Informe Técnico

Análisis de tráfico de datos

khipu

03-04-2017

Contenido

Control de versiones

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

Fecha	Versión	Autor	Cambio
03-04-2017	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 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

Plataforma	Versión	Hash MD5
Android	**6.1.7**	**8ac9e7f30087d8969b6e80c3442de0c8**
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
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	200.0.160.105	TLS v1.2	Sitio web Corpbanca
1.1.1.2	184.28.1.37	TLS v1.2	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	**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	✗	Vulnerable. Utiliza bloque de cifrado de 64 bits
FREAK	CVE-2015-0204	✓	No vulnerable
DROWN	CVE-2016-0703	✓	No vulnerable
LOGJAM	CVE-2015-4000	✓	No vulnerable
BEAST	CVE-2011-3389	✓	No vulnerable
LUCKY13	CVE-2013-0169	✗	Vulnerable. Utiliza “cipher-block chaining” (CBC)
RC4	CVE-2013-2566 CVE-2015-2808	✓	No vulnerable

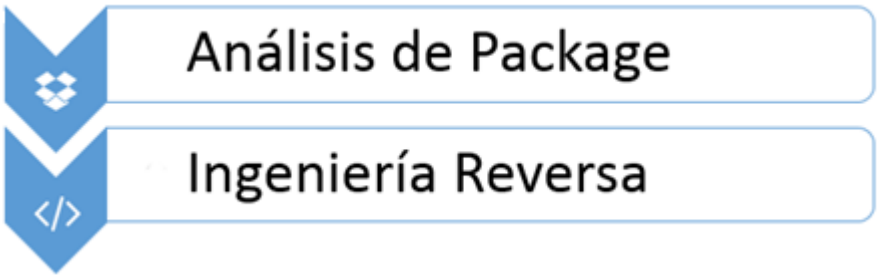
La implementación de SSL/TLS se encuentra con un nivel óptimo de seguridad para el sitio khipu.com y no se encuentra afectado por las vulnerabilidades conocidas hasta el momento de SSL/TLS.

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	8ac9e7f30087d8969b6e80c3442de0c8
SHA1	e63efb8c880920679a6d0a6a8699be5ad8c1f106
SHA256	33cef323ca31399441526160548e9942b27ae5a446c170ff6c44434b65c28064
Tamaño	4.8 MB
Tipo	Android
URLs Interesantes	5
IPs encontradas	0
Emails encontrados	2

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

Se encontraron 2 correos electrónicos dentro del archivo test.xml

transferencias@khipu.com

emilio.davis@khipu.com

5.1.4 Archivo sospechoso

Se encontró el archivo test.xml dentro de la aplicación al momento del análisis, este archivo contiene información de una transacción de prueba, se adjunta como anexo, este tipo de archivos deben ser eliminados antes de pasar a producción la aplicación

5.2 Análisis IPA

No se analizó la aplicación en este periodo

5.2.1 URL detectadas

No se analizó la aplicación en este periodo

5.2.2 Direcciones IPs detectadas

No se analizó la aplicación en este periodo

5.2.3 Emails detectados

No se analizó la aplicación en este periodo

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
Ad-Aware	✓	N/A
AegisLab	✓	N/A
AhnLab-V3	✓	N/A
Alibaba	✓	N/A
ALYac	✓	N/A
Antiy-AVL	✓	N/A
Arcabit	✓	N/A
Avast	✓	N/A
AVG	✓	N/A
Avira	✓	N/A
AVware	✓	N/A
Baidu	✓	N/A
BitDefender	✓	N/A
Bkav	✓	N/A
CAT-QuickHeal	✓	N/A
ClamAV	✓	N/A
CMC	✓	N/A
Comodo	✓	N/A
CrowdStrike Falcon	N/A	N/A
Cyren	✓	N/A
DrWeb	✓	N/A
Emsisoft	✓	N/A
Endgame	N/A	N/A
ESET-NOD32	✓	N/A
F-Prot	✓	N/A
F-Secure	✓	N/A
Fortinet	✓	N/A
GData	✓	N/A
Ikarus	✓	N/A

Invincea	N/A	N/A
Jiangmin	✓	N/A
K7AntiVirus	✓	N/A
K7GW	✓	N/A
Kaspersky	✓	N/A
Kingsoft	✓	N/A
Malwarebytes	✓	N/A
McAfee	✓	N/A
McAfee-GW-Edition	✓	N/A
Microsoft	✓	N/A
eScan	✓	N/A
NANO-Antivirus	✓	N/A
nProtect	✓	N/A
Palo Alto Networks	N/A	N/A
Panda	✓	N/A
Qihoo-360	✓	N/A
Rising	✓	N/A
SentinelOne	N/A	N/A
Sophos	✓	N/A
SUPERAntiSpyware	✓	N/A
Symantec	✓	N/A
Symantec	✓	N/A
Tencent	✓	N/A
TheHacker	✓	N/A
TrendMicro	✓	N/A
TrendMicro-HouseCall	✓	N/A
Trustlook	✓	N/A
VBA32	✓	N/A
VIPRE	✓	N/A
ViRobot	✓	N/A
Webroot	✓	N/A
WhiteArmor	✓	N/A
Yandex	✓	N/A
Zillya	✓	N/A
ZoneAlarm by Check Point	✓	N/A
Zoner	✓	N/A

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 **SWEET32** (CVE-2016-2183, CVE-2016-6329), esta vulnerabilidad afecta a los cifrados que utilizan bloques de 64 bit, como los **3DES**, por lo cual la mitigación para esta vulnerabilidad es desactivar el soporte para cifrados 3DES (usado por navegadores antiguos). 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_abril.cap	ba36856600d2a86de789a6a5c3559603
2	test.xml	0727e51036a8a46dcc1d2f0dd80dac83