Dirigido a:
Eduardo Parraguez
khipu

ABRIL
2019

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
11-04-2019	Kevin Möller	1.0	Creación del documento
11-04-2019	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.

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.

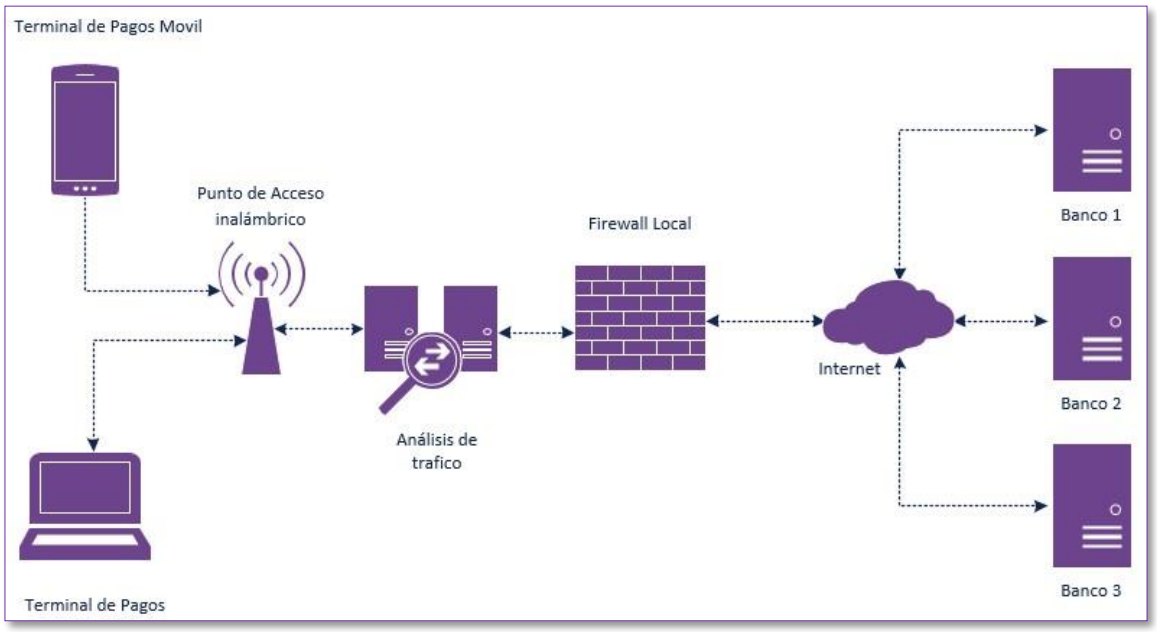
Esta revisión incluye la versión del terminal de pagos disponible para IOS.

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 al terminal de pago de **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 aplicaciones de **iOS** solo en su **HASH.**

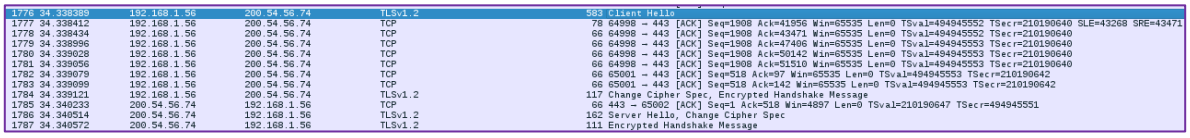
Plataforma	Versión	SHA256SUM
Android	6.9.1	ac7f3db3835729dd63c5c6b623619f0dd94709705867abecb12d5cea1a018d45
iOS	6.29	**7e0028730563cf777d6d952ae0fe08526ec4edf1ae4f50c38c392792d6653e51**
Linux i386	1.17.1922.1	f5533662c3cbce75ecc9d6fdf9632ffb189941533f4992ef0ed8aaf82e6b1b1
Linux x64	1.17.1922.1	9321ae02910a9dfcd8801ca24c11a43e707a62e8b579bcb4a10d79e0e77c908f
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

6.1 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Ripley”

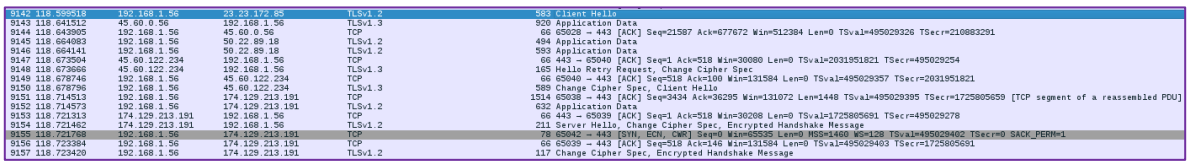
IPA



1776 34.338389	192.168.1.56	200.54.56.74	TLSv1.2	583 Client Hello
1777 34.338412	192.168.1.56	200.54.56.74	TCP	78 64998 → 443 [ACK] Seq=1908 Ack=41956 Win=65535 Len=0 TSval=494945552 TSecr=210190640 SLE=43268 SRE=43471
1778 34.338434	192.168.1.56	200.54.56.74	TCP	66 64998 → 443 [ACK] Seq=1908 Ack=43471 Win=65535 Len=0 TSval=494945552 TSecr=210190640
1779 34.338996	192.168.1.56	200.54.56.74	TCP	66 64998 → 443 [ACK] Seq=1908 Ack=47406 Win=65535 Len=0 TSval=494945553 TSecr=210190640
1780 34.339028	192.168.1.56	200.54.56.74	TCP	66 64998 → 443 [ACK] Seq=1908 Ack=50142 Win=65535 Len=0 TSval=494945553 TSecr=210190640
1781 34.339056	192.168.1.56	200.54.56.74	TCP	66 64998 → 443 [ACK] Seq=1908 Ack=51510 Win=65535 Len=0 TSval=494945553 TSecr=210190640
1782 34.339079	192.168.1.56	200.54.56.74	TCP	66 65001 → 443 [ACK] Seq=518 Ack=97 Win=65535 Len=0 TSval=494945553 TSecr=210190642
1783 34.339099	192.168.1.56	200.54.56.74	TCP	66 65001 → 443 [ACK] Seq=518 Ack=142 Win=65535 Len=0 TSval=494945553 TSecr=210190642
1784 34.339121	192.168.1.56	200.54.56.74	TLSv1.2	117 Change Cipher Spec, Encrypted Handshake Message
1785 34.340233	200.54.56.74	192.168.1.56	TCP	66 443 → 65002 [ACK] Seq=1 Ack=518 Win=4897 Len=0 TSval=210190647 TSecr=494945551
1786 34.340514	200.54.56.74	192.168.1.56	TLSv1.2	162 Server Hello, Change Cipher Spec
1787 34.340572	200.54.56.74	192.168.1.56	TLSv1.2	111 Encrypted Handshake Message

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

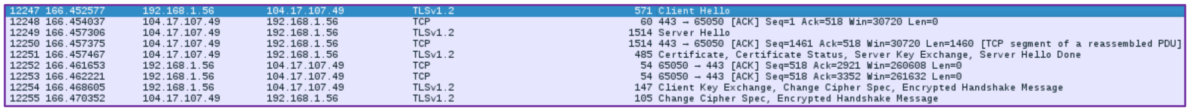
IPA



9142 118.599518	192.168.1.56	23.23.172.85	TLSv1.2	583 Client Hello
9143 118.641512	45.60.0.56	192.168.1.56	TLSv1.3	920 Application Data
9144 118.643005	192.168.1.56	45.60.0.56	TCP	66 65028 → 443 [ACK] Seq=21587 Ack=677672 Win=512384 Len=0 TSval=495029326 TSecr=210883291
9145 118.664083	192.168.1.56	50.22.89.18	TLSv1.2	494 Application Data
9146 118.664141	192.168.1.56	50.22.89.18	TLSv1.2	593 Application Data
9147 118.673504	45.60.122.234	192.168.1.56	TCP	66 443 → 65040 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=2031951821 TSecr=495029254
9148 118.673666	45.60.122.234	192.168.1.56	TLSv1.3	165 Hello Retry Request, Change Cipher Spec
9149 118.678746	192.168.1.56	45.60.122.234	TCP	66 65040 → 443 [ACK] Seq=518 Ack=100 Win=131584 Len=0 TSval=495029357 TSecr=2031951821
9150 118.678786	192.168.1.56	45.60.122.234	TLSv1.3	589 Change Cipher Spec, Client Hello
9151 118.714513	192.168.1.56	174.129.213.191	TCP	1514 65038 → 443 [ACK] Seq=3434 Ack=36295 Win=131072 Len=1448 TSval=495029395 TSecr=1725805659 [TCP segment of a reassembled PDU]
9152 118.714573	192.168.1.56	174.129.213.191	TLSv1.2	632 Application Data
9153 118.721313	174.129.213.191	192.168.1.56	TCP	66 443 → 65039 [ACK] Seq=1 Ack=518 Win=30208 Len=0 TSval=1725805691 TSecr=495029278
9154 118.721462	174.129.213.191	192.168.1.56	TLSv1.2	211 Server Hello, Change Cipher Spec, Encrypted Handshake Message
9155 118.721708	192.168.1.56	174.129.213.191	TCP	78 65042 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 TSval=495029402 TSecr=0 SACK_PERM=1
9156 118.723384	192.168.1.56	174.129.213.191	TCP	66 65038 → 443 [ACK] Seq=518 Ack=146 Win=131584 Len=0 TSval=495029403 TSecr=1725805691
9157 118.723420	192.168.1.56	174.129.213.191	TLSv1.2	117 Change Cipher Spec, Encrypted Handshake Message

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

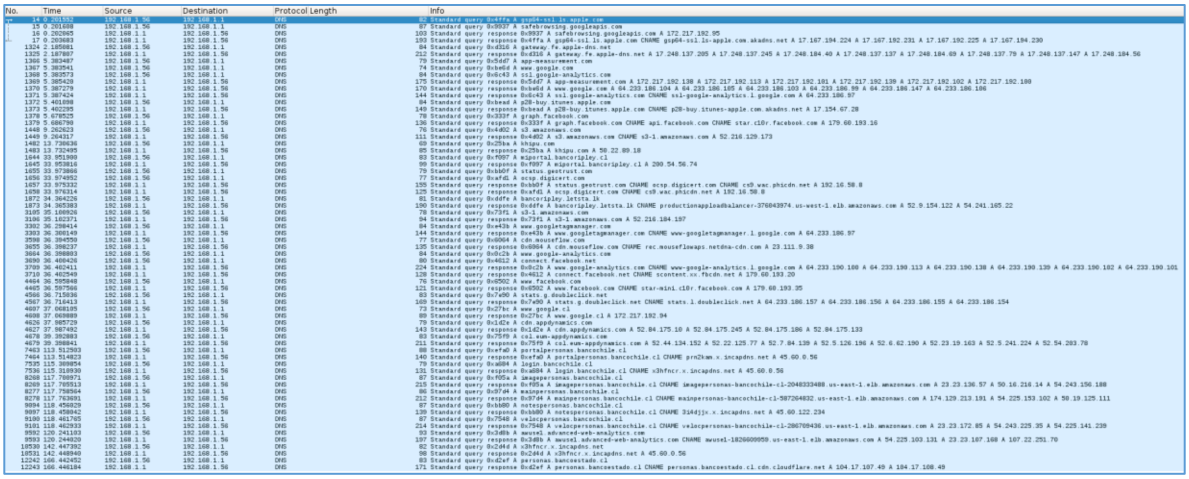
IPA



12247	166.452577	192.168.1.56	104.17.107.49	TLSv1.2	571	Client Hello
12248	166.454037	104.17.107.49	192.168.1.56	TCP	60	443 → 65050 [ACK] Seq=1 Ack=518 Win=30720 Len=0
12249	166.457306	104.17.107.49	192.168.1.56	TLSv1.2	1514	Server Hello
12250	166.457375	104.17.107.49	192.168.1.56	TCP	1514	443 → 65050 [ACK] Seq=1461 Ack=518 Win=30720 Len=1460 [TCP segment of a reassembled PDU]
12251	166.457467	104.17.107.49	192.168.1.56	TLSv1.2	485	Certificate, Certificate Status, Server Key Exchange, Server Hello Done
12252	166.461653	192.168.1.56	104.17.107.49	TCP	54	65050 → 443 [ACK] Seq=518 Ack=2921 Win=260608 Len=0
12253	166.462221	192.168.1.56	104.17.107.49	TCP	54	65050 → 443 [ACK] Seq=518 Ack=3352 Win=261632 Len=0
12254	166.468605	192.168.1.56	104.17.107.49	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
12255	166.470352	104.17.107.49	192.168.1.56	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message

Tráfico DNS

IPA



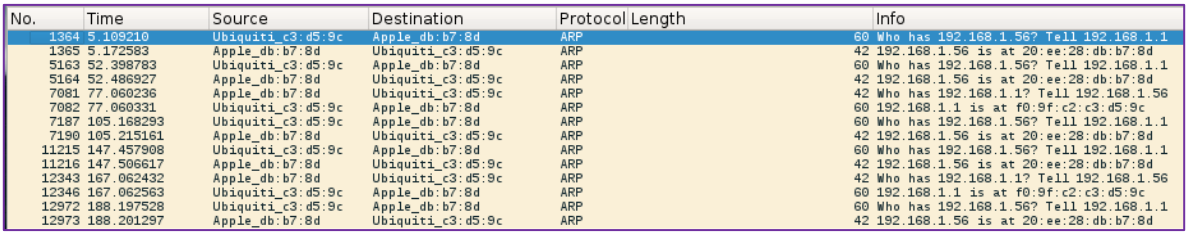
Tráfico HTTP

IPA

No se detecto trafico HTTP durante este análisis.

Otro Tráfico

IPA



No.	Time	Source	Destination	Protocol	Length	Info
1364	5.109210	Ubiquiti_c3:d5:9c	Apple_db:b7:8d	ARP	60	Who has 192.168.1.56? Tell 192.168.1.1
1365	5.172583	Apple_db:b7:8d	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.56 is at 20:ee:28:db:b7:8d
5163	52.398783	Ubiquiti_c3:d5:9c	Apple_db:b7:8d	ARP	60	Who has 192.168.1.56? Tell 192.168.1.1
5164	52.486927	Apple_db:b7:8d	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.56 is at 20:ee:28:db:b7:8d
7081	77.060236	Apple_db:b7:8d	Ubiquiti_c3:d5:9c	ARP	42	Who has 192.168.1.1? Tell 192.168.1.56
7082	77.060331	Ubiquiti_c3:d5:9c	Apple_db:b7:8d	ARP	60	192.168.1.1 is at f0:9f:c2:c3:d5:9c
7187	105.168293	Ubiquiti_c3:d5:9c	Apple_db:b7:8d	ARP	60	Who has 192.168.1.56? Tell 192.168.1.1
7190	105.215161	Apple_db:b7:8d	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.56 is at 20:ee:28:db:b7:8d
11215	147.457908	Ubiquiti_c3:d5:9c	Apple_db:b7:8d	ARP	60	Who has 192.168.1.56? Tell 192.168.1.1
11216	147.506617	Apple_db:b7:8d	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.56 is at 20:ee:28:db:b7:8d
12343	167.062432	Apple_db:b7:8d	Ubiquiti_c3:d5:9c	ARP	42	Who has 192.168.1.1? Tell 192.168.1.56
12346	167.062563	Ubiquiti_c3:d5:9c	Apple_db:b7:8d	ARP	60	192.168.1.1 is at f0:9f:c2:c3:d5:9c
12972	188.197528	Ubiquiti_c3:d5:9c	Apple_db:b7:8d	ARP	60	Who has 192.168.1.56? Tell 192.168.1.1
12973	188.201297	Apple_db:b7:8d	Ubiquiti_c3:d5:9c	ARP	42	192.168.1.56 is at 20:ee:28:db:b7:8d

7 Análisis del terminal de pagos

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

7.1 IPA

Origen	Destino	Tipo de Tráfico	Descripción
192.168.1.56	50.22.89.18	TLSv1.3	khipu
192.168.1. 56	104.17.107.49	TLSv1.2	Banco Ripley
192.168.1. 56	174.129.213.291	TLSv1.2	Banco de Chile
192.168.1. 56	104.17.107.49	TLSv1.2	Banco Estado

8 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

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	✗	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

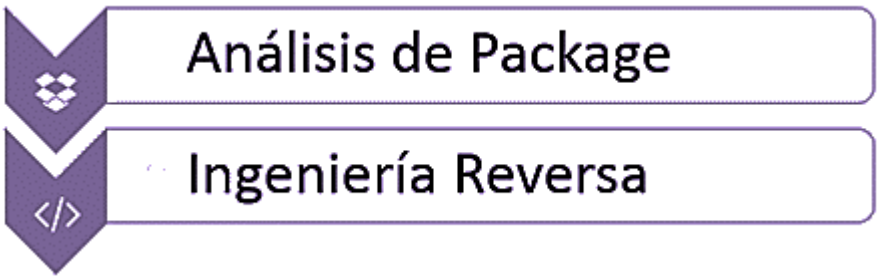
Se detectaron 3 vulnerabilidades en la implementación de SSL/TLS del sitio khipu.com las que afectan la confidencialidad de la información, sin embargo, estas vulnerabilidades tienen un alto grado de dificultad de explotación y se requieren condiciones especiales para su correcta explotación.

9 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

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 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.

11 Análisis IPA

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

Nombre	khipu6.29.ipa
SHA256	7e0028730563cf777d6d952ae0fe08526ec4edf1ae4f50c38c392792d6653e51
Tamaño	14.7 MB
Tipo	.ipa
URLs Interesantes	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 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 el archivo .ipa y el archivo .apk correspondiente a IOS Y Android. En este periodo se analizó la .ipa y la .apk debido a un cambio 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)**	✓
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**	✓
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**	✓
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	✓
		Zillya	✓
		ZoneAlarm by Check Point	✓
		Zoner	✓

13 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 3 vulnerabilidades que afectan a la implementación de SSL/TLS, la primera de **BREACH** (CVE-2013-3587) el cual puede facilitar a la inyección parcial de texto, la segunda es de **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

- http://www.isg.rhul.ac.uk/tls/
- https://raymii.org/s/tutorials/Strong_SSL_Security_On_nginx.html
- https://cipherli.st/

14 Anexos

#	Archivo	SHA256SUM
1	IOS20190411.pcap	a8c53843639227e88cfcca141969f94ee97da745af232ee181316038522b9b79