Informe Técnico

Análisis de tráfico de datos

khipu

10-06-2017

Contenido

Control de versiones

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

Fecha	Versión	Autor	Cambio
10-06-2017	1.0	Diego Zamorano	Creación del documento
12-06-2017	1.0	Fernando Lagos	Revisión General

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 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 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, IOS, Linux y OSX

Plataforma	Versión	Hash MD5
Android	**6.5.2**	**e9181c597cb197c61192d3694140fc33**
iOS	6.9.2	853d54aa80913a5fa08e770617a42566
Linux 32-bit	**1.17.1516.1**	**ca25d9af6027a1f6d8f519862e0b164d**
Linux 64-bit	**1.17.1516.1**	**d60fb0377da0f602dada1fc35a4a012b**
OSX	**1.17.1516.1**	**6b396d42dedc6dac8c773b7f48a965e9**
Windows	1.16.1122.1	53f6300bf769a67e191519a5acfe1d23

3.1 Android

Origen	Destino	Tipo de Tráfico	Descripción
1.1.1.2	50.22.89.18	TLS v1.2	Sitio web khipu
1.1.1.2	200.9.111.205	TLS v1.2	Sitio web BBVA
1.1.1.2	184.28.1.37	TLS v1.2	Sitio web Banco Santander
1.1.1.2	200.68.28.134	TLS v1.1	Sitio web TBanc

3.2 Linux 32-bit

No fue posible realizar la instalación debido a un error de dependencias, indica que necesita el paquete libqt5xmlpatterns y el disponible en el repositorio es libqt5xmlpatterns5

3.3 Linux 64-bit

No se pudieron realizar las pruebas debido a que la aplicación no abre al momento de realizar una transacción, el sitio web de khipu no la detecta como instalada.

3.4 OSX

Origen	Destino	Tipo de Tráfico	Descripción
1.1.1.4	50.22.89.18	TLS v1.2	Sitio web khipu
1.1.1.4	200.9.111.205	TLS v1.22	Sitio web BBVA
1.1.1.4	184.28.1.37	TLS v1.2	Sitio web Banco Santander
1.1.1.4	200.68.28.134	TLS v1.1	Sitio web TBanc

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	**23 / 03 / 2019**
Válido para	www.khipu.com khipu.com
Información Adicional	Nombre Comun=khipu.com Organizacion=Khipu SpA Unidad Organizacional = Hosted by MACROSEGURIDAD.ORG CORPORATION Direccion = Las Urbinas 53 of 132 Localidad=Santiago

Vulnerabilidad	Identificador	Estado	Observaciones
Heartbleed	CVE-2014-0160	✓	No vulnerable
CCS	CVE-2014-0224	✓	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

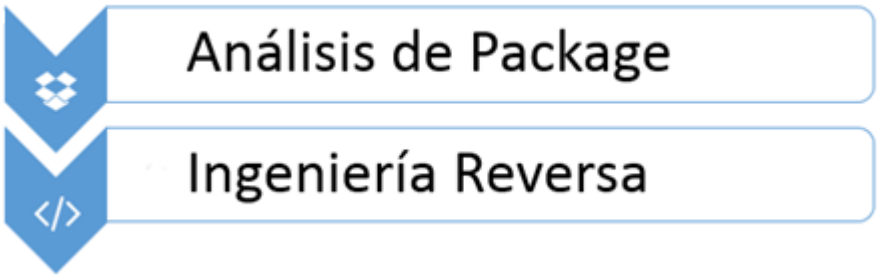
La implementación de SSL/TLS se encuentra con un nivel óptimo de seguridad para el sitio khipu.com y no se encuentra afectado por las vulnerabilidades conocidas hasta el momento de SSL/TLS.

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
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

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	e9181c597cb197c61192d3694140fc33
SHA1	18b3d85a7e50032d21a5517162c3ebf216783610
SHA256	033caf6c829d00a0000f69de59823dac4b8e22913498b9fe44f9a7527cdfb035
Tamaño	5.4 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 direcciones de correo en el análisis

Nombre	
MD5	La aplicación fue analizada en el periodo anterior
SHA1	
SHA256	
Tamaño	
Tipo	
URLs Interesantes	
IPs encontradas	
Emails encontrados	

5.1.4 URL detectadas

La aplicación fue analizada en el periodo anterior

5.1.5 Direcciones IPs detectadas

La aplicación fue analizada en el periodo anterior

5.1.6 Direcciones de correo detectados

La aplicación fue analizada en el periodo anterior

5.2 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.

Android		
Motor	20170611	**Estado**
Ad-Aware	20170611	✓
AegisLab	20170611	✓
AhnLab-V3	20170609	✓
Alibaba	20170611	✓
ALYac	20170611	✓
Antiy-AVL	20170611	✓
Arcabit	20170611	✓
Avast	20170611	✓
AVG	20170611	✓
Avira (no cloud)	20170611	✓
AVware	20170608	✓
Baidu	20170611	✓
BitDefender	20170610	✓
Bkav	20170610	✓
CAT-QuickHeal	20170611	✓
ClamAV	20170611	✓
CMC	20170611	✓
Comodo	20170420	✓
CrowdStrike Falcon (ML)	20170611	N/A
Cyren	20170611	✓
DrWeb	20170611	✓
Emsisoft	20170515	✓
Endgame	20170611	N/A
ESET-NOD32	20170611	✓
F-Prot	20170611	✓
F-Secure	20170611	✓
Fortinet	20170611	✓
GData	20170611	✓

Ikarus	20170607	✓
Invincea	20170611	N/A
Jiangmin	20170611	✓
K7AntiVirus	20170611	✓
K7GW	20170611	✓
Kaspersky	20170611	✓
Kingsoft	20170611	✓
Malwarebytes	20170611	✓
McAfee	20170611	✓
McAfee-GW-Edition	20170610	✓
Microsoft	20170611	✓
eScan	20170611	✓
NANO-Antivirus	20170611	✓
nProtect	20170611	✓
Palo Alto Networks (Known Signatures)	20170611	N/A
Panda	20170611	✓
Qihoo-360	20170611	✓
Rising	20170516	✓
SentinelOne (Static ML)	20170611	N/A
Sophos	20170611	✓
SUPERAntiSpyware	20170611	✓
Symantec	20170608	✓
Symantec Mobile Insight	20170611	✓
Tencent	20170611	✓
TheHacker	20170611	✓
TrendMicro	20170611	✓
TrendMicro-HouseCall	20170611	✓
Trustlook	20170609	✓
VBA32	20170611	✓
VIPRE	20170611	✓
ViRobot	20170611	✓
Webroot	20170608	✓
WhiteArmor	20170608	✓
Yandex	20170610	✓

Zillya	20170611	✓
ZoneAlarm by Check Point	20170611	✓

6. 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 mitigida al soportar la versión 1.1 y 1.2 de TLS, para corregirla es ideal 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 seria deshabilitar los cifrados que utilicen estos métodos y siempre tener la última versión estable de OpenSSL.

6.1 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/

7. Anexos

#	Archivo	MD5
1	android-062017.cap	99cf5bae0f23c45466635a192f05ed1b
2	OSX_062017.cap	84fcc5182c17af052e405febb3d9b4d4