Dirigido a:
Eduardo Parraguez
khipu

AGOSTO
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
06-08-2018	Kevin Möller	1.0	Creación del documento
08-08-2018	Kevin Möller	1.0	Documentación
09-08-2018	Diego Zamorano	1.1	Revisión

Tabla de contenido

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.

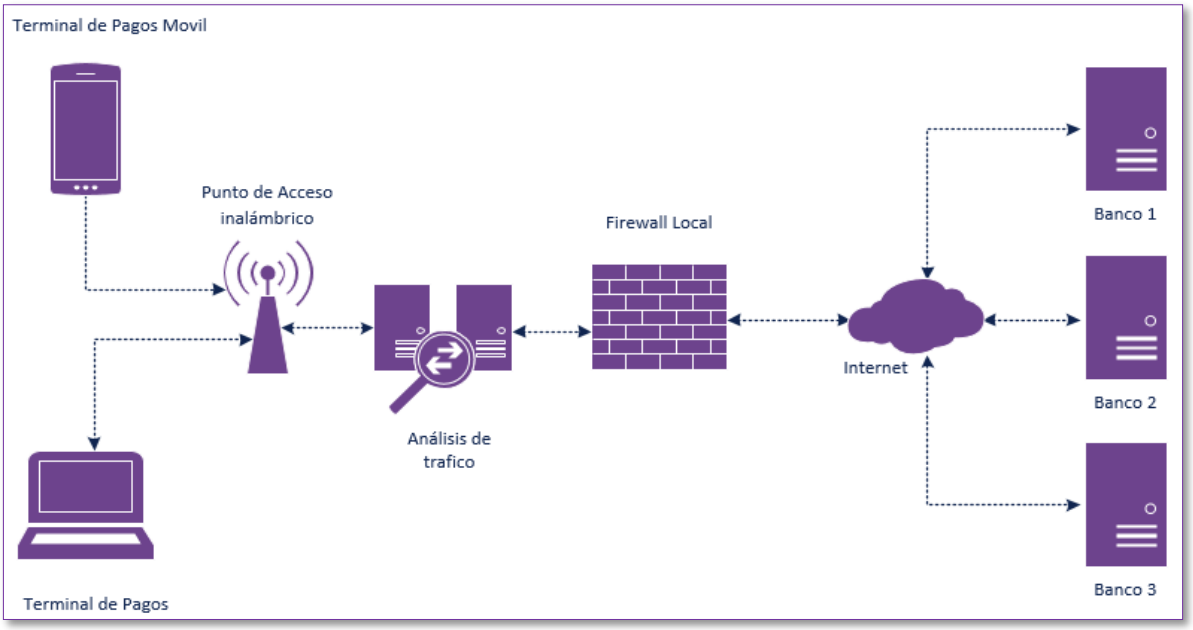
Esta revisión incluye la versión del terminal de pagos disponible para iOS.

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 móvil 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

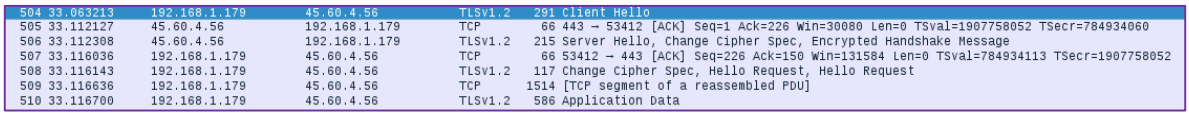
Para el actual periodo se registraron cambios para las aplicaciones de **iOS,** se observaron cambios en su HASH.

Plataforma	Versión	SHA256SUM
Android	6.6.33	a8ff742eb5b82d87cde85a4bf94c298100ef4eebc61dfbbec069a86340f0b4c8
iOS	**6.24**	**442f1a527541c7b7d29fd5965d96c8426f0302fe145e1acfaf0094659cc994f9**
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

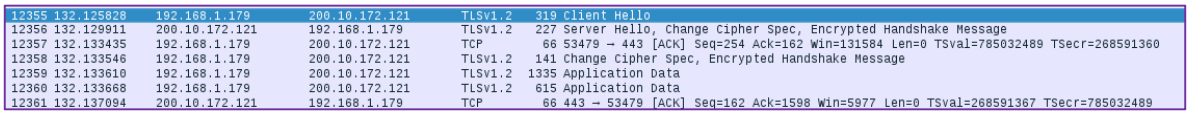
Todo el tráfico analizado entre el terminal de pagos y los bancos se estableció mediante un **canal seguro** de comunicación. Si bien se detectó tráfico no seguro (http) este corresponde a la validación del estado de los certificados SSL de algunos sitios, mediante OCSP y no durante la interacción con 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 “Chile”



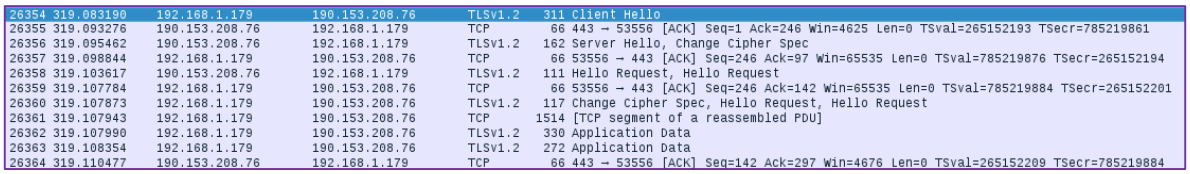
504	33.063213	192.168.1.179	45.60.4.56	TLSv1.2	291 Client Hello
505	33.112127	45.60.4.56	192.168.1.179	TCP	66 443 → 53412 [ACK] Seq=1 Ack=226 Win=30080 Len=0 TSval=1907758052 TSecr=784934060
506	33.112308	45.60.4.56	192.168.1.179	TLSv1.2	215 Server Hello, Change Cipher Spec, Encrypted Handshake Message
507	33.116036	192.168.1.179	45.60.4.56	TCP	66 53412 → 443 [ACK] Seq=226 Ack=150 Win=131584 Len=0 TSval=784934113 TSecr=1907758052
508	33.116143	192.168.1.179	45.60.4.56	TLSv1.2	117 Change Cipher Spec, Hello Request, Hello Request
509	33.116636	192.168.1.179	45.60.4.56	TCP	1514 [TCP segment of a reassembled PDU]
510	33.116700	192.168.1.179	45.60.4.56	TLSv1.2	586 Application Data

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



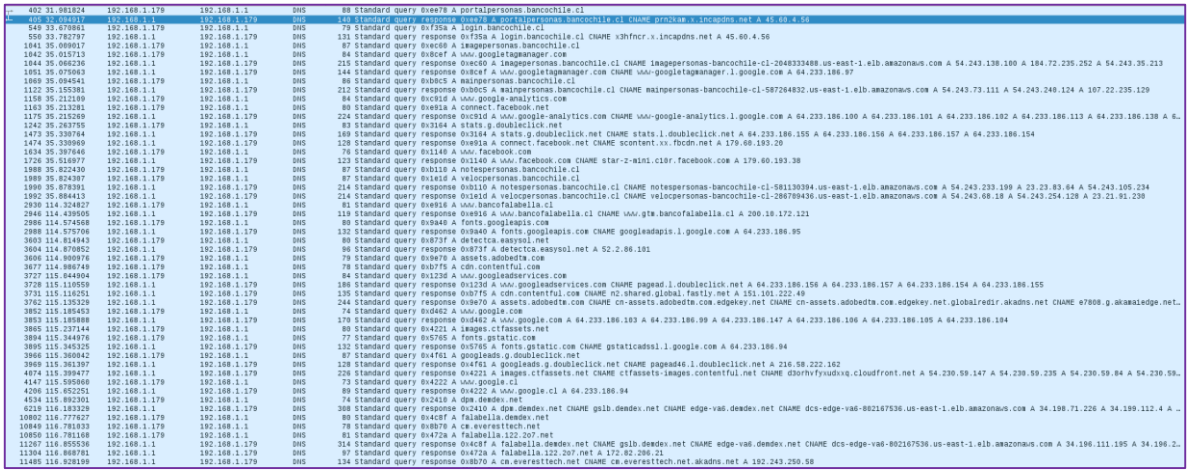
12355	132.125828	192.168.1.179	200.10.172.121	TLSv1.2	319 Client Hello
12356	132.129911	200.10.172.121	192.168.1.179	TLSv1.2	227 Server Hello, Change Cipher Spec, Encrypted Handshake Message
12357	132.133435	192.168.1.179	200.10.172.121	TCP	66 53479 → 443 [ACK] Seq=254 Ack=162 Win=131584 Len=0 TSval=785032489 TSecr=268591360
12358	132.133546	192.168.1.179	200.10.172.121	TLSv1.2	141 Change Cipher Spec, Encrypted Handshake Message
12359	132.133610	192.168.1.179	200.10.172.121	TLSv1.2	1335 Application Data
12360	132.133668	192.168.1.179	200.10.172.121	TLSv1.2	615 Application Data
12361	132.137094	200.10.172.121	192.168.1.179	TCP	66 443 → 53479 [ACK] Seq=162 Ack=1598 Win=5977 Len=0 TSval=268591367 TSecr=785032489

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



26354	319.083190	192.168.1.179	190.153.208.76	TLSv1.2	311 Client Hello
26355	319.093276	190.153.208.76	192.168.1.179	TCP	66 443 → 53556 [ACK] Seq=1 Ack=246 Win=4625 Len=0 TSval=265152193 TSecr=785219861
26356	319.095462	190.153.208.76	192.168.1.179	TLSv1.2	162 Server Hello, Change Cipher Spec
26357	319.098844	192.168.1.179	190.153.208.76	TCP	66 53556 → 443 [ACK] Seq=246 Ack=97 Win=65535 Len=0 TSval=785219876 TSecr=265152194
26358	319.103617	190.153.208.76	192.168.1.179	TLSv1.2	111 Hello Request, Hello Request
26359	319.107784	192.168.1.179	190.153.208.76	TCP	66 53556 → 443 [ACK] Seq=246 Ack=142 Win=65535 Len=0 TSval=785219884 TSecr=265152201
26360	319.107873	192.168.1.179	190.153.208.76	TLSv1.2	117 Change Cipher Spec, Hello Request, Hello Request
26361	319.107943	192.168.1.179	190.153.208.76	TCP	1514 [TCP segment of a reassembled PDU]
26362	319.107990	192.168.1.179	190.153.208.76	TLSv1.2	330 Application Data
26363	319.108354	192.168.1.179	190.153.208.76	TLSv1.2	272 Application Data
26364	319.110477	190.153.208.76	192.168.1.179	TCP	66 443 → 53556 [ACK] Seq=142 Ack=297 Win=4676 Len=0 TSval=265152209 TSecr=785219884

6.4 Tráfico DNS



6.5 Tráfico HTTP

No se detectó trafico http durante este análisis.

6.6 Otro Tráfico

No.	Time	Source	Destination	Protocol	Length	Info
45	14.736701	20:ee:28:db:b7:8d	Tp-LinkT_df:10:c8	ARP	42	Who has 192.168.1.1? Tell 192.168.1.179
46	14.736785	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
90	20.802563	Tp-LinkT_df:10:c8	20:ee:28:db:b7:8d	ARP	42	Who has 192.168.1.179? Tell 192.168.1.1
91	20.915632	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
2387	53.872542	Tp-LinkT_df:10:c8	20:ee:28:db:b7:8d	ARP	42	Who has 192.168.1.179? Tell 192.168.1.1
2388	53.888526	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
2755	87.562588	Tp-LinkT_df:10:c8	20:ee:28:db:b7:8d	ARP	42	Who has 192.168.1.179? Tell 192.168.1.1
2756	87.578614	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
2796	104.743420	20:ee:28:db:b7:8d	Tp-LinkT_df:10:c8	ARP	42	Who has 192.168.1.1? Tell 192.168.1.179
2797	104.743482	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
13051	150.172559	Tp-LinkT_df:10:c8	20:ee:28:db:b7:8d	ARP	42	Who has 192.168.1.179? Tell 192.168.1.1
13052	150.255097	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
23780	194.750052	20:ee:28:db:b7:8d	Tp-LinkT_df:10:c8	ARP	42	Who has 192.168.1.1? Tell 192.168.1.179
23781	194.750115	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
23886	201.482566	Tp-LinkT_df:10:c8	20:ee:28:db:b7:8d	ARP	42	Who has 192.168.1.179? Tell 192.168.1.1
23887	201.552481	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
26012	276.532563	Tp-LinkT_df:10:c8	20:ee:28:db:b7:8d	ARP	42	Who has 192.168.1.179? Tell 192.168.1.1
26013	276.612869	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
26046	284.756021	20:ee:28:db:b7:8d	Tp-LinkT_df:10:c8	ARP	42	Who has 192.168.1.1? Tell 192.168.1.179
26047	284.756084	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
26471	325.692547	Tp-LinkT_df:10:c8	20:ee:28:db:b7:8d	ARP	42	Who has 192.168.1.179? Tell 192.168.1.1
26472	325.765751	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	45.60.4.56	TLSv1.2	Banco Chile
192.168.1. 179	20.10.172.101	TLSv1.2	Banco Falabella
192.168.1. 179	190.153.208.76	TLSv1.2	Banco Itaú

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

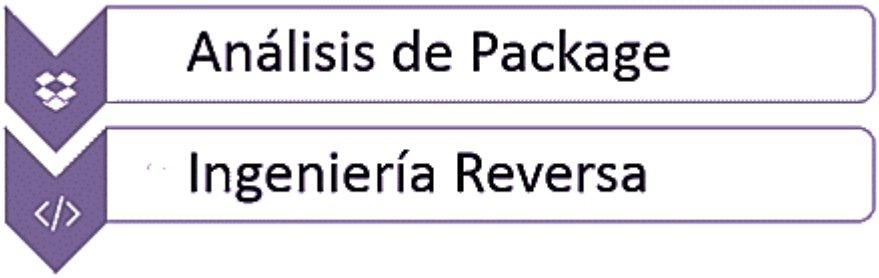
Se detectaron 2 vulnerabilidades en la implementación de SSL/TLS del sitio khipu.com las que afectan la confidencialidad de la información, sin embargo, estas vulnerabilidades tienen un alto grado de dificultad de explotación y se requieren condiciones especiales para su correcta explotación.

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 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	Khipu6.24.ipa
SHA256	442f1a527541c7b7d29fd5965d96c8426f0302fe145e1acfaf0094659cc994f9
Tamaño	10.8 MB
Tipo	iOS
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 .ipa debido a un cambio en su hash.

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
1	khipuiOS08082018.cap	47e83d73d9cedb075d04cb6433bac0a075014 6dd8f1168ca003a8ba375e9cd95