Dirigido a:
Eduardo Parraguez
khipu

MAYO
2020

INFORME TÉCNICO

Análisis de Tráfico de Datos Mayo 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
09-06-2020	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.

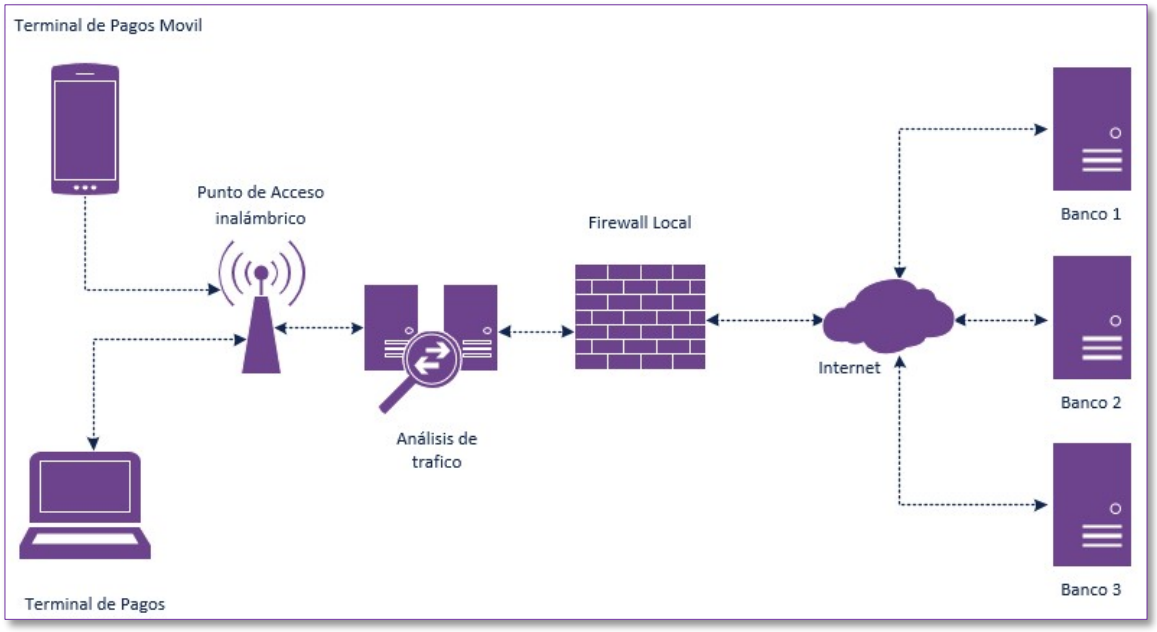
El presente análisis consiste en el monitoreo y análisis de todo el tráfico que genera la aplicación para las distintas plataformas, con el fin de detectar conexiones sospechosas. La revisión incluye la versión del terminal de pagos disponible para IOS y Android.

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 se registraron cambios para la aplicación de **iOS** en su versión y su **Hash**.

Plataforma	Versión	SHA256SUM
Android	7.5.12- Ultima Actualización 15/05/2020	464d1a1529dcea4e475d9354f2effa895e715ce374abfe4332c4c5ff27c71136
iOS	**7.21 - Ultima Actualización 28/05/2020**	**64266b4a3d9c6b5f50c1e246d8b3e44ece2722e9560f80468faa348ee8ea2526**

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

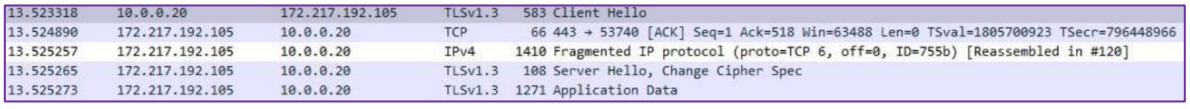
Como se puede ver en las siguientes tablas el tráfico que se genera al utilizar la aplicación de khipu solo se realiza con servidores confiables mediante canales seguros.

7.1 IPA

Origen	Destino	Tipo de Tráfico	Descripción
10.0.0.20	52.116.25.250	TLSv1.2	khipu
10.0.0.20	172.217.192.105	TLSv1.3	Banco Santander
10.0.0.20	104.16.12.14	TLSv1.2	Banco BICE
10.0.0.20	200.11.88.42	TLSv1.2	Banco ITAU

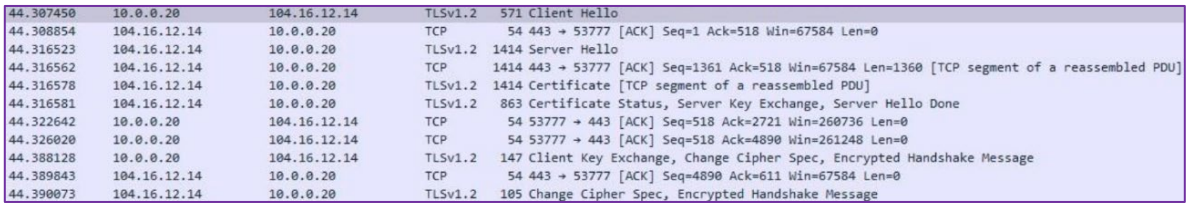
7.2 Tráfico TLS (seguro) entre el terminal de pagos y Banco “Santander”

IPA



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

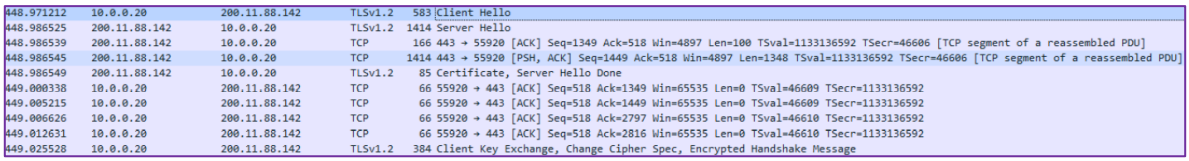
IPA



44.307450	10.0.0.20	104.16.12.14	TLSv1.2	571	Client Hello
44.308854	104.16.12.14	10.0.0.20	TCP	54	443 → 53777 [ACK] Seq=1 Ack=518 Win=67584 Len=0
44.316523	104.16.12.14	10.0.0.20	TLSv1.2	1414	Server Hello
44.316562	104.16.12.14	10.0.0.20	TCP	1414	443 → 53777 [ACK] Seq=1361 Ack=518 Win=67584 Len=1360 [TCP segment of a reassembled PDU]
44.316578	104.16.12.14	10.0.0.20	TLSv1.2	1414	Certificate [TCP segment of a reassembled PDU]
44.316581	104.16.12.14	10.0.0.20	TLSv1.2	863	Certificate Status, Server Key Exchange, Server Hello Done
44.322642	10.0.0.20	104.16.12.14	TCP	54	53777 → 443 [ACK] Seq=518 Ack=2721 Win=260736 Len=0
44.326020	10.0.0.20	104.16.12.14	TCP	54	53777 → 443 [ACK] Seq=518 Ack=4890 Win=261248 Len=0
44.388128	10.0.0.20	104.16.12.14	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
44.389843	104.16.12.14	10.0.0.20	TCP	54	443 → 53777 [ACK] Seq=4890 Ack=611 Win=67584 Len=0
44.390073	104.16.12.14	10.0.0.20	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message

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

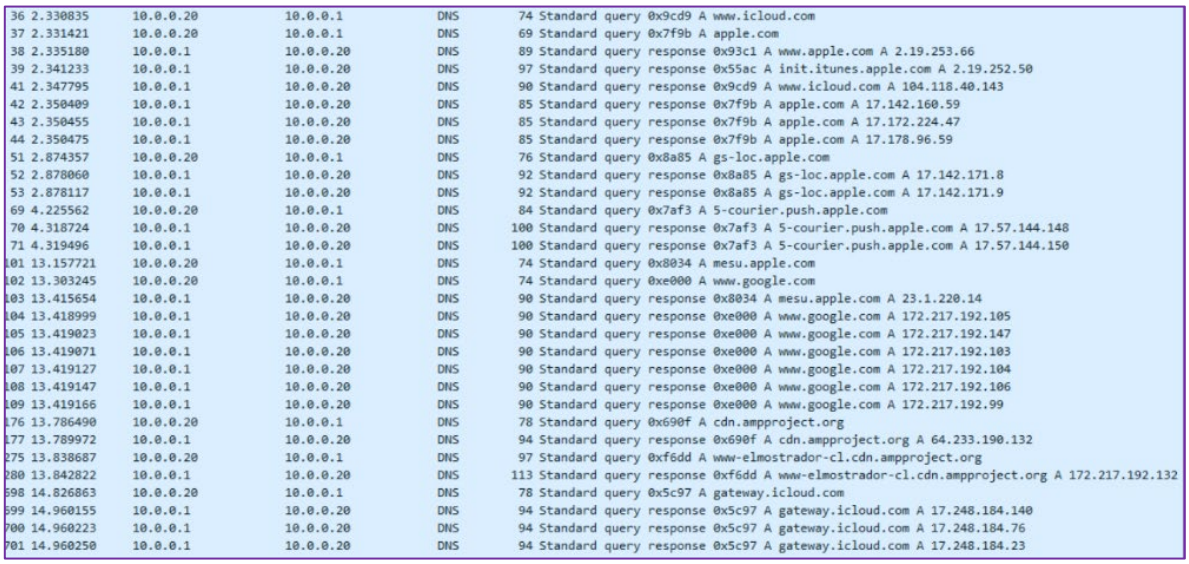
IPA



448.971212	10.0.0.20	200.11.88.142	TLSv1.2	583	Client Hello
448.986525	200.11.88.142	10.0.0.20	TLSv1.2	1414	Server Hello
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]
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]
448.986549	200.11.88.142	10.0.0.20	TLSv1.2	85	Certificate, Server Hello Done
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
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
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
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
449.025528	10.0.0.20	200.11.88.142	TLSv1.2	384	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

Tráfico DNS

IPA



```
36 2.330835     10.0.0.20       10.0.0.1        DNS      74 Standard query 0x9cd9 A www.icloud.com
37 2.331421     10.0.0.20       10.0.0.1        DNS      69 Standard query 0x7f9b A apple.com
38 2.335180     10.0.0.1        10.0.0.20       DNS      89 Standard query response 0x93c1 A www.apple.com A 2.19.253.66
39 2.341233     10.0.0.1        10.0.0.20       DNS      97 Standard query response 0x55ac A init.itunes.apple.com A 2.19.252.50
41 2.347795     10.0.0.1        10.0.0.20       DNS      90 Standard query response 0x9cd9 A www.icloud.com A 104.118.40.143
42 2.350409     10.0.0.1        10.0.0.20       DNS      85 Standard query response 0x7f9b A apple.com A 17.142.160.59
43 2.350455     10.0.0.1        10.0.0.20       DNS      85 Standard query response 0x7f9b A apple.com A 17.172.224.47
44 2.350475     10.0.0.1        10.0.0.20       DNS      85 Standard query response 0x7f9b A apple.com A 17.178.96.59
51 2.874357     10.0.0.20       10.0.0.1        DNS      76 Standard query 0x8a85 A gs-loc.apple.com
52 2.878060     10.0.0.1        10.0.0.20       DNS      92 Standard query response 0x8a85 A gs-loc.apple.com A 17.142.171.8
53 2.878117     10.0.0.1        10.0.0.20       DNS      92 Standard query response 0x8a85 A gs-loc.apple.com A 17.142.171.9
69 4.225562     10.0.0.20       10.0.0.1        DNS      84 Standard query 0x7af3 A 5-courier.push.apple.com
70 4.318724     10.0.0.1        10.0.0.20       DNS     100 Standard query response 0x7af3 A 5-courier.push.apple.com A 17.57.144.148
71 4.319496     10.0.0.1        10.0.0.20       DNS     100 Standard query response 0x7af3 A 5-courier.push.apple.com A 17.57.144.150
101 13.157721   10.0.0.20       10.0.0.1        DNS      74 Standard query 0x8034 A mesu.apple.com
102 13.303245   10.0.0.20       10.0.0.1        DNS      74 Standard query 0xe000 A www.google.com
103 13.415654   10.0.0.1        10.0.0.20       DNS      90 Standard query response 0x8034 A mesu.apple.com A 23.1.220.14
104 13.418999   10.0.0.1        10.0.0.20       DNS      90 Standard query response 0xe000 A www.google.com A 172.217.192.105
105 13.419023   10.0.0.1        10.0.0.20       DNS      90 Standard query response 0xe000 A www.google.com A 172.217.192.147
106 13.419071   10.0.0.1        10.0.0.20       DNS      90 Standard query response 0xe000 A www.google.com A 172.217.192.103
107 13.419127   10.0.0.1        10.0.0.20       DNS      90 Standard query response 0xe000 A www.google.com A 172.217.192.104
108 13.419147   10.0.0.1        10.0.0.20       DNS      90 Standard query response 0xe000 A www.google.com A 172.217.192.106
109 13.419166   10.0.0.1        10.0.0.20       DNS      90 Standard query response 0xe000 A www.google.com A 172.217.192.99
176 13.786490   10.0.0.20       10.0.0.1        DNS      78 Standard query 0x690f A cdn.ampproject.org
177 13.789972   10.0.0.1        10.0.0.20       DNS      94 Standard query response 0x690f A cdn.ampproject.org A 64.233.190.132
275 13.838687   10.0.0.20       10.0.0.1        DNS      97 Standard query 0xf6dd A www-elmostrador-cl.cdn.ampproject.org
280 13.842822   10.0.0.1        10.0.0.20       DNS     113 Standard query response 0xf6dd A www-elmostrador-cl.cdn.ampproject.org A 172.217.192.132
698 14.826863   10.0.0.20       10.0.0.1        DNS      78 Standard query 0x5c97 A gateway.icloud.com
699 14.960155   10.0.0.1        10.0.0.20       DNS      94 Standard query response 0x5c97 A gateway.icloud.com A 17.248.184.140
700 14.960223   10.0.0.1        10.0.0.20       DNS      94 Standard query response 0x5c97 A gateway.icloud.com A 17.248.184.76
701 14.960250   10.0.0.1        10.0.0.20       DNS      94 Standard query response 0x5c97 A gateway.icloud.com A 17.248.184.23
```

Tráfico HTTP

IPA

No se detectó tráfico HTTP durante el periodo de mayo.

Otro Tráfico

IPA

1	0.000000	Apple_db:b7:8d	Broadcast	ARP	42 Who has 10.0.0.20? (ARP Probe)
2	0.000010	Apple_db:b7:8d	Broadcast	ARP	42 Who has 10.0.0.20? (ARP Probe)
3	0.346945	Apple_db:b7:8d	Broadcast	ARP	42 Who has 10.0.0.20? (ARP Probe)
4	0.346954	Apple_db:b7:8d	Broadcast	ARP	42 Who has 10.0.0.20? (ARP Probe)
5	0.703365	Apple_db:b7:8d	Broadcast	ARP	42 Who has 10.0.0.20? (ARP Probe)
6	0.703392	Apple_db:b7:8d	Broadcast	ARP	42 Who has 10.0.0.20? (ARP Probe)
7	1.062550	Apple_db:b7:8d	Broadcast	ARP	42 ARP Announcement for 10.0.0.20
8	1.062561	Apple_db:b7:8d	Broadcast	ARP	42 ARP Announcement for 10.0.0.20
9	1.294145	Apple_db:b7:8d	Broadcast	ARP	42 ARP Announcement for 10.0.0.20
10	1.294156	Apple_db:b7:8d	Broadcast	ARP	42 ARP Announcement for 10.0.0.20
11	1.615555	Apple_db:b7:8d	Broadcast	ARP	42 ARP Announcement for 10.0.0.20
12	1.615567	Apple_db:b7:8d	Broadcast	ARP	42 ARP Announcement for 10.0.0.20
13	1.619434	Apple_db:b7:8d	Broadcast	ARP	42 Who has 10.0.0.1? Tell 10.0.0.20
14	1.619444	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42 10.0.0.1 is at bc:f6:85:21:26:0b
15	1.619449	Apple_db:b7:8d	Broadcast	ARP	42 Who has 10.0.0.1? Tell 10.0.0.20
18	1.791336	Apple_db:b7:8d	Broadcast	ARP	42 Who has 10.0.0.1? Tell 10.0.0.20
19	1.791346	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42 10.0.0.1 is at bc:f6:85:21:26:0b
20	1.791351	Apple_db:b7:8d	Broadcast	ARP	42 Who has 10.0.0.1? Tell 10.0.0.20
240	34.845192	D-LinkIn_21:26:0b	Apple_db:b7:8d	ARP	42 Who has 10.0.0.20? Tell 10.0.0.1

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

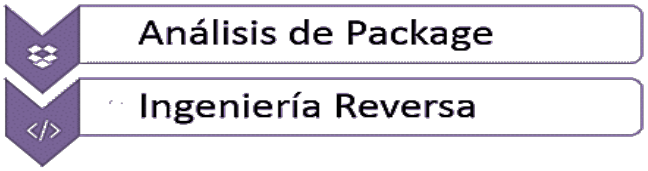
Se detectó 1 potencial vulnerabilidad en la implementación de SSL/TLS del sitio khipu.com la que afecta la confidencialidad de la información, sin embargo, esta vulnerabilidad tiene un alto grado de dificultad de explotación y se requieren condiciones especiales para su reproducción.

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 IPA

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

Nombre	khipu7.21.ipa
SHA256	64266b4a3d9c6b5f50c1e246d8b3e44ece2722e9560f80468faa348ee8ea2526
Tamaño	21.45 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.

12 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).

IPA	
Motor	**Estado**
Ad-Aware	✓
AegisLab	✓
AhnLab-V3	✓
Alibaba	✓
ALYac	✓
Antiy-AVL	✓
Arcabit	✓
Avast	✓
Avast-Mobile	✓
AVG	✓
Avira (no cloud)	✓

IPA	
Baidu	✓
BitDefender	✓
BitDefenderTheta	✓
Bkav	✓
CAT-QuickHeal	✓
ClamAV	✓
Comodo	✓
Cynet	✓
Cyren	✓
DrWeb	✓
Emsisoft	✓
eScan	✓
ESET-NOD32	✓
F-Prot	✓
F-Secure	✓
FireEye	✓

IPA	
Fortinet	✓
GData	✓
Ikarus	✓
Jiangmin	✓
K7AntiVirus	✓
K7GW	✓
Kaspersky	✓
Kingsoft	✓
Malwarebytes	✓
MAX	✓
MaxSecure	✓
McAfee	✓
McAfee-GW-Edition	✓
Microsoft	✓
NANO-Antivirus	✓
Panda	✓

IPA	
Qihoo-360	✓
Rising	✓
Sangfor Engine Zero	✓
SentinelOne (Static ML)	✓
Sophos AV	✓
SUPERAntiSpyware	✓
Symantec	✓
TACHYON	✓
Tencent	✓
TrendMicro	✓
TrendMicro-HouseCall	✓
VBA32	✓
VIPRE	✓
ViRobot	✓

IPA	
Yandex	✓
Zillya	✓
ZoneAlarm by Check Point	✓
Zoner	✓
Acronis	✓

13 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/