Dirigido a:
Eduardo Parraguez
khipu

NOVIEMBRE
2020

INFORME TÉCNICO

Análisis de Tráfico de Datos NOVIEMBRE2020

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
03-12-2020	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.

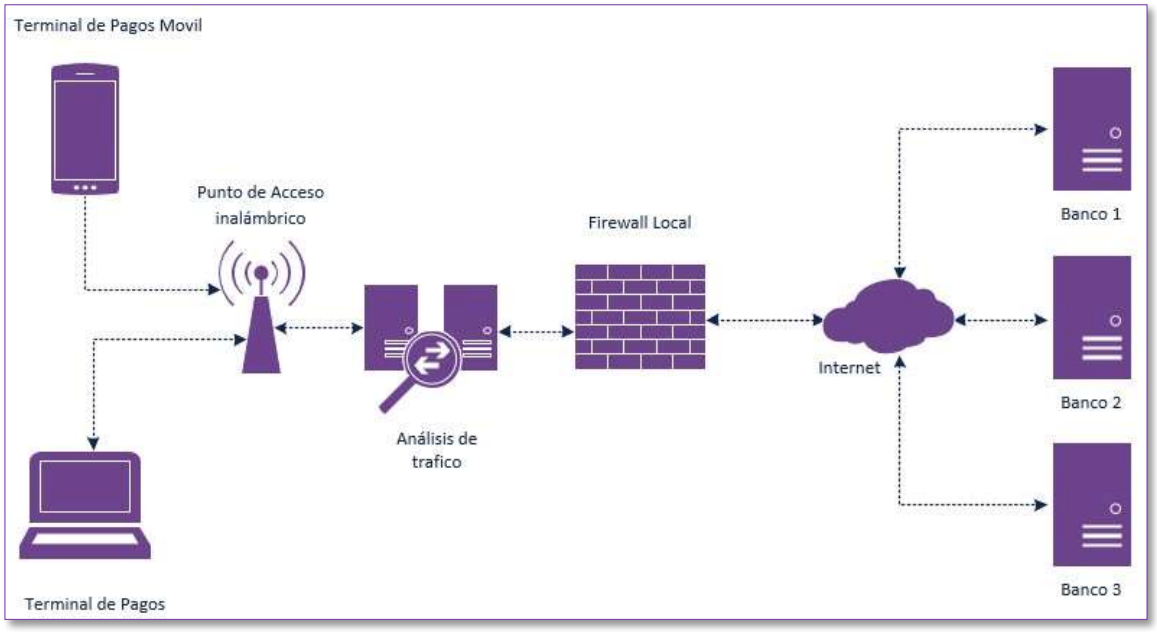
El presente análisis consiste en el monitoreo y análisis de todo el tráfico que genera la aplicación para las distintas plataformas, con el fin de detectar conexiones sospechosas. La revisión incluye la versión del terminal de pagos disponible para IOS y Android.

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 no se registraron cambios para la aplicación de **Android** y **iOS** en su versión.

Plataforma	Versión	SHA256SUM
Android	7.5.19 - Ultima Actualización 16/11/2020	f180e53655571d7dafdf09f54410cf92e9f2a54844fc98bc5ca1615534f257e3
iOS	7.25 - Ultima Actualización 05/09/2020	9f8c7ba90da3fde8f3c1771c134a427988eaf8aa378f22a86939c2bb3585cbe2

6 Análisis 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

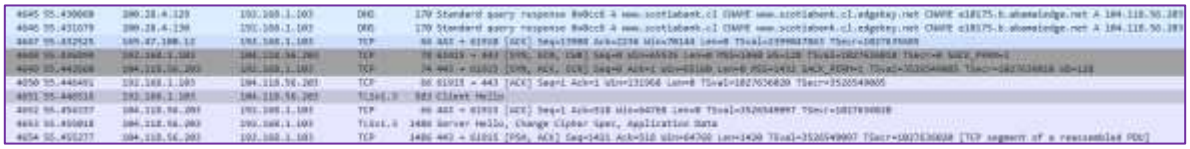
Como se puede ver en las siguientes tablas el tráfico que se genera al utilizar la aplicación de khipu solo se realiza con servidores confiables mediante canales seguros.

7.1 IPA

IPs de Origen	Destino	Tipo de Tráfico	Descripción
192.168.1.103	52.116.25.250 169.47.100.12 169.63.198.82	TLSv1.3	khipu
192.168.1.103	104.118.56.203	TLSv1.3	Banco Scotiabank
192.168.1.103	45.60.0.56	TLSv1.3	Banco Chile
192.168.1.103	200.53.67.183	TLSv1.2	Banco ITAU

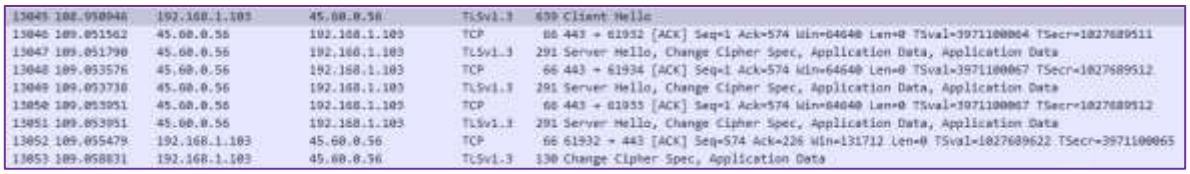
7.2 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Scotiabank”

IPA



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

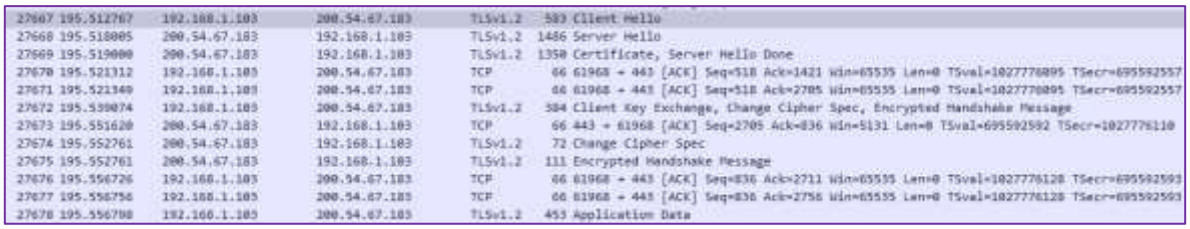
IPA



13045	108.950946	192.168.1.103	45.60.0.56	TLSv1.3	630 Client Hello
13046	109.051562	45.60.0.56	192.168.1.103	TCP	66 443 → 61932 [ACK] Seq=1 Ack=574 Win=64640 Len=0 TSval=3971100064 TSecr=1027689511
13047	109.051790	45.60.0.56	192.168.1.103	TLSv1.3	291 Server Hello, Change Cipher Spec, Application Data, Application Data
13048	109.053576	45.60.0.56	192.168.1.103	TCP	66 443 → 61934 [ACK] Seq=1 Ack=574 Win=64640 Len=0 TSval=3971100067 TSecr=1027689512
13049	109.053738	45.60.0.56	192.168.1.103	TLSv1.3	291 Server Hello, Change Cipher Spec, Application Data, Application Data
13050	109.053951	45.60.0.56	192.168.1.103	TCP	66 443 → 61935 [ACK] Seq=1 Ack=574 Win=64640 Len=0 TSval=3971100067 TSecr=1027689512
13051	109.053951	45.60.0.56	192.168.1.103	TLSv1.3	291 Server Hello, Change Cipher Spec, Application Data, Application Data
13052	109.055479	192.168.1.103	45.60.0.56	TCP	66 61932 → 443 [ACK] Seq=574 Ack=226 Win=131712 Len=0 TSval=1027689622 TSecr=3971100065
13053	109.058831	192.168.1.103	45.60.0.56	TLSv1.3	130 Change Cipher Spec, Application Data

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

IPA



27667	195.512767	192.168.1.103	200.54.67.183	TLSv1.2	583 Client Hello
27668	195.518005	200.54.67.183	192.168.1.103	TLSv1.2	1486 Server Hello
27669	195.519000	200.54.67.183	192.168.1.103	TLSv1.2	1350 Certificate, Server Hello Done
27670	195.521312	192.168.1.103	200.54.67.183	TCP	66 61968 → 443 [ACK] Seq=518 Ack=1421 Win=65535 Len=0 TSval=1027776095 TSecr=695592557
27671	195.521349	192.168.1.103	200.54.67.183	TCP	66 61968 → 443 [ACK] Seq=518 Ack=2705 Win=65535 Len=0 TSval=1027776095 TSecr=695592557
27672	195.539074	192.168.1.103	200.54.67.183	TLSv1.2	584 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
27673	195.551620	200.54.67.183	192.168.1.103	TCP	66 443 → 61968 [ACK] Seq=2705 Ack=836 Win=5131 Len=0 TSval=695592592 TSecr=1027776110
27674	195.552761	200.54.67.183	192.168.1.103	TLSv1.2	72 Change Cipher Spec
27675	195.552761	200.54.67.183	192.168.1.103	TLSv1.2	111 Encrypted Handshake Message
27676	195.556726	192.168.1.103	200.54.67.183	TCP	66 61968 → 443 [ACK] Seq=836 Ack=2711 Win=65535 Len=0 TSval=1027776128 TSecr=695592593
27677	195.556756	192.168.1.103	200.54.67.183	TCP	66 61968 → 443 [ACK] Seq=836 Ack=2756 Win=65535 Len=0 TSval=1027776128 TSecr=695592593
27678	195.556798	192.168.1.103	200.54.67.183	TLSv1.2	453 Application Data

+

Tráfico DNS

IPA

Tráfico HTTP

IPA

No se detectó tráfico HTTP durante el periodo de noviembre.

Otro Tráfico

IPA

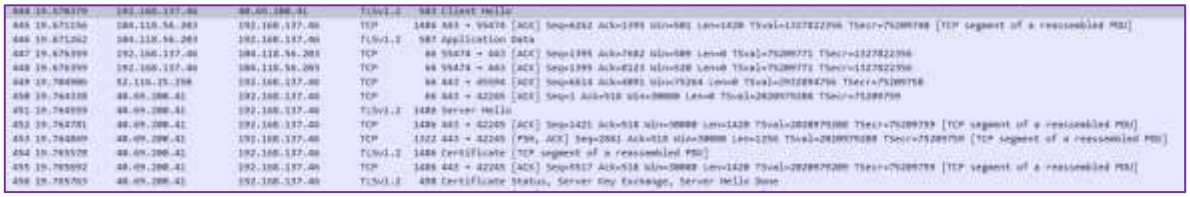
No.	Time	Source	Destination	Protocol	Length	Info
1057	21.985254	AskeyCom_cb:ab:57	Giga-Byt_99:a8:c5	ARP	60	Who has 192.168.1.103? Tell 192.168.1.1
1640	33.676828	AskeyCom_cb:ab:57	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
1693	34.679098	AskeyCom_cb:ab:57	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
1713	35.680848	AskeyCom_cb:ab:57	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
6148	60.640944	AskeyCom_cb:ab:57	Broadcast	ARP	60	Who has 192.168.1.110? Tell 192.168.1.1
6315	68.073703	AskeyCom_cb:ab:57	Giga-Byt_99:a8:c5	ARP	60	Who has 192.168.1.103? Tell 192.168.1.1
16319	113.938692	AskeyCom_cb:ab:57	Giga-Byt_99:a8:c5	ARP	60	Who has 192.168.1.103? Tell 192.168.1.1
23470	161.611543	AskeyCom_cb:ab:57	Giga-Byt_99:a8:c5	ARP	60	Who has 192.168.1.103? Tell 192.168.1.1
31208	207.652364	AskeyCom_cb:ab:57	Giga-Byt_99:a8:c5	ARP	60	Who has 192.168.1.103? Tell 192.168.1.1
36600	256.588877	AskeyCom_cb:ab:57	Giga-Byt_99:a8:c5	ARP	60	Who has 192.168.1.103? Tell 192.168.1.1
36702	261.941894	AskeyCom_cb:ab:57	Broadcast	ARP	60	Who has 192.168.1.110? Tell 192.168.1.1
1058	21.985280	Giga-Byt_99:a8:c5	AskeyCom_cb:ab:57	ARP	42	192.168.1.103 is at 1c:1b:0d:99:a8:c5
5485	56.836361	Giga-Byt_99:a8:c5	Google_26:76:ad	ARP	42	192.168.1.103 is at 1c:1b:0d:99:a8:c5
6316	68.073725	Giga-Byt_99:a8:c5	AskeyCom_cb:ab:57	ARP	42	192.168.1.103 is at 1c:1b:0d:99:a8:c5
16320	113.938721	Giga-Byt_99:a8:c5	AskeyCom_cb:ab:57	ARP	42	192.168.1.103 is at 1c:1b:0d:99:a8:c5
23471	161.611575	Giga-Byt_99:a8:c5	AskeyCom_cb:ab:57	ARP	42	192.168.1.103 is at 1c:1b:0d:99:a8:c5
24916	178.772903	Giga-Byt_99:a8:c5	Google_26:76:ad	ARP	42	192.168.1.103 is at 1c:1b:0d:99:a8:c5
31209	207.652395	Giga-Byt_99:a8:c5	AskeyCom_cb:ab:57	ARP	42	192.168.1.103 is at 1c:1b:0d:99:a8:c5
33836	224.225804	Giga-Byt_99:a8:c5	Google_26:76:ad	ARP	42	192.168.1.103 is at 1c:1b:0d:99:a8:c5
33878	225.226891	Giga-Byt_99:a8:c5	Google_26:76:ad	ARP	42	192.168.1.103 is at 1c:1b:0d:99:a8:c5
36601	256.588909	Giga-Byt_99:a8:c5	AskeyCom_cb:ab:57	ARP	42	192.168.1.103 is at 1c:1b:0d:99:a8:c5
4140	53.503135	Google_26:76:ad	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.110
4412	53.965804	Google_26:76:ad	Broadcast	ARP	60	Who has 192.168.1.106? Tell 192.168.1.110
5484	56.836353	Google_26:76:ad	Broadcast	ARP	60	Who has 192.168.1.103? Tell 192.168.1.110
24898	178.513371	Google_26:76:ad	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.110
24902	178.572940	Google_26:76:ad	Broadcast	ARP	60	Who has 192.168.1.106? Tell 192.168.1.110
24915	178.772872	Google_26:76:ad	Broadcast	ARP	60	Who has 192.168.1.103? Tell 192.168.1.110
33835	224.225773	Google_26:76:ad	Giga-Byt_99:a8:c5	ARP	60	Who has 192.168.1.103? Tell 192.168.1.110
33877	225.226860	Google_26:76:ad	Giga-Byt_99:a8:c5	ARP	60	Who has 192.168.1.103? Tell 192.168.1.110

7.5 APK

IPs de Origen	Destino	Tipo de Tráfico	Descripción
192.168.137.1	52.116.25.250 169.47.100.12 169.63.198.82	TLSv1.2	khipu
192.168.137.46	104.118.56.203	TLSv1.3	Banco Scotiabank
192.168.137.46	45.60.0.56	TLSv1.3	Banco Chile
192.168.137.46	200.11.88.142	TLSv1.	Banco

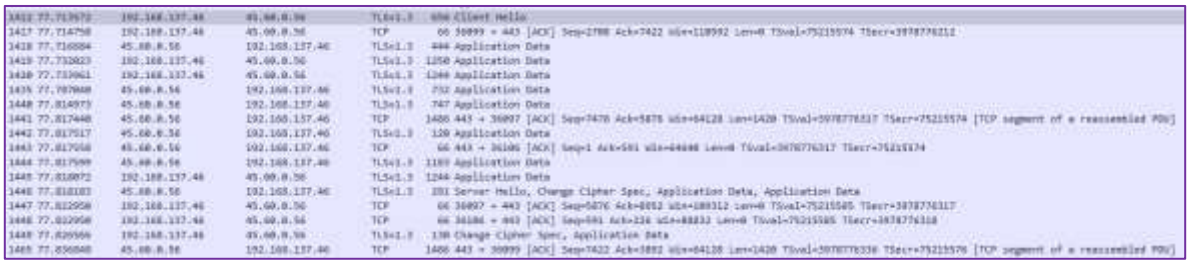
7.6 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Scotiabank”

APK



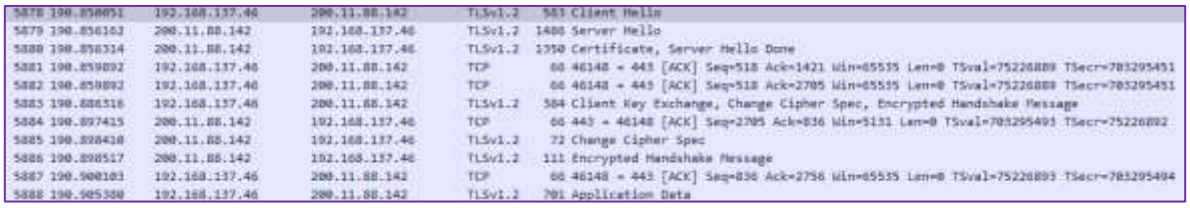
7.7 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Chile”

APK



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

APK



Tráfico DNS

APK

Tráfico HTTP

APK

No se detectó tráfico HTTP durante el periodo de noviembre.

Otro Tráfico

APK

	Time	Source	Destination	Protocol	Length	Info
12	5.058174	d6:09:71:e2:ef:80	Tp-LinkT_56:10:7e	ARP	42	Who has 192.168.137.1? Tell 192.168.137.46
13	5.058208	Tp-LinkT_56:10:7e	d6:09:71:e2:ef:80	ARP	42	192.168.137.1 is at d0:37:45:56:10:7e

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

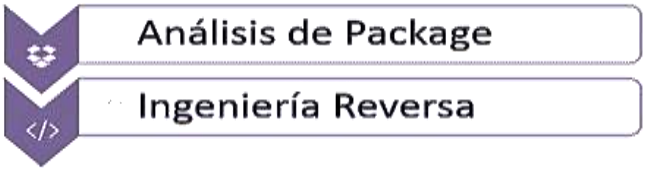
Se detectó 1 potencial vulnerabilidad en la implementación de SSL/TLS del sitio khipu.com la que afecta la confidencialidad de la información, sin embargo, esta vulnerabilidad tiene un alto grado de dificultad de explotación y se requieren condiciones especiales para su reproducción.

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	f180e53655571d7dafdf09f54410cf92e9f2a54844fc98bc5ca1615534f257e3
Tamaño	9.8 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.

12 Análisis IPA

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

Nombre	khipu 7.25.ipa
SHA256	9f8c7ba90da3fde8f3c1771c134a427988eaf8aa378f22a86939c2bb3585cbe2
Tamaño	45.8 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 el archivo .IPA (iOS) y APK (Android)

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)**	✓
Baidu	✓	**Babable**	✓

BitDefender	✓	**Baidu**	✓
BitDefenderTheta	✓	**BitDefender**	✓
Bkav	✓	**Bkav**	✓
CAT-QuickHeal	✓	**CAT-QuickHeal**	✓
ClamAV	✓	**ClamAV**	✓
Comodo	✓	**CMC**	✓
Cynet	✓	**Comodo**	✓
Cyren	✓	**Cyren**	✓
DrWeb	✓	**DrWeb**	✓
Emsisoft	✓	**Emsisoft**	✓
eScan	✓	**ESET-NOD32**	✓
ESET-NOD32	✓	**F-Prot**	✓
F-Prot	✓	**F-Secure**	✓
F-Secure	✓	**FireEye**	✓
FireEye	✓	**Fortinet**	✓
Fortinet	✓	**GData**	✓
GData	✓	**Ikarus**	✓

Ikarus	✓	**Jiangmin**	✓
Jiangmin	✓	**K7AntiVirus**	✓
K7AntiVirus	✓	**K7GW**	✓
K7GW	✓	**Kaspersky**	✓
Kaspersky	✓	**Kingsoft**	✓
Kingsoft	✓	**Malwarebytes**	✓
Malwarebytes	✓	**MAX**	✓
MAX	✓	**MaxSecure**	✓
MaxSecure	✓	**McAfee**	✓
McAfee	✓	**McAfee-GW-Edition**	✓
McAfee-GW-Edition	✓	**Microsoft**	✓
Microsoft	✓	**NANO-Antivirus**	✓
NANO-Antivirus	✓	**Panda**	✓
Panda	✓	**Qihoo-360**	✓
Qihoo-360	✓	**Rising**	✓
Rising	✓	**Sophos AV**	✓

Sangfor Engine Zero	✓	**SUPERAntiSpyware**	✓
SentinelOne (Static ML)	✓	**Symantec**	✓
Sophos AV	✓	**TACHYON**	✓
SUPERAntiSpyware	✓	**Tencent**	✓
Symantec	✓	**TheHacker**	✓
TACHYON	✓	**TotalDefense**	✓
Tencent	✓	**TrendMicro**	✓
TrendMicro	✓	**TrendMicro-ZHouseCall**	✓
TrendMicro-HouseCall	✓	**Trustlook**	✓
VBA32	✓	**VBA32**	✓
VIPRE	✓	**VIPRE**	✓
ViRobot	✓	**ViRobot**	✓
Yandex	✓	**Yandex**	✓
Zillya	✓	**Zillya**	✓
ZoneAlarm by Check Point	✓	**ZoneAlarm by Check Point**	✓
Zoner	✓	**Zoner**	✓

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)	✓
Baidu	✓	Babable	✓
BitDefender	✓	Baidu	✓
BitDefenderTheta	✓	BitDefender	✓
Bkav	✓	Bkav	✓

CAT-QuickHeal	✓	**CAT-QuickHeal**	✓
ClamAV	✓	**ClamAV**	✓
Comodo	✓	**CMC**	✓
Cynet	✓	**Comodo**	✓
Cyren	✓	**Cyren**	✓
DrWeb	✓	**DrWeb**	✓
Emsisoft	✓	**Emsisoft**	✓
eScan	✓	**ESET-NOD32**	✓
ESET-NOD32	✓	**F-Prot**	✓
F-Prot	✓	**F-Secure**	✓
F-Secure	✓	**FireEye**	✓
FireEye	✓	**Fortinet**	✓
Fortinet	✓	**GData**	✓
GData	✓	**Ikarus**	✓
Ikarus	✓	**Jiangmin**	✓
Jiangmin	✓	**K7AntiVirus**	✓
K7AntiVirus	✓	**K7GW**	✓
K7GW	✓	**Kaspersky**	✓

Kaspersky	✓	**Kingsoft**	✓
Kingsoft	✓	**Malwarebytes**	✓
Malwarebytes	✓	**MAX**	✓
MAX	✓	**MaxSecure**	✓
MaxSecure	✓	**McAfee**	✓
McAfee	✓	**McAfee-GW-Edition**	✓
McAfee-GW-Edition	✓	**Microsoft**	✓
Microsoft	✓	**NANO-Antivirus**	✓
NANO-Antivirus	✓	**Panda**	✓
Panda	✓	**Qihoo-360**	✓
Qihoo-360	✓	**Rising**	✓
Rising	✓	**Sophos AV**	✓
Sangfor Engine Zero	✓	**SUPERAntiSpyware**	✓
SentinelOne (Static ML)	✓	**Symantec**	✓
Sophos AV	✓	**TACHYON**	✓
SUPERAntiSpyware	✓	**Tencent**	✓

Symantec	✓	**TheHacker**	✓
TACHYON	✓	**TotalDefense**	✓
Tencent	✓	**TrendMicro**	✓
TrendMicro	✓	**TrendMicro-ZHouseCall**	✓
TrendMicro-HouseCall	✓	**Trustlook**	✓
VBA32	✓	**VBA32**	✓
VIPRE	✓	**VIPRE**	✓
ViRobot	✓	**ViRobot**	✓
Yandex	✓	**Yandex**	✓
Zillya	✓	**Zillya**	✓
ZoneAlarm by Check Point	✓	**ZoneAlarm by Check Point**	✓
Zoner	✓	**Zoner**	✓

14 Vulnerabilidades declaradas

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

En este período de análisis se detectó 1 potencial vulnerabilidad que afectan a la implementación de SSL/TLS, 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/