	10.0.0.21	10.0.0.1	DNS	95	Standard query 0x7656 A daypass.api-glb-mia.smoot.apple.com
32376	532.820230	10.0.0.1	10.0.0.21	DNS	111	Standard query response 0x7656 A daypass.api-glb-mia.smoot.apple.com A 17.249.153.246
32450	549.152119	10.0.0.21	10.0.0.1	DNS	88	Standard query 0xe654 A smp-device-content.apple.com
32451	549.203396	10.0.0.1	10.0.0.21	DNS	104	Standard query response 0xe654 A smp-device-content.apple.com A 23.198.178.172
32622	566.406367	10.0.0.21	10.0.0.1	DNS	85	Standard query 0xef28 A 33-courier.push.apple.com
32630	566.669982	10.0.0.1	10.0.0.21	DNS	101	Standard query response 0xef28 A 33-courier.push.apple.com A 17.57.144.37
32631	566.670039	10.0.0.1	10.0.0.21	DNS	101	Standard query response 0xef28 A 33-courier.push.apple.com A 17.57.144.36
32711	571.364354	10.0.0.21	10.0.0.1	DNS	85	Standard query 0x79f6 A 50-courier.push.apple.com

Tráfico HTTP

IPA

No se detectó tráfico HTTP durante el período de noviembre.

Otro Tráfico

IPA

No.	Time	Source	Destination	Protocol	Length	Info
2611	19.626453	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.21? Tell 10.0.0.1
2998	20.458515	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.21 is at 20:ee:28:db:b7:8d
8790	66.990433	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.21? Tell 10.0.0.1
8791	66.995672	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.21 is at 20:ee:28:db:b7:8d
15408	112.046432	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.21? Tell 10.0.0.1
15427	112.073890	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.21 is at 20:ee:28:db:b7:8d
23283	156.586450	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.21? Tell 10.0.0.1
23284	156.694184	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.21 is at 20:ee:28:db:b7:8d
24480	193.962479	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.21? Tell 10.0.0.1
24481	194.073659	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.21 is at 20:ee:28:db:b7:8d
30971	263.338461	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.21? Tell 10.0.0.1
30972	263.395354	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.21 is at 20:ee:28:db:b7:8d
31852	434.090435	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.21? Tell 10.0.0.1
31853	434.094874	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.21 is at 20:ee:28:db:b7:8d
32262	481.450453	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.21? Tell 10.0.0.1
32263	481.508480	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.21 is at 20:ee:28:db:b7:8d
32264	481.621690	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	Who has 10.0.0.1? Tell 10.0.0.21
32265	481.621703	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	10.0.0.1 is at bc:f6:85:21:26:0b
32373	521.898459	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.21? Tell 10.0.0.1
32374	521.956672	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.21 is at 20:ee:28:db:b7:8d
32453	549.290435	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.21? Tell 10.0.0.1
32455	549.398889	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.21 is at 20:ee:28:db:b7:8d
32720	572.586439	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.21? Tell 10.0.0.1
32722	572.646644	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.21 is at 20:ee:28:db:b7:8d
32733	601.002461	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42	Who has 10.0.0.21? Tell 10.0.0.1
32734	601.828163	Apple_db:b7:8d	D-LinkIn_21:26:0b	ARP	42	10.0.0.21 is at 20:ee:28:db:b7:8d

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 – 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	✓	No vulnerable
RC4	CVE-2013-2566 CVE-2015-2808	✓	No vulnerable

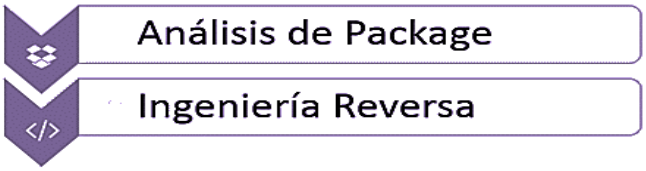
Se detectaron 1 potencial vulnerabilidad en la implementación de SSL/TLS del sitio khipu.com las que afectan la confidencialidad de la información, sin embargo, esta vulnerabilidad tienen un alto grado de dificultad de explotación y se requieren condiciones especiales para su reproducción.

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	97f717a992c4f16552532127ae4191474b6886cb9efcd25ebb4d8f8f1154dda2
Tamaño	9.17 MB
Tipo	.apk
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 de correo en el análisis.

12 Análisis IPA

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

Nombre	khipu715.ipa
SHA256	6ea87c85620c60a7f8675be6fc0fac47bd142ed84bcb6de83ca16d5b27d98a91
Tamaño	16.03 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	✓
		Yandex	✓

IPA		APK	
		Zillya	✓
		ZoneAlarm by Check Point	✓
		Zoner	✓

14 Vulnerabilidades declaradas

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

En este período de análisis se encontraron 1 potenciales vulnerabilidad 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.

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	APK20191227.pcap	ae05efd5fad9ea0c4dbdb7dccaf18959763c2b8d84b296d4a2d1a2d3c39d63bb
2	IOS20191227.pcap	f075bf53500e2d71878d080a7690bfb40e3041d1409f8e664184ed06c74bc7ac