Informe Técnico

Análisis de tráfico de datos

khipu

10-05-2017

Contenido

Control de versiones

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

Fecha	Versión	Autor	Cambio
10-05-2017	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, IOS y OSX

Plataforma	Versión	Hash MD5
Android	**6.2.2**	**7d9a8abe2ccd235c9a3b6c91ec237222**
iOS	**6.9.2**	**853d54aa80913a5fa08e770617a42566**
Linux i386	1.16.1923.1	7e6704435581c5bfb44e25c7ce3e36ed
Linux x64	1.16.1923.1	852afd6a4094da6b748857a641f8ed67
OSX	**1.17.1427.1**	**627a61a5f8cecc70e7a5b47c0cda07a0**
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	200.68.28.131	TLS v1.1	Sitio web BCI
1.1.1.2	200.29.162.187	TLS v1.2	Sitio web Banco Estado
1.1.1.2	184.28.1.191	TLS v1.2	Sitio web Scotiabank

3.2 IOS

Origen	Destino	Tipo de Tráfico	Descripción
1.1.1.3	50.22.89.18	TLS v1.2	Sitio web khipu
1.1.1.3	200.68.28.131	TLS v1.1	Sitio web BCI
1.1.1.3	200.29.162.187	TLS v1.2	Sitio web Banco Estado
1.1.1.3	184.28.1.191	TLS v1.2	Sitio web Scotiabank

3.3 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	200.68.28.131	TLS v1.1	Sitio web BCI
1.1.1.4	200.29.162.187	TLS v1.2	Sitio web Banco Estado
1.1.1.4	184.28.1.191	TLS v1.2	Sitio web Scotiabank

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

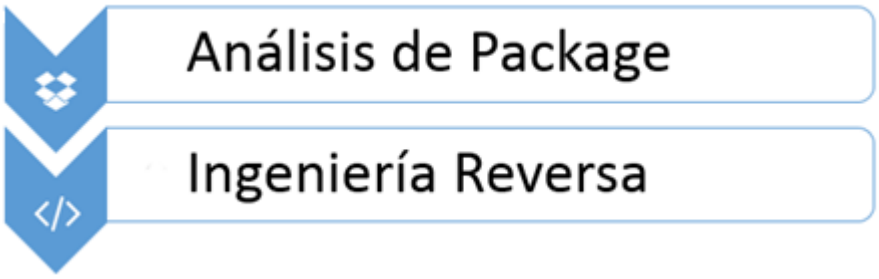
La implementación de SSL/TLS se encuentra con un nivel óptimo de seguridad para el sitio khipu.com y no se encuentra afectado por las vulnerabilidades conocidas hasta el momento de SSL/TLS.

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	7d9a8abe2ccd235c9a3b6c91ec237222
SHA1	ad42540f138427bfb56ebda9bbfb9dff11d48a06
SHA256	464d1a1529dcea4e475d9354f2effa895e715ce374abfe4332c4c5ff27c71136
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

Nombre	khipu 6.9.2.ipa
MD5	853d54aa80913a5fa08e770617a42566
SHA1	bb83b65210aac235729526d0b0bc1122ef9a9bbe
SHA256	50eabb2e8f2916401765f54340400e2f819f7b58ecc75eef9edad6d8e9eae082
Tamaño	13.7 MB
Tipo	iPhone
URLs Interesantes	0
IPs encontradas	0
Emails encontrados	0

5.2.1 URL detectadas

No se encontraron URL en el análisis

5.2.2 Direcciones IPs detectadas

No se encontraron direcciones IP en el análisis

5.2.3 Direcciones de correo detectados

No se encontraron direcciones de correo 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.

iOS			Android		
Motor	**Actualización**	**Estado**	**Motor**	**Actualización**	**Estado**
Ad-Aware	20170512	✓	Ad-Aware	20170512	✓
AegisLab	20170512	✓	AegisLab	20170512	✓
AhnLab-V3	20170512	✓	AhnLab-V3	20170512	✓
Alibaba	20170512	✓	Alibaba	20170512	✓
ALYac	20170512	✓	ALYac	20170512	✓
Arcabit	20170512	✓	Antiy-AVL	20170512	✓
Avast	20170512	✓	Arcabit	20170512	✓
AVG	20170512	✓	Avast	20170512	✓
Avira (no cloud)	20170512	✓	AVG	20170512	✓
AVware	20170512	✓	Avira (no cloud)	20170512	✓
Baidu	20170503	✓	AVware	20170512	✓
BitDefender	20170512	✓	Baidu	20170503	✓
Bkav	20170512	N/A	BitDefender	20170512	✓
CAT-QuickHeal	20170512	✓	Bkav	20170512	✓
ClamAV	20170512	✓	CAT-QuickHeal	20170512	✓
CMC	20170511	✓	ClamAV	20170512	✓
Comodo	20170512	✓	CMC	20170511	✓
CrowdStrike Falcon	20170130	N/A	Comodo	20170512	✓
Cyren	20170512	✓	CrowdStrike Falcon	20170130	N/A
DrWeb	20170512	✓	Cyren	20170512	✓
Endgame	20170503	N/A	DrWeb	20170512	✓
ESET-NOD32	20170512	✓	Emsisoft	20170512	✓
F-Prot	20170512	✓	Endgame	20170503	N/A
F-Secure	20170512	✓	ESET-NOD32	20170512	✓
Fortinet	20170512	✓	F-Prot	20170512	✓
GData	20170512	✓	F-Secure	20170512	✓
Ikarus	20170512	✓	Fortinet	20170512	✓
Invincea	20170413	N/A	GData	20170512	✓

Jiangmin	20170512	✓	Ikarus	20170512	✓
K7AntiVirus	20170512	✓	Invincea	20170413	N/A
K7GW	20170512	✓	Jiangmin	20170512	✓
Kaspersky	20170512	✓	K7AntiVirus	20170512	✓
Kingsoft	20170512	✓	K7GW	20170512	✓
Malwarebytes	20170512	✓	Kaspersky	20170512	✓
McAfee	20170512	✓	Kingsoft	20170512	✓
McAfee-GW-Edition	20170511	✓	Malwarebytes	20170512	✓
Microsoft	20170512	✓	McAfee	20170512	✓
eScan	20170512	✓	McAfee-GW-Edition	20170511	✓
NANO-Antivirus	20170512	✓	Microsoft	20170512	✓
nProtect	20170512	✓	eScan	20170512	✓
Palo Alto Networks	20170512	N/A	NANO-Antivirus	20170512	✓
Panda	20170512	✓	nProtect	20170512	✓
Qihoo-360	20170512	✓	Palo Alto Networks	20170512	N/A
Rising	20170511	✓	Panda	20170512	✓
SentinelOne (Static ML)	20170330	N/A	Qihoo-360	20170512	✓
Sophos	20170512	✓	Rising	20170512	✓
SUPERAntiSpyware	20170512	✓	SentinelOne	20170330	N/A
Symantec	20170511	✓	Sophos	20170512	✓
Symantec Mobile Insight	20170512	N/A	SUPERAntiSpyware	20170512	✓
Tencent	20170512	✓	Symantec	20170511	✓
TheHacker	20170508	✓	Symantec Mobile Insight	20170512	✓
TrendMicro	20170512	N/A	Tencent	20170512	✓
TrendMicro-HouseCall	20170512	✓	TheHacker	20170508	✓
VBA32	20170512	✓	TrendMicro	20170512	N/A
VIPRE	20170512	✓	TrendMicro-HouseCall	20170512	N/A
ViRobot	20170512	✓	VBA32	20170512	✓
Webroot	20170512	✓	VIPRE	20170512	✓
WhiteArmor	20170512	✓	ViRobot	20170512	✓
Yandex	20170510	✓	Webroot	20170512	✓
Zillya	20170511	✓	WhiteArmor	20170512	✓

ZoneAlarm by Check Point	20170512	✓	Yandex	20170510	✓
Zoner	20170512	✓	Zillya	20170511	✓
			ZoneAlarm by Check Point	20170512	✓
			Zoner	20170512	✓

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_mayo.cap	c056286097bb7c71e0c13088c4f4c713
2	ios_mayo.cap	3e8fdd4846b20052ce3d15b5302fbf6e
3	osx_mayo.cap	b7bbc898f6778f00a86b4f278f2397ac
4	test.xml	0727e51036a8a46dcc1d2f0dd80dac83