FORO EJECUTIVO

CIBERSEGURIDAD EN EL sector financiero

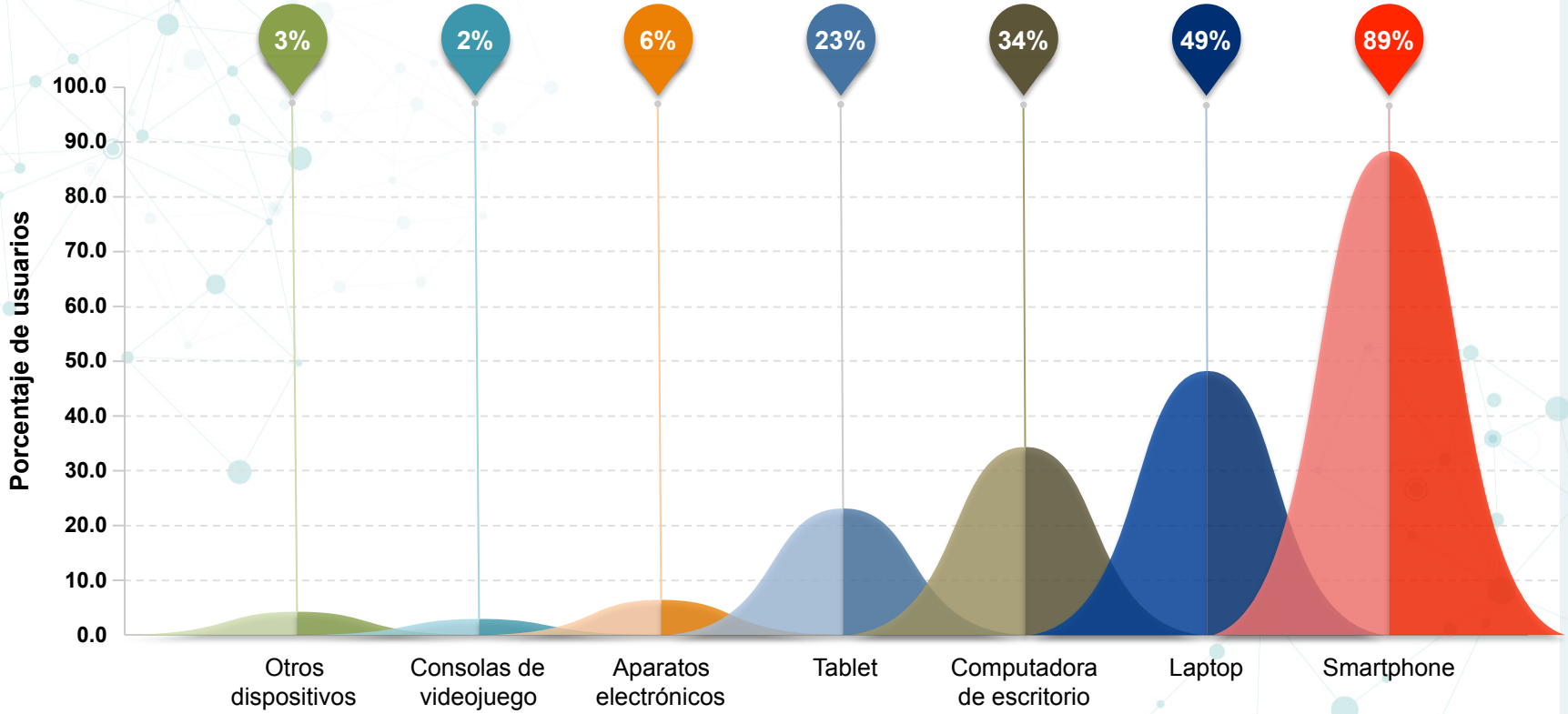
CIBERCRIMEN: INCERTIDUMBRE Y COMPLEJIDAD

Seguridad en Móviles

Mauricio Olivera
Coordinador de Innovación y Desarrollo Tecnológico
SCITUM

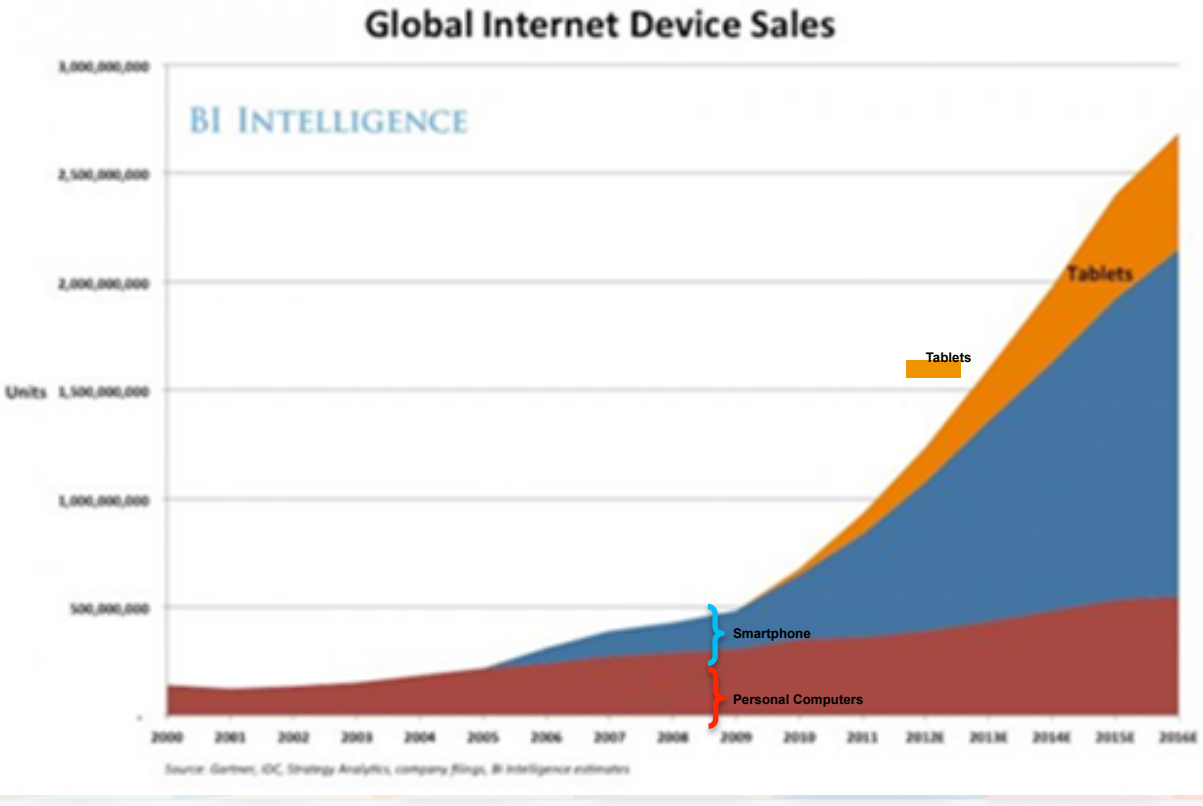
Scitum | TELMEX está contigo

Usuarios de Internet, 2017 (INEGI)



79.1 millones de usuarios

Usuario



79.1 millones de usuarios

Scitum | TELMEX está contigo

Seguridad actual en la empresa

Scitum | TELMEX está contigo

Seguridad actual en la empresa

Scitum | TELMEX está contigo

Seguridad actual en la empresa

Scitum | TELMEX está contigo

Uso del dispositivo móvil

e-mail empresarial y personal

Fotografías

Contactos

Pagos electrónicos

Videos

Chat/SMS

Aplicaciones empresariales

Documentos en la nube

Redes sociales

Geolocalización

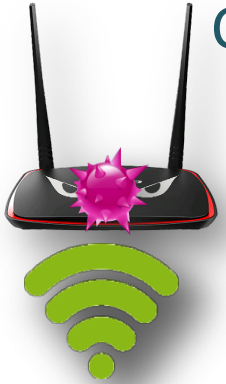
Archivos

Registro de llamadas

¿Cómo pueden atacarnos?

Entrar a sitios falsos

Conexión a WiFi desconocido



Descargar aplicaciones de sitios no oficiales

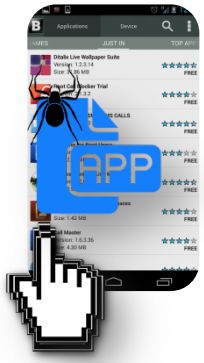
Recepción de mensajes de texto y correos electrónicos

¿Cómo pueden atacarnos?

Entrar a sitios falsos

Todo esto puede presentar una amenaza a la seguridad

Recepción de mensajes de texto y correos electrónicos



Descargar aplicaciones de sitios no oficiales

¿Cómo nos afecta?

Nuestra información queda en manos del atacante

Pagos electrónicos

Fotografías

Archivos

Contactos

Chat/SMS

¿Cómo nos afecta?

Incluso información que represente una

pérdida monetaria

Pagos electrónicos

Fotografías

Archivos

Contactos

Chat/SMS

¿Cómo nos afecta?

Remotamente un atacante puede…

… tomarnos fotografías

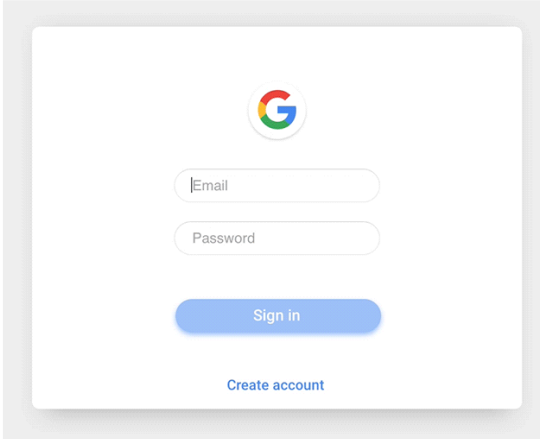
… abrir el micrófono y escucharnos

… tomarnos video

¿Cómo nos afecta?

Remotamente un atacante puede…

… robar nuestra identidad



¿Cómo nos afecta?

Remotamente un atacante puede…

… saber nuestra ubicación

… todo esto, ¡sin que nos demos cuenta!

iOS

2014

Masque
7.x, 8.x

Wirelurker

2014-4487
< 8.1.3
Used in
JailBreak

2015

ICMP Double
Direct

xCode Ghost

YiSpector
iOS 8.4 &
below
impacted

2016

Pegasus
Remote IOS
exploit;

Stagefright
for iOS
CVE-2016-4637

Android

2014

TowelRoot
200M devices
Impacted

DoubleDirect

HeartBleed
800K devices
Impacted

2015

StageFright
95% of
Android
Impacted

Wormhole
(Moplus
SDK)

Oxygen
SwiftKey

2016

Triada
Zygote
system
exploit

Humming-
Bad;
Hummer
Malware

QuadRooter

AirDroid

Godless

Gooligan

Drammer

DirtyCow

PokeMon
Go Guide

2017

Humming-
Whale
(HummingBad
variant)

= Zimperium Labs Discovery

iOS

Masque 7.x, 8.x

Wirelurker

2014-4487 < 8.1.3 Used in JailBreak

ICMP Double Direct

xCode Ghost

YiSpector iOS 8.4 & below impacted

Pegasus Remote IOS exploit;

Stagefright for iOS CVE-2016-4637

ANDROID

TowelRoot 200M devices Impacted

DoubleDirect

HeartBleed 800K devices Impacted

StageFright 95% of Android Impacted

Wormhole (Moplus SDK)

Oxygen SwiftKey

Triada Zygote system exploit

Humming-Bad; Hummer Malware

QuadRooter

AirDroid

Humming-Whale (HummingBad variant)

Godless

Gooligan

Drammer

DirtyCow

PokeMon Go Guide

= Zimperium Labs Discovery

2014

2015

2016

2017

Scitum | TELMEX está contigo

IMPRESO | MILENIO RADIO | MILENIO TV | MARTES, 20/06/17 | INGRESAR | REGÍSTRATE

MILENIO.COM

TENDENCIAS

Política | Firmas | Estados | Policía | Tendencias | Negocios | Cultura | VR360 | Tribuna

Internacional | El Polígrafo | Fotogalerías | Moneros | Laberinto | Mujeres | Salud | Viajes

¿Qué es Pegasus?, el malware usado para espiar en México

A través de mensajes de texto, las víctimas recibían enlaces para descargar el malware que permitía el acceso a archivos del teléfono e incluso la activación del micrófono y la cámara del teléfono.

Ir a comentarios | Me gusta 178 | 16 | Compartir 193 | G+1 0

Fox, "el demócrata" quiere impedir el cambio en 2018: AMLO

Combatiremos terrorismo sea quien sea responsable: May

Piratas informáticos realizaron un robo millonario en bancos de varios países. (Shutterstock)

Masque 7.x, 8.x

TowelRoot 200M device Impacted

Pegasus Remote IOS exploit;

Stagefright for iOS CVE-2016-4637

Triada Zygote system exploit

Humming-Bad; Hummer Malware

QuadRooter

AirDroid

Humming-Whale (HummingBad variant)

Godless

Gooligan

Drammer

DirtyCow

PokeMon Go Guide

2016

2017

= Zimperium Labs Discovery

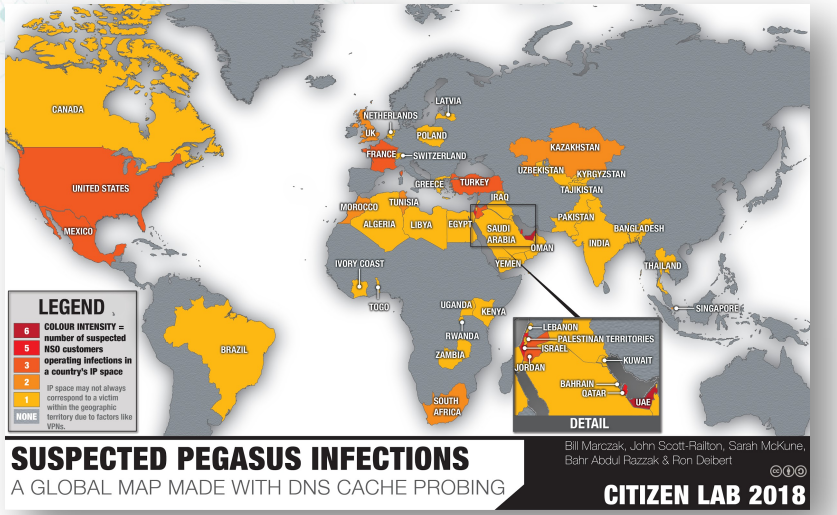
Scitum | TELMEX está contigo

THECITIZENLAB

Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries

By Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert

September 18, 2018

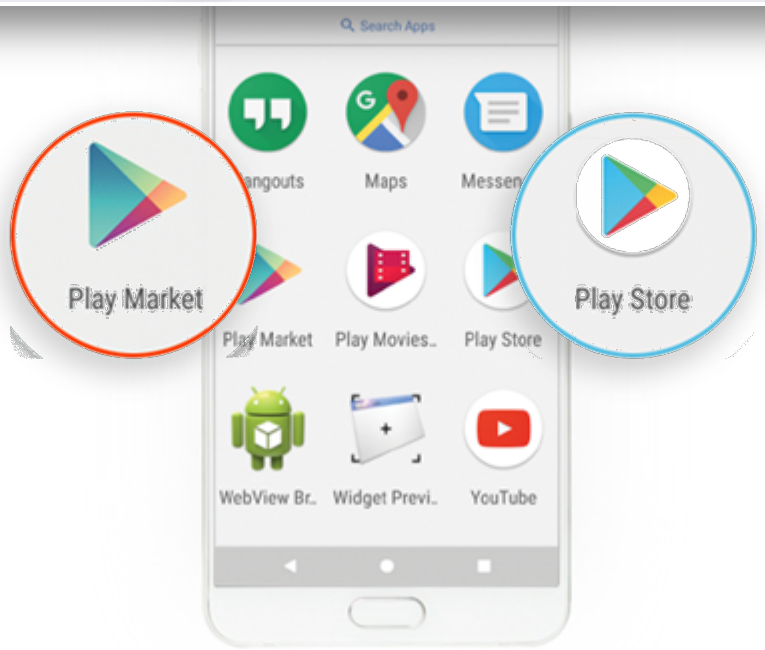


Operator name	Dates operator was active	Suspected country focus	Political themes?	Suspected infections
RECKLESS-1	Sep 2016 – Jun 2017	Mexico	Yes	–
RECKLESS-2	Oct 2016 – Jun 2017	Mexico	Yes	–
MAYBERECKLESS	Sep 2017 – present	–	–	Mexico
PRICKLYPEAR	Oct 2016 – present	Mexico	–	Mexico, USA (Arizona)
AGUILAREAL	Sep 2016 – present	Mexico	–	Mexico
MACAW	Nov 2017 – present	Honduras	Yes	–

Fake Play Market: Zimperium's z9 against Social Engineering Attack Vectors

zLabs | Android | Sep 19 2018 |

Play Market:
FAKE



Play Store:
REAL

Scitum | TELMEX está contigo

national

ANZ and Commonwealth Bank targeted by fake Android Google Play store apps

SCAMMERS have tricked 1000 Australian customers of the ANZ and Commonwealth Banks to reveal their secret details after creating fake downloadable apps.

Staff writer

News Corp Australia Network SEPTEMBER 20, 2018 9:06AM

Dos tendencias encontradas

Ciberataques

Escritorio → Móvil

SPAM → Dirigido

Fastidio → Ganancia $$$

Android → IOS

Tecnología móvil

Llamada + Texto + mail + Corporativo → BYOD

Conveniencia → Productividad

Horas laborales → Cualquier hora

Scitum | TELMEX está contigo

Dos tendencias encontradas

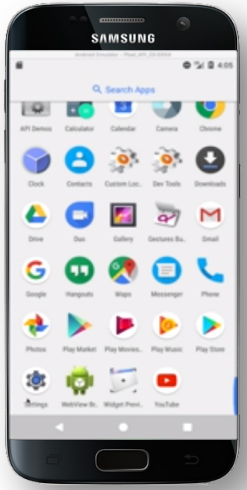
Scitum | TELMEX está contigo

Principales amenazas

Acceso físico

Código malicioso

Redes inseguras



Vulnerabilidades
o apps falsas

Fuga de información

Algunas recomendaciones

- Contraseñas fuertes y con cambios periódicos
- Cifrado del dispositivo
- Apps conocidas (validadas y autorizadas)
- Actualizaciones
- Conexión a WiFi de confianza
- “App store” legítimos (y no apk)
- Respaldos
- Cargas “de corriente” (no USB solamente)
- Conexión con VPN
- Borrado remoto
- Antivirus
- Programas de concientización (awareness)
- Servicio de protección contra AMENAZAS AVANZADAS


Protección de datos
Scitum
08:00
TUESDAY, JUNE 20
TELMEX
está contigo
Protección de nuestra
PRIVACIDAD

GRACIAS

DESCARGUE ESTA PRESENTACIÓN EN

resources | scitum

resources.scitum.com.mx

Scitum | TELMEX está contigo