Dirigido a:
Eduardo Parraguez
khipu

OCTUBRE
2020

INFORME TÉCNICO

Análisis de Tráfico de Datos OCTUBRE 2020

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
06-11-2020	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.

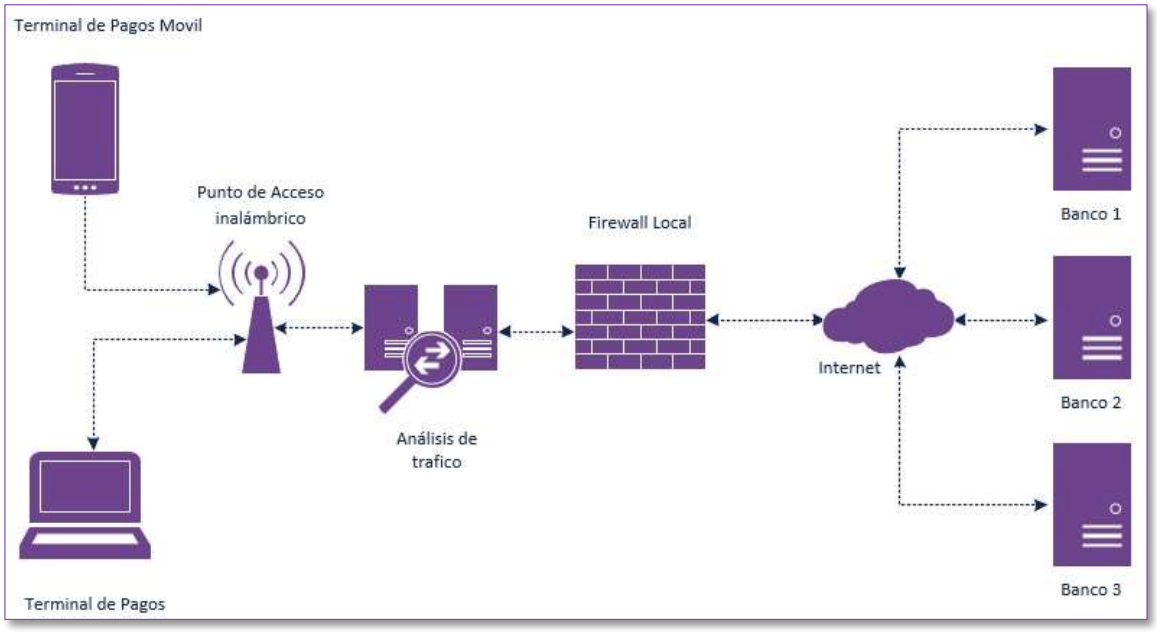
El presente análisis consiste en el monitoreo y análisis de todo el tráfico que genera la aplicación para las distintas plataformas, con el fin de detectar conexiones sospechosas. La revisión incluye la versión del terminal de pagos disponible para IOS y Android.

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	7.5.17 - Ultima Actualización 01/09/2020	bcdcb62639750d61fdf18e19937b52d13c190061cf89a0e3cc037c49c9de6acc
iOS	7.25 - Ultima Actualización 05/09/2020	36f3a7e0d8869852c0b63662208146e00c17a1d291559e7732486ac9370a7f51

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

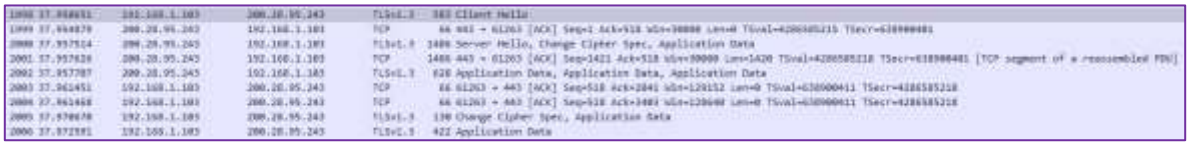
Como se puede ver en las siguientes tablas el tráfico que se genera al utilizar la aplicación de khipu solo se realiza con servidores confiables mediante canales seguros.

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	200.28.95.243	TLSv1.3	Banco Santander
192.168.1.103	104.118.62.97	TLSv1.3	Banco Estado
192.168.1.103	200.10.167.103	TLSv1.2	Banco Falabella

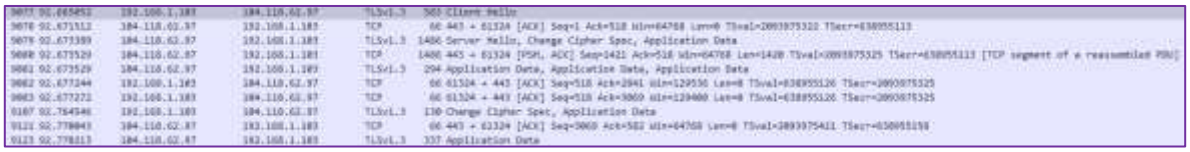
7.2 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Santander”

IPA



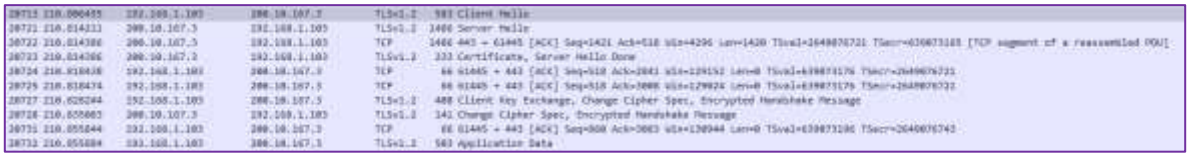
7.3 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Estado”

IPA



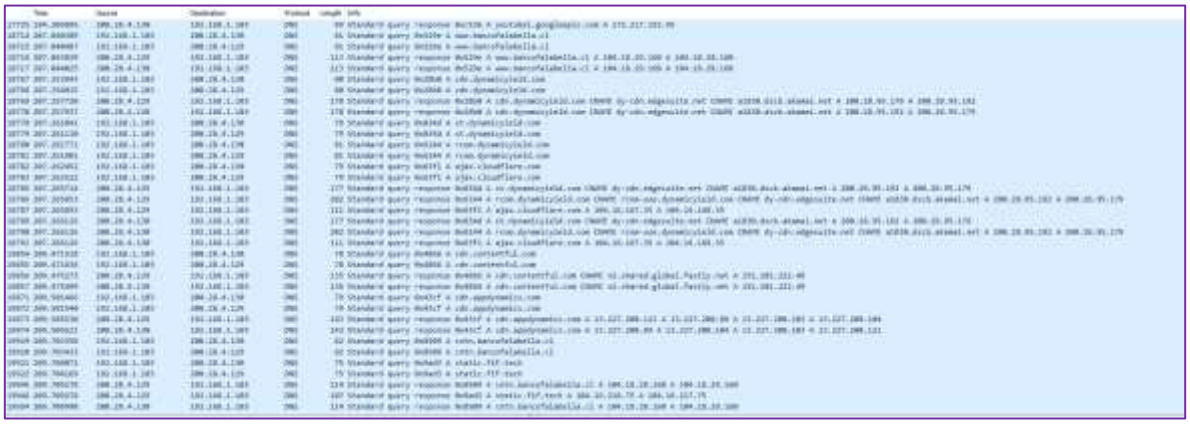
7.4 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Falabella”

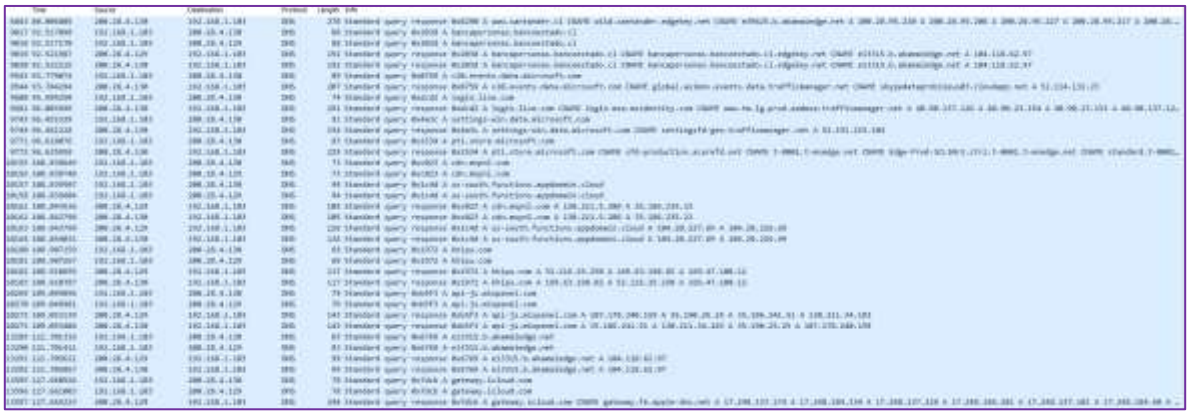
IPA

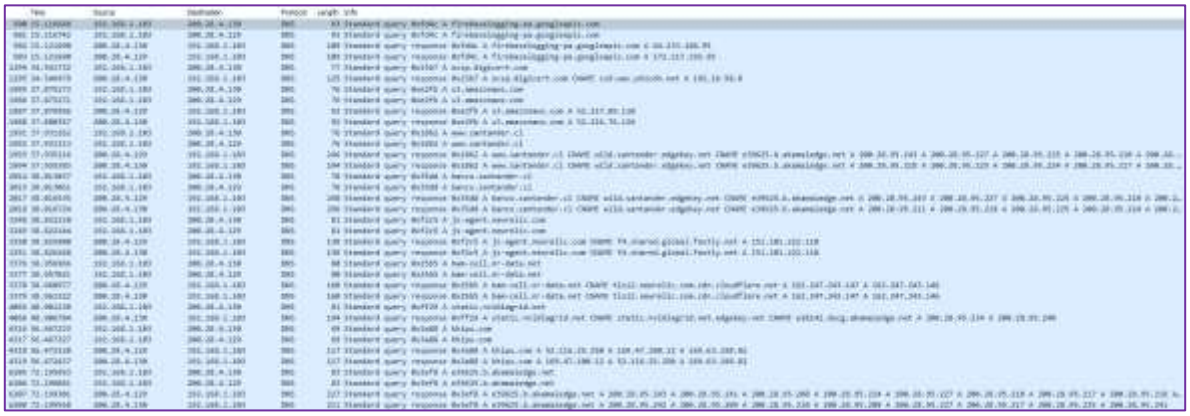


Tráfico DNS

IPA







Tráfico HTTP

IPA

No se detectó tráfico HTTP durante el periodo de OCTUBRE.

Otro Tráfico

IPA

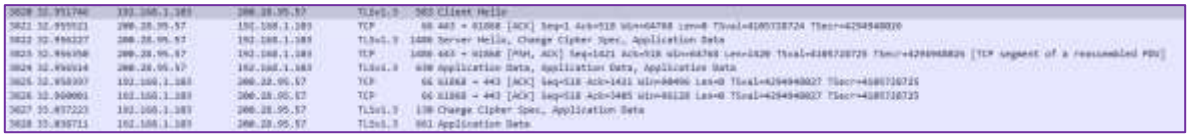
	Time	Source	Destination	Protocol	Length	Info
16900	174.168906	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
16956	174.694851	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
16962	175.695150	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17029	177.181550	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17030	177.694831	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17077	178.695128	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17092	180.138449	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17136	180.694803	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17142	181.695115	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17211	183.168469	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17212	183.694785	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17259	184.695109	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17272	186.142469	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17314	186.694758	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17317	187.695073	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17403	189.181814	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17408	189.695732	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17462	190.695035	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17466	192.138776	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17520	192.695703	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17713	193.695037	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17803	195.165779	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17804	195.695686	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17863	196.695012	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17875	198.139950	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17921	198.695663	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17930	199.694995	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17976	201.174979	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
17977	201.695644	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
18091	202.694966	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
18163	204.132322	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
18231	204.695616	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
18283	205.694942	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
18771	207.260132	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
19803	208.195267	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103
19850	209.195558	Giga-Byt_99:a8:c5	Broadcast	ARP	42	Who has 192.168.1.98? Tell 192.168.1.103

7.5 APK

IPs de Origen	Destino	Tipo de Tráfico	Descripción
192.168.1.103	52.116.25.250 169.47.100.12 169.63.198.82	TLSv1.2	khipu
192.168.1.103	200.28.95.57	TLSv1.3	Banco Santander
192.168.1.103	104.118.62.97	TLSv1.3	Banco Estado
192.168.1.103	104.18.28.160	TLSv1.3	Banco Falabella

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

APK

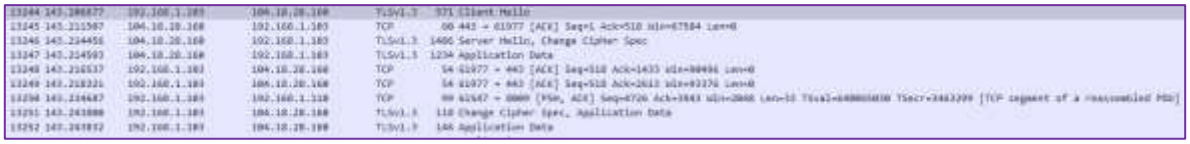


7.7 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Estado”

APK

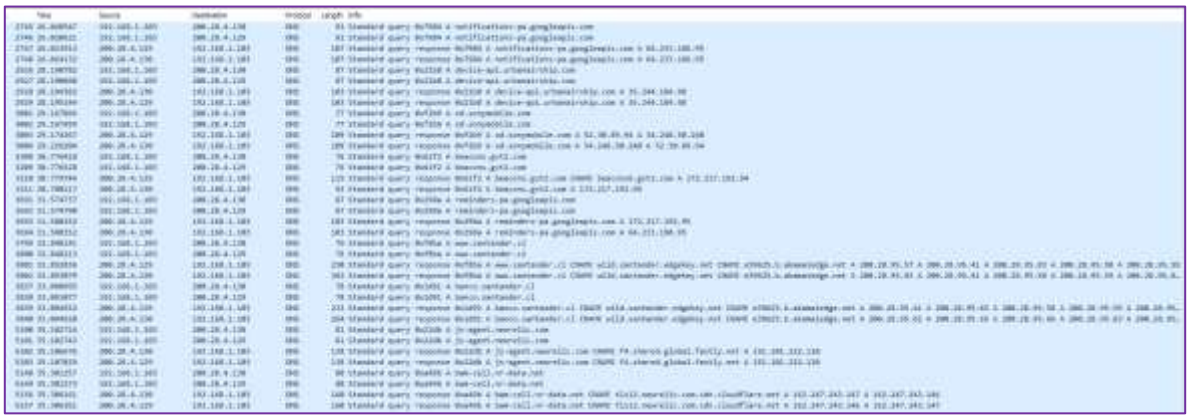
7.8 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Falabella”

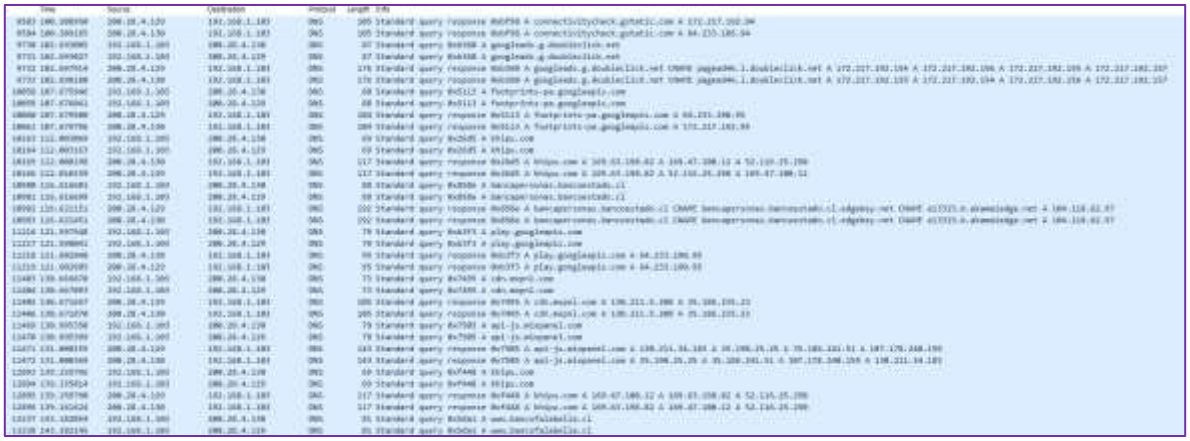
APK



Tráfico DNS

APK





Tráfico HTTP

APK

No se detectó tráfico HTTP durante el periodo de OCTUBRE.

Otro Tráfico

APK

No se detectó tráfico durante el periodo de OCTUBRE.

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

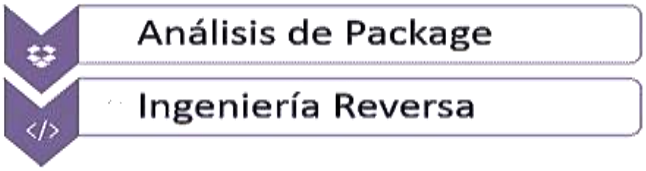
Se detectó 1 potencial vulnerabilidad en la implementación de SSL/TLS del sitio khipu.com la que afecta la confidencialidad de la información, sin embargo, esta vulnerabilidad tiene un alto grado de dificultad de explotación y se requieren condiciones especiales para su reproducción.

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	bcdcb62639750d61fdf18e19937b52d13c190061cf89a0e3cc037c49c9de6acc
Tamaño	9.65 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	36f3a7e0d8869852c0b63662208146e00c17a1d291559e7732486ac9370a7f51
Tamaño	21.42 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/