Informe Técnico

Análisis de tráfico de datos

khipu

08-02-2017

Contenido

Control de versiones

El siguiente cuadro muestra el historial de cambios sobre el presente documento.

Fecha	Versión	Autor	Cambio
08-02-2017	0.1	Diego Zamorano	Creación del documento

1. Introducción

La aplicación khipu permite a las 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 uso de páginas correctas 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 los datos de sus usuarios tales como cuenta corriente, clave, etc, a servidores propios ni a terceros.

Mediante esta auditoría y análisis de tráfico se busca certificar que los datos de los usuarios no son compartidos con 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 las versiones del terminal de pagos disponible para Windows, OSX, Linux, iOS y Android

2. Objetivo

Certificar que khipu no recibe las claves bancarias de sus usuarios ni las comparte con terceros.

3. Ámbito

Para el actual periodo se registraron cambios en la aplicación para Android e iOS.

Plataforma	Versión	Hash MD5
Android	**6.1.4**	**0351ab98e63142c0302eec69d10bc293**
iOS	**6.8**	**fc0ca917089b830f5624ab95bf2ae386**
Linux i386	1.16.1923.1	7e6704435581c5bfb44e25c7ce3e36ed
Linux x64	1.16.1923.1	852afd6a4094da6b748857a641f8ed67
OSX	1.16.2020.1	9c4f52fdfb0747ad685d813097584330
Windows	1.16.1122.1	53f6300bf769a67e191519a5acfe1d23

3.1 Android

Origen	Destino	Tipo de Tráfico	Descripción
10.0.0.203	50.22.89.18	TLS v1.2	Sitio web khipu
10.0.0.203	200.9.111.205	TLS v1.2	Sitio web BBVA
10.0.0.203	200.0.160.105	TLS v1.2	Sitio web CorpBanca
10.0.0.203	104.114.253.235	TLS v1.2	Sitio web Banco Santander

3.2 iOS

Origen	Destino	Tipo de Tráfico	Descripción
10.0.0.9	50.22.89.18	TLS v1.2	Sitio web khipu
10.0.0.9	200.9.111.205	TLS v1.2	Sitio web BBVA
10.0.0.9	200.0.160.105	TLS v1.2	Sitio web CorpBanca
10.0.0.9	104.114.253.235	TLS 1.2	Sitio web Banco Santander

4. Análisis SSL

El siguiente análisis tiene como objetivo determinar el nivel de seguridad en la implementación de SSL/TLS, se realizaran pruebas para determinar si se ve afectado por las vulnerabilidades conocidas hasta el momento

4.1 khipu.com – 50.22.89.18

Host / IP / Puerto	khipu.com / 50.22.89.18 / 443
Expiración	**24 / 03 / 2017**
Válido para	www.khipu.com khipu.com
Información Adicional	commonName=khipu.com organizationalUnitName=COMODO EV SGC SSL organizationalUnitName=Hosted by MACROSEGURIDAD.ORG CORPORATION organizationName=Khipu SpA streetAddress=Las Urbinas 53 of 132 localityName=Santiago

Vulnerabilidades Conocidas									
HEARTBLEED	BREACH	POODLE	FREAK	LOGJAM	BEAST	RC4	SLOTH	DROWN	Padding Oracle
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

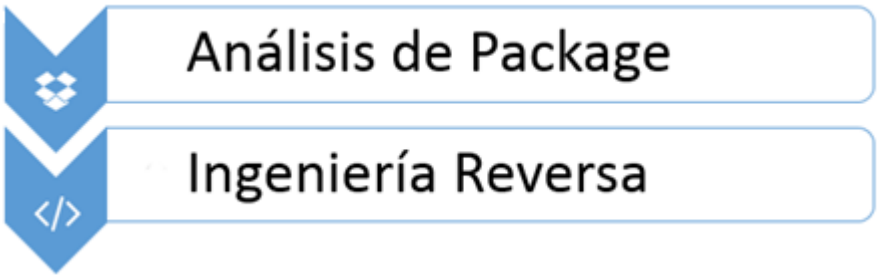
La implementación de SSL/TLS se encuentra con un nivel óptimo de seguridad para el sitio khipu.com y no se encuentra afectado por las vulnerabilidades conocidas hasta el momento de SSL/TLS.

4.1.1 Referencias

Heartbleed	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
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

5. 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 caso de Android se analiza el archivo APK y 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.

5.1 Análisis APK

El resultado del análisis para la aplicación móvil es el siguiente

Nombre	com.khipu.android
MD5	0351ab98e63142c0302eec69d10bc293
SHA1	27a507ad9027c774c4ac5ef03c8b2ede34d49e6a
SHA256	72cbab76d69fc43163836ed5bc3fd056cd5ce7ee30cb71a72844cc0ea116bd48
Tamaño	4.7 MB
Tipo	Android
URLs Interesantes	5
IPs encontradas	0
Emails encontrados	0

5.1.1 URLs detectadas

1. https://khipu.com/payment/simplified/
2. https://khipu.com/payment/show/
3. https://khipu.com/payment/end/
4. **https://khipu.com/cerebro/**
5. https://khipu.com/app/2.0/automaton

La cuarta URL tiene un formulario de autenticación al cual se le realizó un ataque de fuerza bruta con un diccionario simple de 1.000.000 de palabras, sin embargo, no se logró obtener ninguna credencial para acceder al sistema. Se recomienda agregar un método de protección para prevenir ataques de fuerza bruta sobre el formulario.

5.1.2 Direcciones IPs detectadas

No se encontraron direcciones IP en el análisis

5.1.3 Emails detectados

No se encontraron emails en el análisis

5.2 Análisis IPA

El resultado del análisis para la aplicación móvil es la siguiente

Nombre	com.khipu.ios.Khipu
MD5	fc0ca917089b830f5624ab95bf2ae386
SHA1	a31234ced4be40a1de8c797268c8f780fb9f394b
SHA256	83bf655d0ceefdb09297b90e7ebe268f8071d7479ec352dbe58b77f09263ad93
Tamaño	13.4 MB
Tipo	iPhone
URLs Interesantes	0
IPs detectadas	0
Emails detectados	0

5.2.1 URL detectadas

No se encontraron direcciones IP en el análisis

5.2.2 Direcciones IPs detectadas

No se encontraron direcciones IP en el análisis

5.2.3 Emails detectados

No se encontraron emails en el análisis

5.3 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. Adicionalmente se revisaron los permisos que solicita la aplicación al momento de ser instalada.

Antivirus	Android	iOS	Actualización
ALYac	✓	✓	20170207
AVG	✓	✓	20170207
AVware	✓	✓	20170207
Ad-Aware	✓	✓	20170207
AegisLab	✓	✓	20170207
AhnLab-V3	✓	✓	20170207
Alibaba	✓	✓	20170122
Antiy-AVL	✓	✓	20170207
Arcabit	✓	✓	20170207
Avast	✓	✓	20170207
Avira (no cloud)	✓	✓	20170207
Baidu	✓	✓	20170207
BitDefender	✓	✓	20170207
Bkav	✓	✓	20170207
CAT-QuickHeal	✓	✓	20170207
CMC	✓	✓	20170207
ClamAV	✓	✓	20170207
Comodo	✓	✓	20170207
CrowdStrike Falcon (ML)	N/A	N/A	20170130
Cyren	✓	✓	20170207
DrWeb	✓	✓	20170207
ESET-NOD32	✓	✓	20170207
Emsisoft	✓	✓	20170207
F-Prot	✓	✓	20170207
F-Secure	✓	✓	20170207
Fortinet	✓	✓	20170207
GData	✓	✓	20170207
Ikarus	✓	✓	20170207
Invincea	N/A	N/A	20170203

Jiangmin	✓	✓	20170207
K7AntiVirus	✓	✓	20170207
K7GW	✓	✓	20170207
Kaspersky	✓	✓	20170207
Kingsoft	✓	✓	20170207
Malwarebytes	✓	✓	20170207
McAfee	✓	✓	20170207
McAfee-GW-Edition	✓	✓	20170207
eScan	✓	✓	20170207
Microsoft	✓	✓	20170207
NANO-Antivirus	✓	✓	20170207
Panda	✓	✓	20170207
Qihoo-360	✓	✓	20170207
Rising	✓	✓	20170207
SUPERAntiSpyware	✓	✓	20170207
Sophos	✓	✓	20170207
Symantec	✓	✓	20170207
Tencent	✓	✓	20170207
TheHacker	✓	✓	20170205
TrendMicro	✓	✓	20170207
TrendMicro-HouseCall	✓	✓	20170207
Trustlook	N/A	N/A	20170207
VBA32	✓	✓	20170207
VIPRE	✓	✓	20170207
ViRobot	✓	✓	20170207
WhiteArmor	✓	✓	20170202
Yandex	✓	✓	20170206
Zillya	✓	✓	20170207
Zoner	✓	✓	20170207
nProtect	✓	✓	20170207

6. Vulnerabilidades declaradas

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

No se reportaron vulnerabilidades para este periodo

7. Anexos

#	Archivo	MD5
1	Android_Febrero.pcap	1f3e6a9ae04d4848f99ce68a11f0046e
2	iOS_Febrero.pcap	818b0900b1b57a59bab59b816e830bcf