Informe Técnico

Análisis de tráfico de datos

khipu

13-01-2017

Contenido

Control de versiones

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

Fecha	Versión	Autor	Cambio
08-01-2017	0.1	Diego Zamorano	Creación del documento
09-01-2017	1.0	Fernando Lagos	Revisión general
13-01-2017	1.1	Hernán Möller	Análisis de Malware

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 **no se registraron cambios** para todas las aplicaciones.

Plataforma	Versión	Hash MD5
Android	5.1.5	619f7fffa5d19531a98372e5e913bfb8
iOS	6.5	22a1f2bc7ff7a2e4fc3a72cb94d34d26
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

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
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

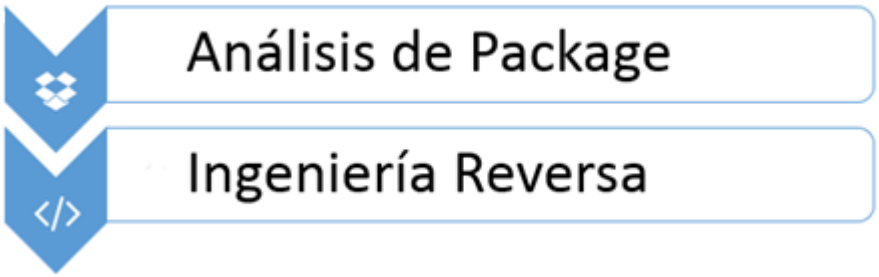
La implementación de SSL/TLS se encuentra con un nivel óptimo de seguridad para el sitio khipu.com y no se encuentra afectado por las vulnerabilidades conocidas hasta el momento de SSL/TLS.

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	9a771cdd2a47e643901a5d2eec129a7c
SHA1	1ab0df30764bb115ad4a6853439fbc30daedc19e
SHA256	866f7eb72835071ecd1dbedc49b235a13e01d7e7f7b6c5f59923f8069e5b4344
Tamaño	4.8MB
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	22a1f2bc7ff7a2e4fc3a72cb94d34d26
SHA1	d7ce19e3710cb3d40692843a10c435d616668de7
SHA256	ddd33412423df0e2850cd3b1458a0ae4c01aab5ce86a5de59629e98d17d6f7db
Tamaño	13.3 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	✓	✓	20170113
AVG	✓	✓	20170113
AVware	Sin información	✓	20170113
Ad-Aware	✓	✓	20170113
AegisLab	✓	✓	20170113
AhnLab-V3	✓	✓	20170113
Alibaba	✓	✓	20170113
Antiy-AVL	Sin información	✓	20170113
Arcabit	✓	✓	20170113
Avast	✓	✓	20170113
Avira (no cloud)	✓	✓	20170113
Baidu	✓	✓	20170113
BitDefender	✓	✓	20170113
Bkav	Sin información	Sin información	20170113
CAT-QuickHeal	✓	✓	20170113
CMC	✓	✓	20170113
ClamAV	✓	✓	20170113
Comodo	✓	✓	20170113
CrowdStrike Falcon (ML)	Sin información	Sin información	20161024
Cyren	✓	✓	20170113
DrWeb	Sin información	✓	20170113
ESET-NOD32	✓	✓	20170113
Emsisoft	✓	✓	20170113
F-Prot	✓	✓	20170113
F-Secure	Sin información	✓	20170113
Fortinet	✓	✓	20170113
GData	✓	✓	20170113
Ikarus	✓	✓	20170113
Invincea	Sin información	Sin información	20170111
Jiangmin	✓	✓	20170113

K7AntiVirus	✓	✓	20170113
K7GW	✓	✓	20170113
Kaspersky	✓	✓	20170113
Kingsoft	✓	✓	20170113
Malwarebytes	✓	✓	20170113
McAfee	Sin información	✓	20170108
McAfee-GW-Edition	Sin información	✓	20170113
eScan	✓	✓	20170113
Microsoft	Sin información	✓	20170113
NANO-Antivirus	Sin información	✓	20170113
Panda	✓	✓	20170112
Qihoo-360	✓	✓	20170113
Rising	✓	✓	20170113
SUPERAntiSpyware	✓	✓	20170113
Sophos	✓	✓	20170113
Symantec	✓	✓	20170112
Tencent	✓	✓	20170113
TheHacker	✓	✓	20170111
TrendMicro	✓	Sin información	20170113
TrendMicro-HouseCall	✓	✓	20170113
Trustlook	✓	Sin información	20170113
VBA32	✓	✓	20170113
VIPRE	Sin información	✓	20170113
ViRobot	✓	✓	20170113
WhiteArmor	✓	✓	20170111
Yandex	✓	✓	20170112
Zillya	✓	✓	20170113
Zoner	✓	✓	20170113
nProtect	✓	✓	20170113

6. Vulnerabilidades declaradas

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

#	Nombre	Descripción	Impacto

No se reportaron vulnerabilidades para este periodo

7. Anexos

#	Archivo	MD5