NIVEL

Dirigido a:
Eduardo Parraguez
khipu

JULIO
2018

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
06-07-2018	Kevin Möller	1.0	Creación del documento
06-07-2018	Kevin Möller	1.0	Documentación
09-07-2018	Diego Zamorano	1.1	Revisión y corrección

Tabla de contenido

1 Control de versiones 2
2 Introducción 4
3 Objetivo 5
4 Metodología 6
5 Ámbito 7
6 Análisis de tráfico de datos 8
6.1 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Banco Estado” 8
6.2 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Santander” 8
6.3 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Consorcio” 9
6.4 Tráfico DNS 9
6.5 Tráfico HTTP 10
6.6 Otro Tráfico 10
6.7 Análisis del terminal de pagos 11
6.7.1 iOS 11
7 Análisis SSL 12
7.1 khipu.com – 50.22.89.18 puerto 443 12
7.2 Referencias 13
8 Ethical Hacking Mobile 14
8.1 Procesos automatizados y verificación manual 14
8.2 Análisis IPA 15
8.2.1 URLs detectadas 15
8.2.2 Direcciones IPs detectadas 15
8.2.3 Direcciones de correo detectados 15
8.3 Análisis de Malware 16
9 Vulnerabilidades declaradas 23
10 Anexos 24

2 Introducción

La aplicación khipu permite a personas y empresas, pagar y cobrar, usando sus cuentas corrientes o cuentas vista del banco, de manera fácil y segura.
El terminal de pago de khipu es un navegador web especializado en pagos, por lo que, valida el correcto uso de las páginas de los bancos, forma parte de un sistema que genera comprobantes de pago firmados electrónicamente, es reconocido por los principales antivirus del mundo y se instala desde fuentes oficiales de cada plataforma.

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

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

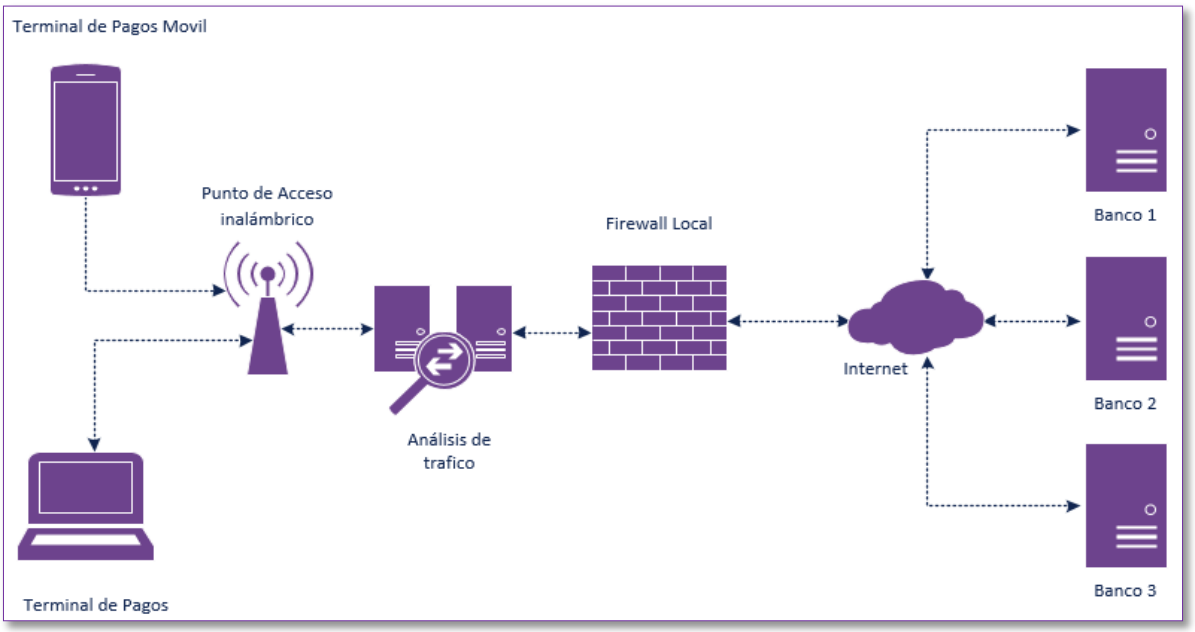
Esta revisión incluye las versiones del terminal de pagos disponible para Windows, OSX, Linux, iOS y Android.

3 Objetivo

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

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 aplicación de **iOS,** se observaron cambios en su HASH.

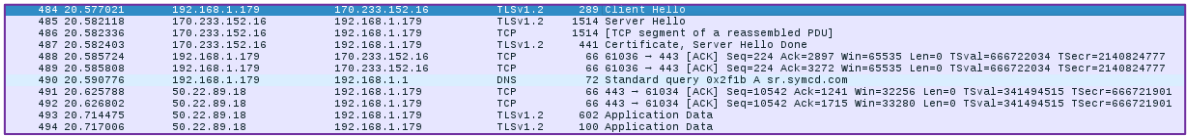
Plataforma	Versión	SHA256SUM
Android	6.6.33	a8ff742eb5b82d87cde85a4bf94c298100ef4eebc61dfbbec069a86340f0b4c8
iOS	**6.23**	**182941ab726a2cddc446d2e134b11957aa1e089b36506843b79dca5c54f2c0f4**
Linux i386	1.17.1922.1	f5533662c3cbce75ecc9d6fdf9632ffb189941533f4992ef0ed8aaf82e6b1b1
Linux x64	1.17.1922.1	9321ae02910a9dfcd8801ca24c11a43e707a62e8b579bcb4a10d79e0e77c908f
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 "Banco Estado"

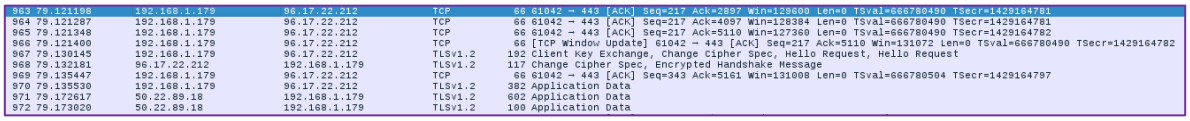
IPA



484	20.577021	192.168.1.179	170.233.152.16	TLSv1.2	289 Client Hello
485	20.582118	170.233.152.16	192.168.1.179	TLSv1.2	1514 Server Hello
486	20.582336	170.233.152.16	192.168.1.179	TCP	1514 [TCP segment of a reassembled PDU]
487	20.582403	170.233.152.16	192.168.1.179	TLSv1.2	441 Certificate, Server Hello Done
488	20.585724	192.168.1.179	170.233.152.16	TCP	66 61036 → 443 [ACK] Seq=224 Ack=2897 Win=65535 Len=0 TSval=666722034 TSecr=2140824777
489	20.585808	192.168.1.179	170.233.152.16	TCP	66 61036 → 443 [ACK] Seq=224 Ack=3272 Win=65535 Len=0 TSval=666722034 TSecr=2140824777
490	20.590776	192.168.1.179	192.168.1.1	DNS	72 Standard query 0x2f1b A sr.symcd.com
491	20.625788	50.22.89.18	192.168.1.179	TCP	66 443 → 61034 [ACK] Seq=10542 Ack=1241 Win=32256 Len=0 TSval=341494515 TSecr=666721901
492	20.626802	50.22.89.18	192.168.1.179	TCP	66 443 → 61034 [ACK] Seq=10542 Ack=1715 Win=33280 Len=0 TSval=341494515 TSecr=666721901
493	20.714475	50.22.89.18	192.168.1.179	TLSv1.2	602 Application Data
494	20.717006	50.22.89.18	192.168.1.179	TLSv1.2	100 Application Data

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

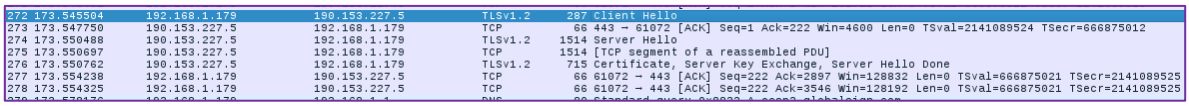
IPA



963	79.121198	192.168.1.179	96.17.22.212	TCP	66 61042 → 443 [ACK] Seq=217 Ack=2897 Win=129600 Len=0 TSval=666780490 TSecr=1429164781
964	79.121287	192.168.1.179	96.17.22.212	TCP	66 61042 → 443 [ACK] Seq=217 Ack=4097 Win=128384 Len=0 TSval=666780490 TSecr=1429164781
965	79.121348	192.168.1.179	96.17.22.212	TCP	66 61042 → 443 [ACK] Seq=217 Ack=5110 Win=127360 Len=0 TSval=666780490 TSecr=1429164782
966	79.121400	192.168.1.179	96.17.22.212	TCP	66 [TCP Window Update] 61042 → 443 [ACK] Seq=217 Ack=5110 Win=131072 Len=0 TSval=666780490 TSecr=1429164782
967	79.130145	192.168.1.179	96.17.22.212	TLSv1.2	192 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
968	79.132181	96.17.22.212	192.168.1.179	TLSv1.2	117 Change Cipher Spec, Encrypted Handshake Message
969	79.135447	192.168.1.179	96.17.22.212	TCP	66 61042 → 443 [ACK] Seq=343 Ack=5161 Win=131008 Len=0 TSval=666780504 TSecr=1429164797
970	79.135530	192.168.1.179	96.17.22.212	TLSv1.2	382 Application Data
971	79.172617	50.22.89.18	192.168.1.179	TLSv1.2	602 Application Data
972	79.173020	50.22.89.18	192.168.1.179	TLSv1.2	100 Application Data

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

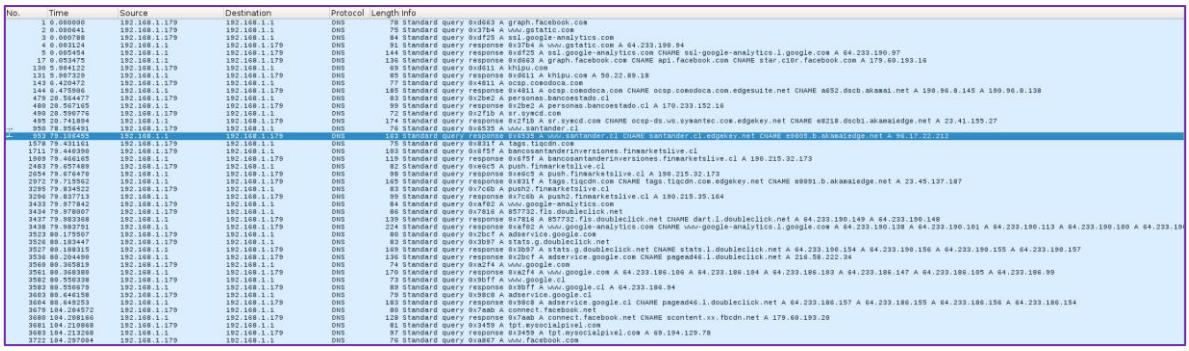
IPA



272	173.545504	192.168.1.179	190.153.227.5	TLSv1.2	287 Client Hello
273	173.547750	190.153.227.5	192.168.1.179	TCP	66 443 → 61072 [ACK] Seq=1 Ack=222 Win=4600 Len=0 TSval=2141089524 TSecr=666875012
274	173.550488	190.153.227.5	192.168.1.179	TLSv1.2	1514 Server Hello
275	173.550697	190.153.227.5	192.168.1.179	TCP	1514 [TCP segment of a reassembled PDU]
276	173.550762	190.153.227.5	192.168.1.179	TLSv1.2	715 Certificate, Server Key Exchange, Server Hello Done
277	173.554238	192.168.1.179	190.153.227.5	TCP	66 61072 → 443 [ACK] Seq=222 Ack=2897 Win=128832 Len=0 TSval=666875021 TSecr=2141089525
278	173.554325	192.168.1.179	190.153.227.5	TCP	66 61072 → 443 [ACK] Seq=222 Ack=3546 Win=128192 Len=0 TSval=666875021 TSecr=2141089525

6.4 Tráfico DNS

IPA

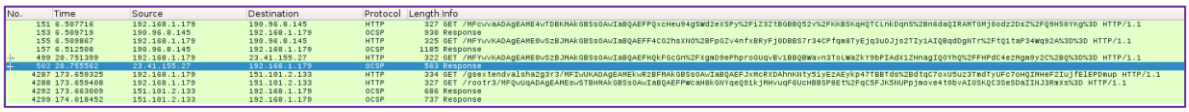


No.	Time	Source	Destination	Protocol	Length	Info
	1 0.000000	192.168.1.179	192.168.1.1	DNS	78	Standard query 0xdd63 A graph.facebook.com
	2 0.000641	192.168.1.179	192.168.1.1	DNS	75	Standard query 0x37b4 A www.gstatic.com
	3 0.000788	192.168.1.179	192.168.1.1	DNS	84	Standard query 0xdf25 A ssl.google-analytics.com
	4 0.003124	192.168.1.1	192.168.1.179	DNS	91	Standard query response 0x37b4 A www.gstatic.com A 64.233.190.94
	5 0.005454	192.168.1.1	192.168.1.179	DNS	144	Standard query response 0xdf25 A ssl.google-analytics.com CNAME ssl-google-analytics.l.google.com A 64.233.190.97
	17 0.053475	192.168.1.1	192.168.1.179	DNS	136	Standard query response 0xd663 A graph.facebook.com CNAME api.facebook.com CNAME star.c10r.facebook.com A 179.60.193.16
	130 5.994122	192.168.1.179	192.168.1.1	DNS	69	Standard query 0xd611 A khipu.com
	131 5.997329	192.168.1.1	192.168.1.179	DNS	85	Standard query response 0xd611 A khipu.com A 50.22.89.18
	143 6.420472	192.168.1.179	192.168.1.1	DNS	77	Standard query 0x4911 A ocsp.comodoca.com
	144 6.475906	192.168.1.1	192.168.1.179	DNS	185	Standard query response 0x4911 A ocsp.comodoca.com CNAME ocsp.comodoca.com.edgesuite.net CNAME a652.dscb.akamai.net A 190.96.8.145 A 190.96.8.138
	479 20.564477	192.168.1.179	192.168.1.1	DNS	83	Standard query 0x2be2 A personas.bancoestado.cl
	480 20.567165	192.168.1.1	192.168.1.179	DNS	99	Standard query response 0x2be2 A personas.bancoestado.cl A 170.233.152.16
	489 20.590776	192.168.1.179	192.168.1.1	DNS	72	Standard query 0x2f1b A sr.symcd.com
	495 20.741894	192.168.1.1	192.168.1.179	DNS	174	Standard query response 0x2f1b A sr.symcd.com CNAME ocsp-ds.ws.symantec.com.edgekey.net CNAME e8218.dscb1.akamaiedge.net A 23.41.155.27
	950 78.956491	192.168.1.179	192.168.1.1	DNS	76	Standard query 0x6535 A www.santander.cl
	952 79.106455	192.168.1.1	192.168.1.179	DNS	163	Standard query response 0x6535 A www.santander.cl CNAME santander.cl.edgekey.net CNAME e8805.b.akamaiedge.net A 96.17.22.212
	1578 79.431161	192.168.1.179	192.168.1.1	DNS	75	Standard query 0x831f A tags.tiqcdn.com
	1711 79.446398	192.168.1.179	192.168.1.1	DNS	103	Standard query 0x6f5f A bancosantanderinversiones.finamarketslive.cl
	1969 79.466165	192.168.1.1	192.168.1.179	DNS	119	Standard query response 0x6f5f A bancosantanderinversiones.finamarketslive.cl A 190.215.32.173
	2483 79.657489	192.168.1.179	192.168.1.1	DNS	82	Standard query 0x46c5 A push.finamarketslive.cl
	2654 79.676478	192.168.1.1	192.168.1.179	DNS	98	Standard query response 0x46c5 A push.finamarketslive.cl A 190.215.32.173
	2972 79.715562	192.168.1.1	192.168.1.179	DNS	165	Standard query response 0x831f A tags.tiqcdn.com CNAME tags.tiqcdn.com.edgekey.net CNAME e8091.b.akamaiedge.net A 23.45.137.187
	3295 79.834522	192.168.1.179	192.168.1.1	DNS	83	Standard query 0x7c6b A push2.finamarketslive.cl
	3296 79.837713	192.168.1.1	192.168.1.179	DNS	99	Standard query response 0x7c6b A push2.finamarketslive.cl A 190.215.35.164
	3433 79.877842	192.168.1.179	192.168.1.1	DNS	84	Standard query 0xafd2 A www.google-analytics.com
	3434 79.878007	192.168.1.179	192.168.1.1	DNS	86	Standard query 0x7816 A 857732.fls.doubleclick.net
	3437 79.883368	192.168.1.1	192.168.1.179	DNS	139	Standard query response 0x7816 A 857732.fls.doubleclick.net CNAME dart.l.doubleclick.net A 64.233.190.149 A 64.233.190.148
	3438 79.883791	192.168.1.1	192.168.1.179	DNS	224	Standard query response 0xafd2 A www.google-analytics.com CNAME www-google-analytics.l.google.com A 64.233.190.138 A 64.233.190.101 A 64.233.190.113 A 64.233.190.100 A 64.233.19
	3523 80.175507	192.168.1.179	192.168.1.1	DNS	80	Standard query 0x2bcf A adservice.google.com
	3526 80.183447	192.168.1.179	192.168.1.1	DNS	83	Standard query 0x3b97 A stats.g.doubleclick.net
	3527 80.188315	192.168.1.1	192.168.1.179	DNS	169	Standard query response 0x3b97 A stats.g.doubleclick.net CNAME stats.l.doubleclick.net A 64.233.190.154 A 64.233.190.156 A 64.233.190.155 A 64.233.190.157
	3536 80.204480	192.168.1.1	192.168.1.179	DNS	136	Standard query response 0x2bcf A adservice.google.com CNAME pagead46.l.doubleclick.net A 216.58.222.34
	3560 80.365818	192.168.1.179	192.168.1.1	DNS	74	Standard query 0xa2f4 A www.google.com
	3561 80.368388	192.168.1.1	192.168.1.179	DNS	179	Standard query response 0xa2f4 A www.google.com A 64.233.186.106 A 64.233.186.104 A 64.233.186.103 A 64.233.186.147 A 64.233.186.105 A 64.233.186.99
	3582 80.556239	192.168.1.179	192.168.1.1	DNS	73	Standard query 0x9bff A www.google.cl
	3583 80.559679	192.168.1.1	192.168.1.179	DNS	89	Standard query response 0x9bff A www.google.cl A 64.233.186.94
	3603 80.646158	192.168.1.179	192.168.1.1	DNS	79	Standard query 0x98c8 A adservice.google.cl
	3604 80.649253	192.168.1.1	192.168.1.179	DNS	183	Standard query response 0x98c8 A adservice.google.cl CNAME pagead46.l.doubleclick.net A 64.233.186.157 A 64.233.186.155 A 64.233.186.156 A 64.233.186.154
	3679 104.204572	192.168.1.179	192.168.1.1	DNS	80	Standard query 0x7aab A connect.facebook.net
	3680 104.209166	192.168.1.1	192.168.1.179	DNS	128	Standard query response 0x7aab A connect.facebook.net CNAME scontent.xx.fbcdn.net A 179.60.193.20
	3681 104.210868	192.168.1.179	192.168.1.1	DNS	81	Standard query 0x3459 A tpt.mysocialpixel.com
	3683 104.213260	192.168.1.1	192.168.1.179	DNS	97	Standard query response 0x3459 A tpt.mysocialpixel.com A 69.194.129.78
	3722 104.297094	192.168.1.179	192.168.1.1	DNS	76	Standard query 0xa867 A www.facebook.com

3722	104.297094	192.168.1.179	192.168.1.1	DNS	76 Standard query 0xa867 A www.facebook.com
3726	104.404537	192.168.1.1	192.168.1.179	DNS	123 Standard query response 0xa867 A www.facebook.com CNAME star-z-mini.c10r.facebook.com A 179.60.193.38
3779	104.898871	192.168.1.179	192.168.1.1	DNS	82 Standard query 0x6b8d A e9805.b.akamaiedge.net
3783	105.047346	192.168.1.1	192.168.1.179	DNS	98 Standard query response 0x6b8d A e9805.b.akamaiedge.net A 96.17.22.212
3915	118.914513	192.168.1.179	192.168.1.1	DNS	76 Standard query 0x7b4a A www.santander.cl
3918	118.970276	192.168.1.1	192.168.1.179	DNS	163 Standard query response 0x7b4a A www.santander.cl CNAME santander.cl.edgekey.net CNAME e8805.b.akamaiedge.net A 96.17.22.212
4086	161.184190	192.168.1.179	192.168.1.1	DNS	75 Standard query 0xe211 A www.gstatic.com
4087	161.187672	192.168.1.1	192.168.1.179	DNS	91 Standard query response 0xe211 A www.gstatic.com A 64.233.190.94
4043	161.282638	192.168.1.179	192.168.1.1	DNS	82 Standard query 0xcfb3 A star.c10r.facebook.com
4046	161.337505	192.168.1.1	192.168.1.179	DNS	98 Standard query response 0xcfb3 A star.c10r.facebook.com A 179.60.193.16
4258	172.524603	192.168.1.179	192.168.1.1	DNS	81 Standard query 0xfa3d A www.bancoconsorcio.cl
4265	173.533102	192.168.1.1	192.168.1.179	DNS	97 Standard query response 0xfa3d A www.bancoconsorcio.cl A 190.153.227.5
4266	173.535535	192.168.1.179	192.168.1.1	DNS	81 Standard query 0xfa3d A www.bancoconsorcio.cl
4268	173.538702	192.168.1.1	192.168.1.179	DNS	97 Standard query response 0xfa3d A www.bancoconsorcio.cl A 190.153.227.5
4279	173.579176	192.168.1.179	192.168.1.1	DNS	80 Standard query 0x8822 A ocsp2.globalsign.com
4280	173.636054	192.168.1.1	192.168.1.179	DNS	217 Standard query response 0x8822 A ocsp2.globalsign.com CNAME global.prd.cdn.globalsign.com CNAME prod.globalsign.map.fastly.net A 151.101.2.133 A 151.101.66.133 A 151.101.130.133

6.5 Tráfico HTTP

IPA



No.	Time	Source	Destination	Protocol	Length	Info
151	6.507716	192.168.1.179	190.96.8.145	HTTP	327	GET /MFGvVwADAgEAME4wTDBKMAkGBSsOAwIaBQAEFPQxcHeu94gSWd2exSPy%2F1Z3ZtBOBBQ52v%2FKkBSkqHqTCLnkDqn5%2Bn6daQIRAHTGHji6odz2DsZ%2FQ9HS8YkgK%3D HTTP/1.1
153	6.509719	190.96.8.145	192.168.1.179	OCSP	930	Response
155	6.509867	192.168.1.179	190.96.8.145	HTTP	325	GET /MFYwVKADAgEAME0wSzBJMAkGBSsOAwIaBQAEFF4C02hsXH0%2BFpGZv4nfxBRyFj0DBBS7r34CPfqm8TyEjq3uOJjs2TIy1AIQ8qdDgNTr%2FtQitaP34Wq92A%3D%3D HTTP/1.1
157	6.512508	190.96.8.145	192.168.1.179	OCSP	1185	Response
499	20.751399	192.168.1.179	23.41.155.27	HTTP	322	GET /MFYwVKADAgEAME0wSzBJMAkGBSsOAwIaBQAEFHQkFGcGn%2FxgaD9ePhproGUqvBv1BBQBWavn3ToLWaZkY9bPIAdX1ZHnagIQ0YhQ%2FFHFdC4e2Mga0y2C%2BQ%3D%3D HTTP/1.1
502	20.781582	23.41.155.27	192.168.1.179	OCSP	563	Response
4287	173.659325	192.168.1.179	151.101.2.133	HTTP	334	GET /gsextendvalsha2g3r3/MFIwUKADAgEAMEkwR2BFMAkGBSsOAwIaBQAEFJxMcRtDAhhKHTy5iyEzAEykp47TBBTds%2BdTqC7oxU5u23TmdTyUFc7oHQIMHeF2IujfElEPDmup HTTP/1.1
4288	173.659408	192.168.1.179	151.101.2.133	HTTP	327	GET /rootr3/MFQwUqADAgEAMEswSTBHMAkGBSsOAwIaBQAEFPWcaH8kGNYqeQ91kjMHvuqF6UcHBBSPBEt%2FqC5FJkSHUPpjmove4t0bvAIOSkQC3Se5DaIIhJ3RmXs%3D HTTP/1.1
4292	173.663009	151.101.2.133	192.168.1.179	OCSP	686	Response
4299	174.018452	151.101.2.133	192.168.1.179	OCSP	737	Response

6.6 Otro Tráfico

IPA

No.	Time	Source	Destination	Protocol	Length	Info
128	5.008145	Tp-LinkT_df:10:c8	20:ee:28:db:b7:8d	ARP	42	Who has 192.168.1.179? Tell 192.168.1.1
129	5.046988	20:ee:28:db:b7:8d	Tp-LinkT_df:10:c8	ARP	42	192.168.1.179 is at 20:ee:28:db:b7:8d
700	55.408127	Tp-LinkT_df:10:c8	20:ee:28:db:b7:8d	ARP	42	Who has 192.168.1.179? Tell 192.168.1.1
701	55.428070	20:ee:28:db:b7:8d	Tp-LinkT_df:10:c8	ARP	42	192.168.1.179 is at 20:ee:28:db:b7:8d
703	56.623689	20:ee:28:db:b7:8d	Tp-LinkT_df:10:c8	ARP	42	Who has 192.168.1.1? Tell 192.168.1.179
704	56.623750	Tp-LinkT_df:10:c8	20:ee:28:db:b7:8d	ARP	42	192.168.1.1 is at a4:2b:b0:df:10:c8
3796	109.018129	Tp-LinkT_df:10:c8	20:ee:28:db:b7:8d	ARP	42	Who has 192.168.1.179? Tell 192.168.1.1
3797	109.021726	20:ee:28:db:b7:8d	Tp-LinkT_df:10:c8	ARP	42	192.168.1.179 is at 20:ee:28:db:b7:8d
3940	146.629965	20:ee:28:db:b7:8d	Tp-LinkT_df:10:c8	ARP	42	Who has 192.168.1.1? Tell 192.168.1.179
3941	146.630026	Tp-LinkT_df:10:c8	20:ee:28:db:b7:8d	ARP	42	192.168.1.1 is at a4:2b:b0:df:10:c8
4093	164.358148	Tp-LinkT_df:10:c8	20:ee:28:db:b7:8d	ARP	42	Who has 192.168.1.179? Tell 192.168.1.1
4094	164.383677	20:ee:28:db:b7:8d	Tp-LinkT_df:10:c8	ARP	42	192.168.1.179 is at 20:ee:28:db:b7:8d

6.7 Análisis del terminal de pagos

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

6.7.1 iOS

Origen	Destino	Tipo de Tráfico	Descripción
192.168.1.179	50.22.89.18	TLSv1.2	khipu
192.168.1. 179	170.233.152.16	TLSv1.2	Banco Estado
192.168.1. 179	96.17.22.212	TLSv1.2	Banco Santander
192.168.1. 179	190.153.227.5	TLSv1.2	Banco Consorcio

7 Análisis SSL

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

7.1 khipu.com – 50.22.89.18 puerto 443

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

DROWN	CVE-2016-0703	✓	No vulnerable
LOGJAM	CVE-2015-4000	✓	No vulnerable
BEAST	CVE-2011-3389	✗	Vulnerable
LUCKY13	CVE-2013-0169	✗	Vulnerable
RC4	CVE-2013-2566 CVE-2015-2808	✓	No vulnerable

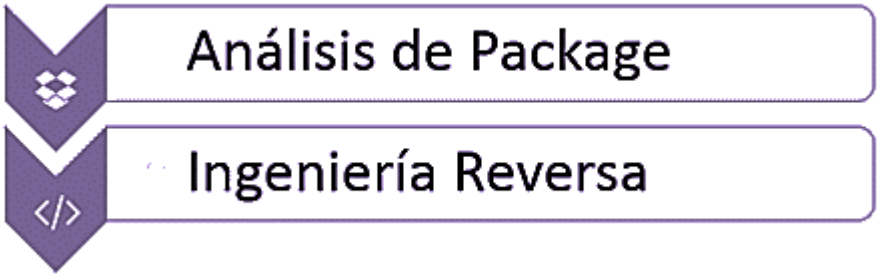
Se detectaron 2 vulnerabilidades en la implementación de SSL/TLS del sitio khipu.com las que afectan la confidencialidad de la información, sin embargo, estas vulnerabilidades tienen un alto grado de dificultad de explotación y se requieren condiciones especiales para su correcta explotación.

7.2 Referencias

Nombre	Link de referencia
Heartbleed	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
ROBOT	https://robotattack.org/
BREACH	http://breachattack.com/
POODLE	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555
FREAK	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204
Logjam	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
BEAST	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3389
RC4	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2566
SLOTH	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7575
DROWN	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0800
Padding Oracle	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2107
SWEET32	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2183
LUCKY13	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0169

8 Ethical Hacking Mobile

8.1 Procesos automatizados y verificación manual



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

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

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

8.2 Análisis IPA

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

Nombre	khipu.apk
SHA256	182941ab726a2cddc446d2e134b11957aa1e089b36506843b79dca5c54f2c0f4
Tamaño	9.8 MB
Tipo	IPA
URLs Interesantes	0
IPs encontradas	0
Emails encontrados	0

8.2.1 URLs detectadas

No se encontraron URLs en el análisis.

8.2.2 Direcciones IPs detectadas

No se encontraron direcciones IP en el análisis.

8.2.3 Direcciones de correo detectados

No se encontraron direcciones de correo en el análisis.

8.3 Análisis de Malware

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

Android	
Motor	**Estado**
Ad-Aware	✓
AegisLab	✓
AhnLab-V3	✓
Alibaba	✓
ALYac	✓
Antiy-AVL	✓
Arcabit	✓
Avast	✓
Avast Mobile Security	✓
AVG	✓
Avira	✓
AVware	✓
Baidu	✓
BitDefender	✓

Bkav	✓
CAT-QuickHeal	✓
ClamAV	✓
CMC	✓
Comodo	✓
Cyren	✓
Emsisoft	✓
eScan	✓
ESET-NOD32	✓
F-Prot	✓
F-Secure	✓
Fortinet	✓
GData	✓
Ikarus	✓
Jiangmin	✓
K7AntiVirus	✓
K7GW	✓
Kaspersky	✓
Kingsoft	✓

Malwarebytes	✓
MAX	✓
McAfee	✓
McAfee-GW-Edition	✓
Microsoft	✓
NANO-Antivirus	✓
nProtect	✓
Panda	✓
Qihoo-360	✓
Rising	✓
Sophos AV	✓
SUPERAntiSpyware	✓
Symantec	✓
Symantec Mobile Insight	✓
Tencent	✓
TheHacker	✓
TrendMicro	✓
TrendMicro-HouseCall	✓
Trustlook	✓

VBA32	✓
VIPRE	✓
ViRobot	✓
Webroot	✓
WhiteArmor	✓
Yandex	✓
Zillya	✓
ZoneAlarm	✓
Zoner	✓

iOS	
Motor	**Estado**
Ad-Aware	✓
AegisLab	✓
AhnLab-V3	✓
Alibaba	✓
ALYac	✓
Antiy-AVL	✓
Arcabit	✓
Avast	✓
Avast Mobile Security	✓
AVG	✓
Avira	✓
AVware	✓
Baidu	✓
BitDefender	✓
Bkav	✓
CAT-QuickHeal	✓
ClamAV	✓
CMC	✓

Comodo	✓
Cyren	✓
Emsisoft	✓
eScan	✓
ESET-NOD32	✓
F-Prot	✓
F-Secure	✓
Fortinet	✓
GData	✓
Ikarus	✓
Jiangmin	✓
K7AntiVirus	✓
K7GW	✓
Kaspersky	✓
Kingsoft	✓
Malwarebytes	✓
MAX	✓
McAfee	✓
McAfee-GW-Edition	✓

Microsoft	✓
NANO-Antivirus	✓
nProtect	✓
Panda	✓
Qihoo-360	✓
Rising	✓
Sophos AV	✓
SUPERAntiSpyware	✓
Symantec	✓
Symantec Mobile Insight	✓
Tencent	✓
TheHacker	✓
TrendMicro	✓
TrendMicro-HouseCall	✓
Trustlook	✓
VBA32	✓
VIPRE	✓
ViRobot	✓
Webroot	✓

WhiteArmor	✓
Yandex	✓
Zillya	✓
ZoneAlarm	✓
Zoner	✓

9 Vulnerabilidades declaradas

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

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

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

Referencias

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

10 Anexos

#	Archivo	SHA256SUM
2	Khipu_09072018.cap	f3fb44ac0dcc1057ff48aab49cee168369b7acf1d0086d5f60baa93ddda70a42