



Sinfonier



Tacyt



Faast

# Cazando cibercriminales con: OSINT + Cloud Computing + Big Data

*Chema Alonso*  
(@chemaalonso)



tacyt : THE TOOL FOR APP  
CYBER INTELLIGENCE

# Problem: Cybercrime in Android



Sinfonier



Tacyt



Faast

The collage features three news articles. The top-left article from **ars technica** is titled "Family of 'BadNews' malware in Google Play downloaded up to 9 million times" and mentions that the apps steal sensitive data and push SMS app that racks up charges to pricey service. The top-right article from **c/net** is titled "Malware went undiscovered for weeks on Google Play" and explains that breaking the malware into separate, staged payloads allowed the Trojan's authors to avoid detection by Google's automated screening process. The bottom article from **IDG News Service** is titled "Malware-infected Android apps spike in the Google Play store" and notes that Wallpaper Dragon Ball and Finger Hockey were among the most downloaded malicious apps.

**ars technica**

MAIN MENU MY STORIES: 0 FORUMS SUBSCRIBE JOBS

RISK ASSESSMENT / SECURITY & HACKTIV

**Family of "BadNews" malware in Google Play downloaded up to 9 million times**

Apps steal sensitive data, push SMS app that racks up charges to pricey service.

by Dan Goodin - Apr 20 2013, 5:21pm +0200

**c/net**

English Reviews News Download CNETTV How To De

CNET > News > Security & Privacy > Malware went undiscovered for weeks on Google Play

**Malware went undiscovered for weeks on Google Play**

Breaking the malware into separate, staged payloads allowed the Trojan's authors to avoid detection by Google's automated screening process.

by Steven Musil

Home > Security

**Malware-infected Android apps spike in the Google Play store**

Wallpaper Dragon Ball and Finger Hockey were among the most downloaded malicious apps

By Zach Miners

February 19, 2014 04:29 PM ET 4 Comments

in Share 17 Twitter g+1 Facebook Like 51 More

IDG News Service - The number of mobile apps infected with malware in Google's Play store nearly quadrupled between 2011 and 2013, a security group has reported.

PM PDT

More +

Comments 5

android.dragonball

# Problem: Cybercrime in Google Play



## Whatsapp Free

Appfree Inc. - 14 de septiembre de 2013  
Sociedad

Instalada

Esta aplicación es compatible con tu dispositivo.

★★★★★ (199)



## Whatsapp - Free

LJ AP DEV - 14 de octubre de 2013  
Sociedad

Instalar



Añadir a la lista de deseos

Esta aplicación es compatible con tu dispositivo.



## Whatsapp 2013 free

AppDev tech company - 19 de octubre de 2013  
Comunicación

Instalada

Esta aplicación es compatible con tu dispositivo.



## gratis Whatsapp

WhatsMessenger, Inc. - 20 de octubre de 2013  
Comunicación



## WhatsApp Messenger

Whatsapp tech inc - 23 de octubre de 2013  
Sociedad

Instalar



Añadir a la lista de deseos

Esta aplicación es compatible con tu dispositivo.

★★★★★ (3)



## WhatsApp Messenger

WhatsApp Inc. - 23 de octubre de 2013  
Comunicación

Instalada

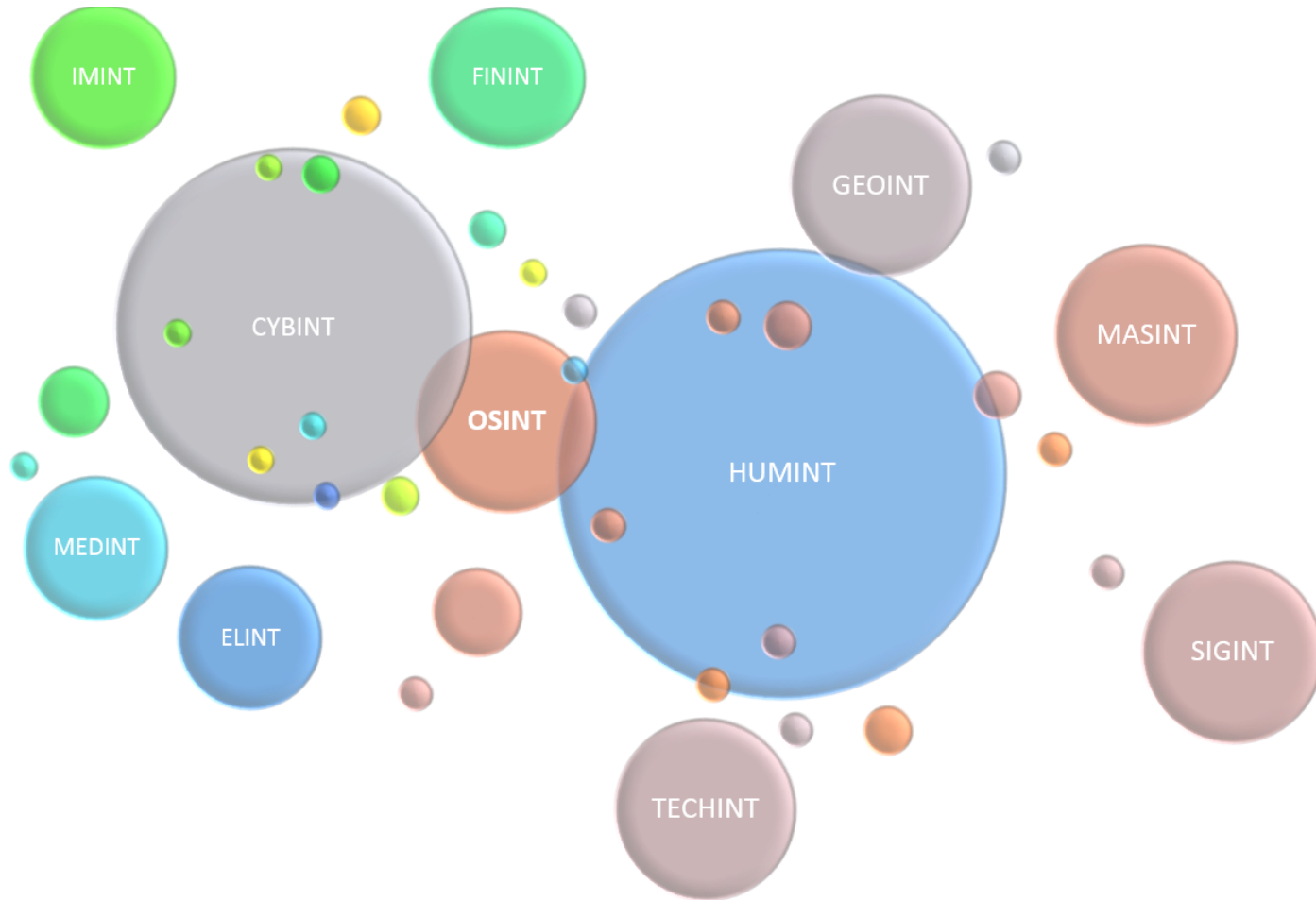
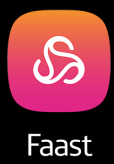
Esta aplicación es compatible con tu dispositivo.

★★★★★ (4,548,135)



Desarrollador destacado

# *Intelligence & Security*





# OSINT (Open Source Intelligence)



- OSINT is the art and science of creating ethical, evidence-based decision support using only open sources and methods, legal and ethical in every respect.
  - Big data to store & process
  - Analytic toolkits to detect *patterns and anomalies*
- Beyond that, OSINT is all about *humans—analysts who can think, and deciders who can listen.*

*Robert David Steele on OSINT – 2014*

# OSINT



Sinfonier



Tacyt



Faast

- *Useful*
- *Not less powerful than other \*INTs\**
- *Not more powerful than other \*INTs\**
- *Sometimes not that easy to build up*
- *Not always free*
- *Not always easy*

- *Goal: Build an OSINT platform*
  - *Android Markets*
    - *Google Play Included*
    - *Process all data related to apps & markets*
  - *Build up a Big Data*
  - *Build a real time processing tool for analyst*
  - *Create connections to other security tools*

## A Measurement Study of Google Play

Nicolas Viennot  
Computer Science  
Department  
Columbia University  
New York, NY, USA  
nviennot@cs.columbia.edu

Edward Garcia  
Computer Science  
Department  
Columbia University  
New York, NY, USA  
ewg2115@columbia.edu

Jason Nieh  
Computer Science  
Department  
Columbia University  
New York, NY, USA  
nieh@cs.columbia.edu

### ABSTRACT

Although millions of users download and use third-party Android applications from the Google Play store, little information is known on an aggregated level about these applications. We have built PLAYDRONE, the first scalable Google Play store crawler, and used it to index and analyze over 1,100,000 applications in the Google Play store on a daily basis, the largest such index of Android applications. PLAYDRONE leverages various hacking techniques to circumvent Google's roadblocks for indexing Google Play store content, and makes proprietary application sources available, including source code for over 880,000 free applications. We demonstrate the usefulness of PLAYDRONE in decompiling and analyzing application content by exploring four previously unaddressed issues: the characterization of Google Play application content at large scale and its evolution over time, library usage in applications and its impact on application portability, duplicative application content in Google Play, and the ineffectiveness of OAuth and related service authentication mechanisms resulting in malicious users being able to easily gain unauthorized access to user data and resources on Amazon Web Services and Facebook.

### Keywords

Android; Authentication; Clone Detection; Decompilation; Google Play; Mobile Computing; OAuth; Security;

### 1. INTRODUCTION

The Google Play store allows users to download and use a vast amount of third-party applications. Millions of users register personal information both with Google and third-party services to download and use these applications on their personal Android phones and tablets. Hundreds of thousands of developers upload content to the Google Play store and millions of users download the content despite the fact that the content is largely unchecked.

However, little is known at an aggregate level about the hundreds of thousands of applications available in the Google Play store. This is due in large part to the lack of scalable tools available for discovering and analyzing Android applications in the Google Play store. Application source code is also only available to the respective third-party developers. Not even Google has access to the source code, as applications are submitted directly as compressed binary packages by application developers to Google Play. Fur-

- *Real Time integration of apps*
- *Real Time processing of filters*
- *Interactive Console*
- *Cross-Market analysis*
- *Cross-Time results (Dead apps)*
- *API*

# *Tacyt Demo 1:*



Sinfonier



Tacyt

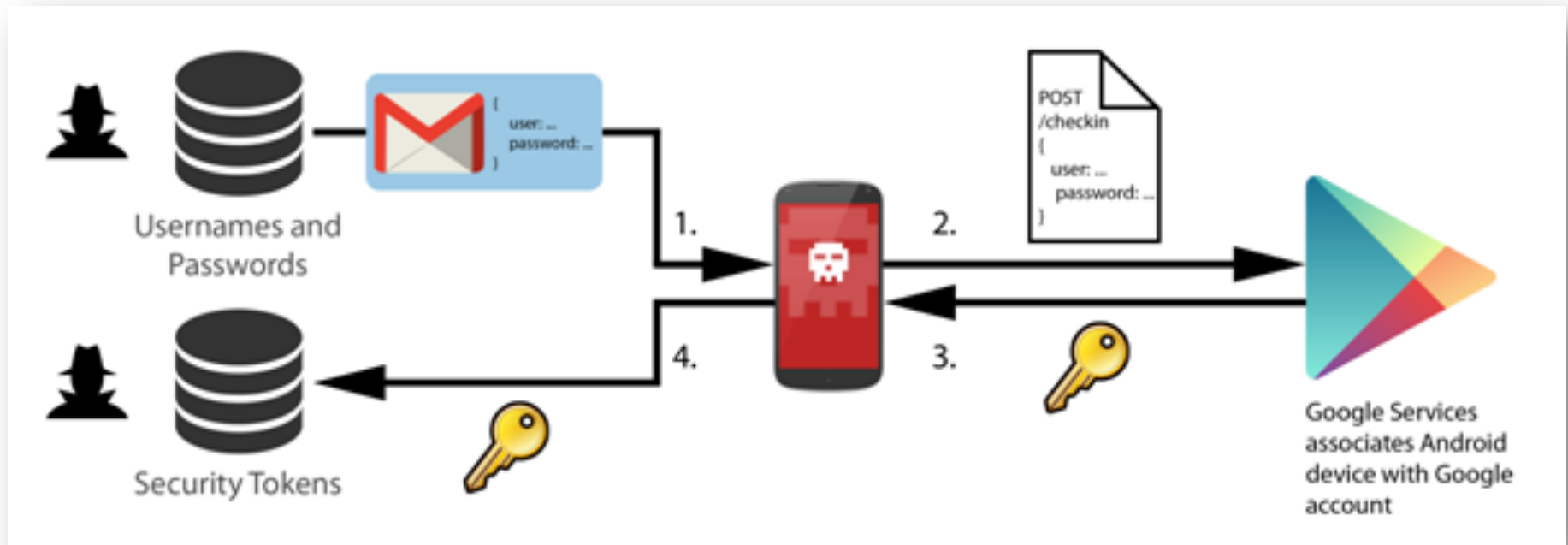


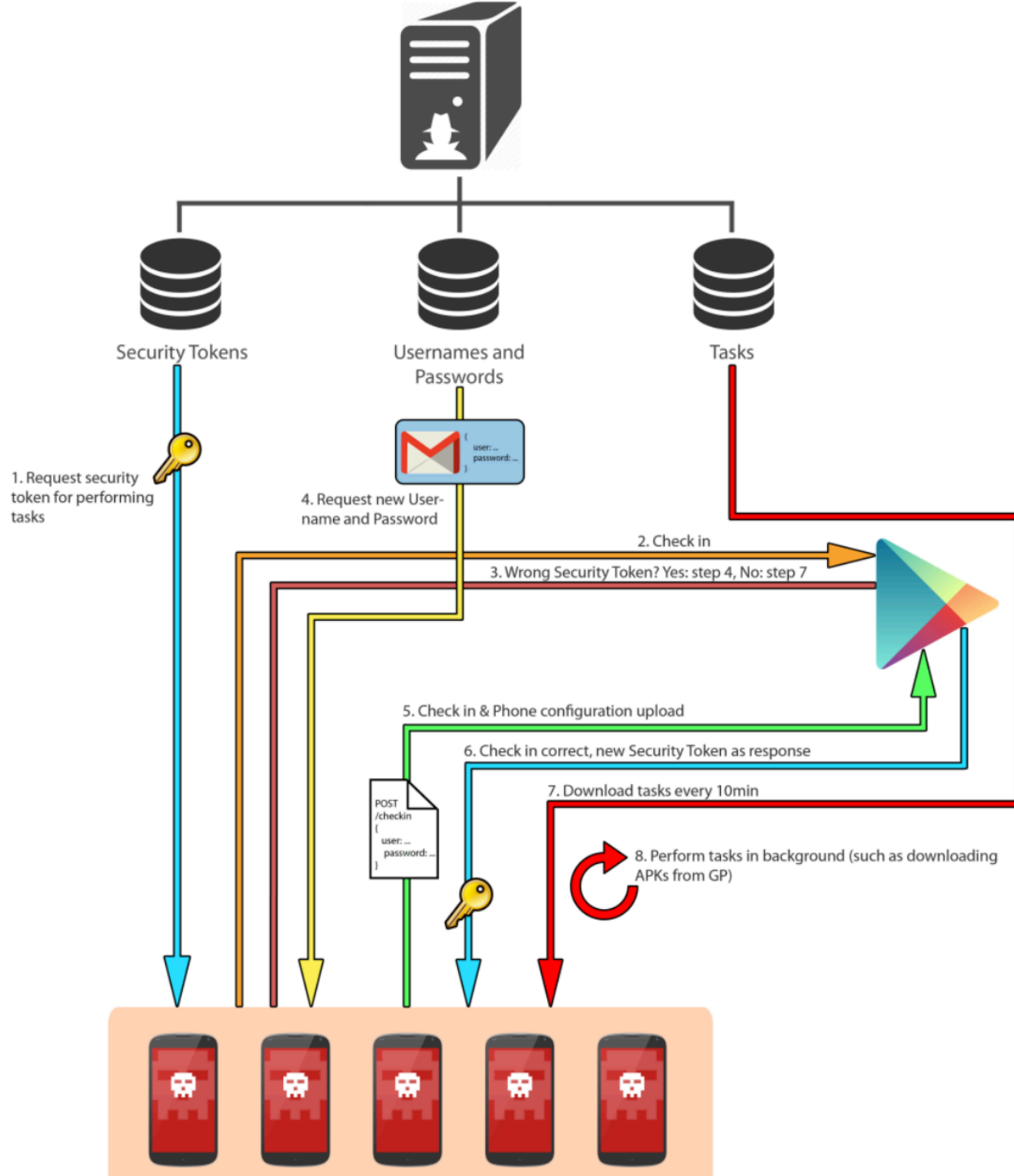
Faast

*Fake Apps + Fake Devs*



# Shuaban Botnet





# Shuaban Botnet



Sinfonier



Tacyt



Faast

## ACCOUNT

ID	用户名	密码	创建时间	设备标识	地区	操作
10661	stcloudbv29@gmail.com	*****	2014-11-06,23:32:10	7005fa5fca	巴西	<a href="#">修改</a> <a href="#">删除</a>
10662	amandacq92@gmail.com	*****	2014-10-29,18:26:43	bf81f80f7d	巴西	<a href="#">修改</a> <a href="#">删除</a>
10663	besscwb6@gmail.com	*****	2014-11-06,23:37:14			
10664	isaacpd70@gmail.com	*****	2014-10-29,18:34:31			
10665	nilslvb@gmail.com	*****	2014-11-06,23:42:50			

## User Accounts

User	From Host
dujiadui	%
jiankongbao	60.195.252.106
jiankongbao	60.195.252.108
root	%
root	localhost.localdomain
root	127.0.0.1
root	::1

## *Tacyt Demo 2:*



Sinfonier



Tacyt



Faast

*Shuabang Botnet*

# Security Solutions



Sinfonier



Tacyt



Faast

- *Antivirus*
  - *They do they work well, but are good detecting, **not discovering***
- *Reputation*
  - *Voting, users, opinions*
- *Automatic Report*
  - *False positives*
  - *False negatives*
- *Sandboxes*
  - *Slow, bypass, Slow*

celularis ANDROID APPLE HTC NOKIA SAMSUNG SONY OPINION

## Los antivirus en Android no sirven para nada

30 30 DE MAYO DE 2013, 19:13

Muchos dicen que basta con tener sentido común basta para no tener antivirus en Android, que no es cierto, ya que en Google Play también ha habido malware. ¿Entonces? ¿Qué hace falta para no tener antivirus en Android? De momento, no lo sabemos, pero al fin y al cabo, da igual, ninguno sirve para nada.

SHA256: fc4f2c2f88e4366fc19d1350cc54f3e5c0f083e33238f784341b6ff5dcee3ce1

Nombre: com.ndsonkentucky.kumanda.apk

Detecciones: 0 / 57

Fecha de análisis: 2015-01-20 07:37:29 UTC ( hace 38 minutos )

Analisis Detalles Información adicional Comentarios 0 Votos Información de comportamiento

Antivirus	Resultado	Actualización
ALYac	✓	20150120
AVG	✓	20150120

# Reputation Report



Sinfonier



Tacyt



Faast

## Threat Report of Android App

trustlook.com  
03/28/2014 12:05 p.m.

**com.originalsongs321**



 **Risk Status: Safe**

 **Risk Score:**

**0** /10



### App Summary

<b>App Name</b>	com.originalsongs321
<b>MD5</b>	522A750170F42863121F6B2ACCB09965
<b>SHA1</b>	ECFC861666A94CAD19E15389D77997F87CEFC754



Summary  
Behaviours Details  
General Info.  
Permissions  
Activities  
Services  
Receivers  
Libraries  
ELF Files  
s  
tification  
ential Risky  
ngs



# Reputation Report



Sinfonier



Tacyt



Faast

## Threat Report of Android App

trustlook.com  
03/29/2014 2:29 a.m.

com.whatsapp



 Risk Status: **Low Risk**

 Risk Score:

**3** /10



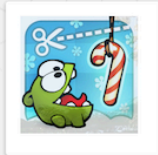
### App Summary

App Name	com.whatsapp
MD5	ABC553D30FC4E2F83BA5961389512D42
SHA1	3D5E31B4234FFA0254FF5E6AC844FB28180D0BBF

- Apply some intelligence to *the way attackers work* on Google Play. Anomalies & Singularities.
- Do not concentrate on DETECTING, but on *CORRELATING* data. Detecting is difficult, but once you know your enemy and with the right amount of information and data, correlating is easy.
- We try to find *singularities*
- *Avoid code*. Code is a wall you go against again and again. Attackers know how to avoid being detected.

- *We need to know our enemies and what makes them singular.*
- *Android apps are **APK**, which are just Java files, which are just ZIP files signed with a selfsigned certificate. We have identified and dissected most of the technical characteristics.*
- *Android apps are **hosted in Google Play**, with a developer, comments, descriptions, images, versions, categories...*
- *There is plenty of information. Almost **50 “checkpoints”** .*

# Gremlin App

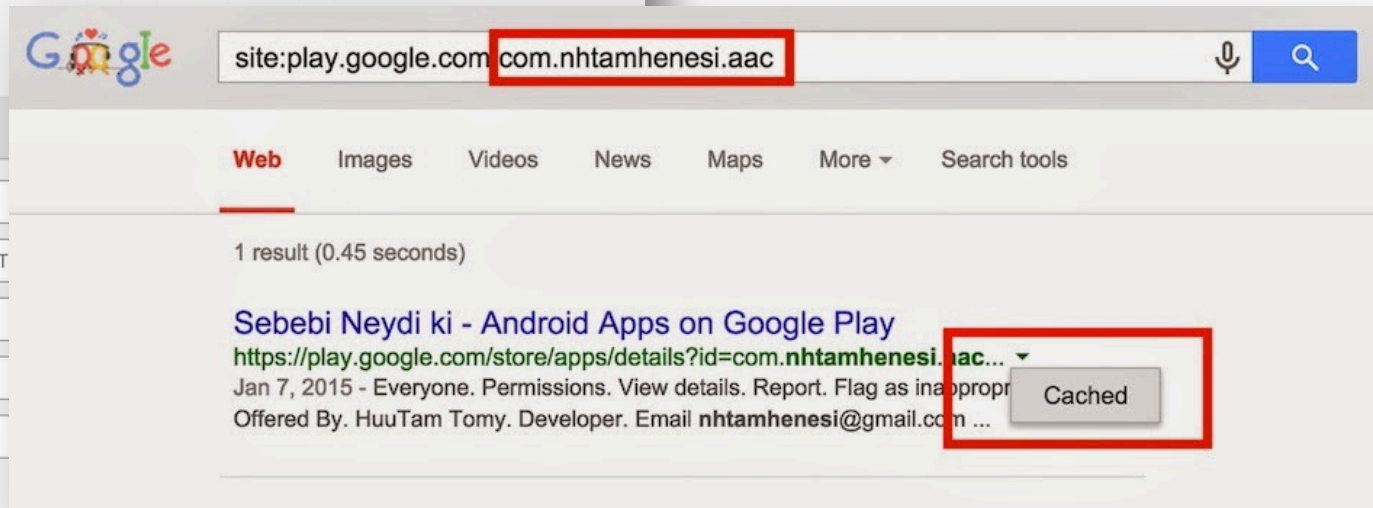


## Cut Rope Christmas

Download app

### General information

Origin	GooglePlay
Category	GAME_ADVENT
Size	63,350 bytes
Number of downloads	50
Version code	1
Description	Feed the animal
Title	Cut Rope Christmas
Package name	com.nhtamhenesi.aac



# Gremlin App



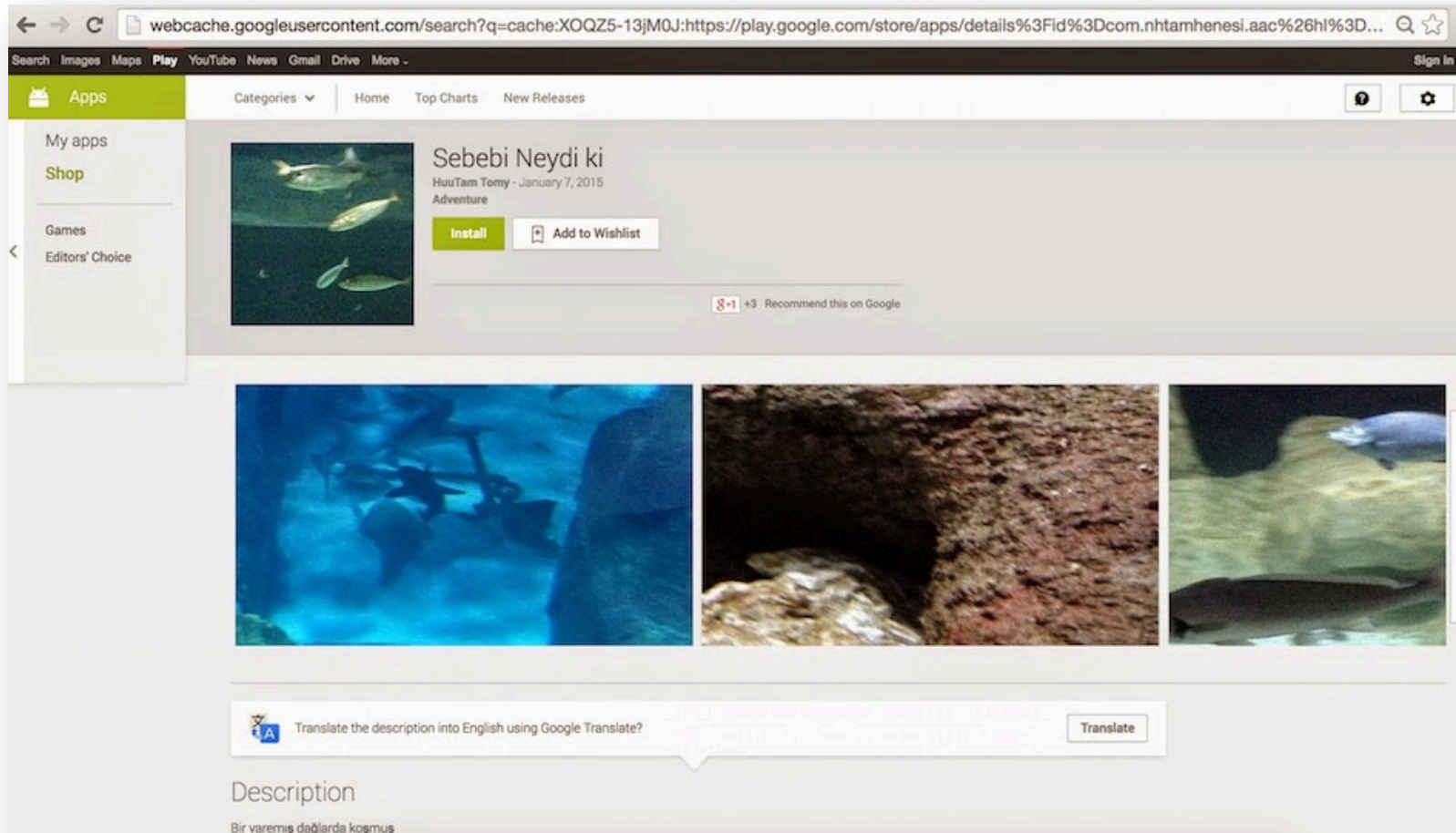
Sinfonier



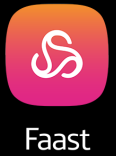
Tacyt



Faast



# Buying Gremlin Apps



The screenshot shows the Google Play Store interface for the app 'Pixel Battery Saver'. On the left, there's a preview of the app's icon (a purple circle with a white battery icon) and a preview of the app's interface showing 'NEW COOL FEATURES' and 'COMING SOON!'. The main content area displays the app's title 'Pixel Battery Saver', its category 'Android > App', and its statistics: 'Total Installations / Current Installations' as '250000 / 50000'. Below this, it says 'Full App Transfer Price USD:'. The app's description is 'Internet security free antivirus and speed booster - January 14, 2015 Tools'. There are 'Install' and 'Add to Wishlist' buttons. The app has a rating of 4.9 stars from 4,910 reviews and is marked as 'Editors' Choice'.

- *But... What apps make sense to mutate?*



# *APT Providers: Gremlin apps for targeted attacks*



Sinfonier



Tacyt



Faast

- *Lets find some applications that fit with different target profile.*
- *These apps needs to be attractive but don' t seem to provide a critical functionality because It is needed that once they are installed, keep under the radar.*
- *We need a rich porfolio of applications.*

# *“Perfet” Target Apps*



## Apps



### Deployment Tracker Pro

Users can track multiple deployments with this cloud enabled Deployment Tracker. Access deployments across devices and view deployments on a searchable and editable list. Track your deployments like a pro!



### Military Mobile

This app deploys with Military Bases, Military Ranks, Military Ribbons, Military Quizzes, a unique and integrated Deployment Tracker, and a rich set of social features. The perfect reference for US Soldiers.

- How to select the perfect set of applications for an APT once the reconnaissance of the victim has been achieved.*

# APT Providers: Gremlin apps for targeted attacks



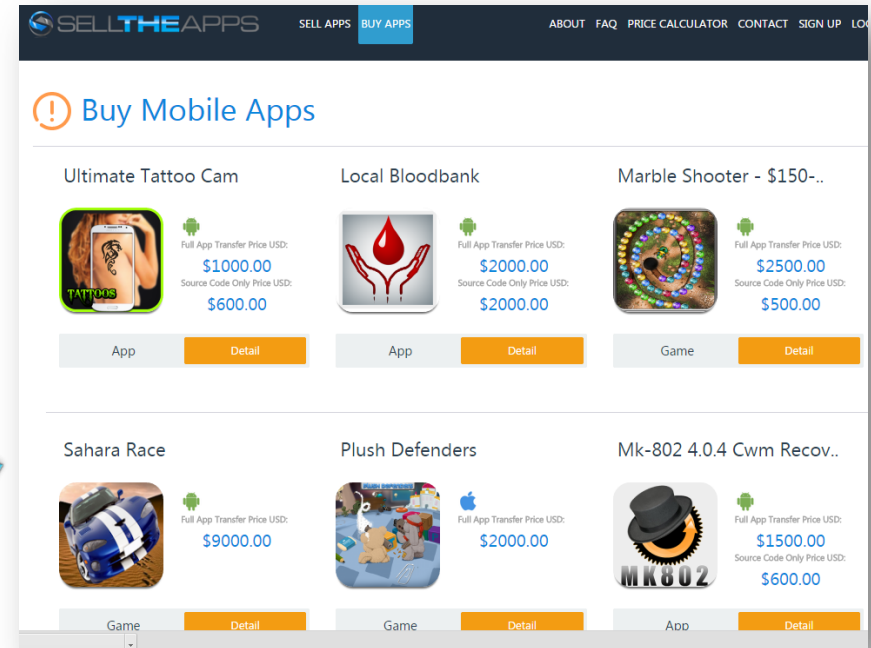
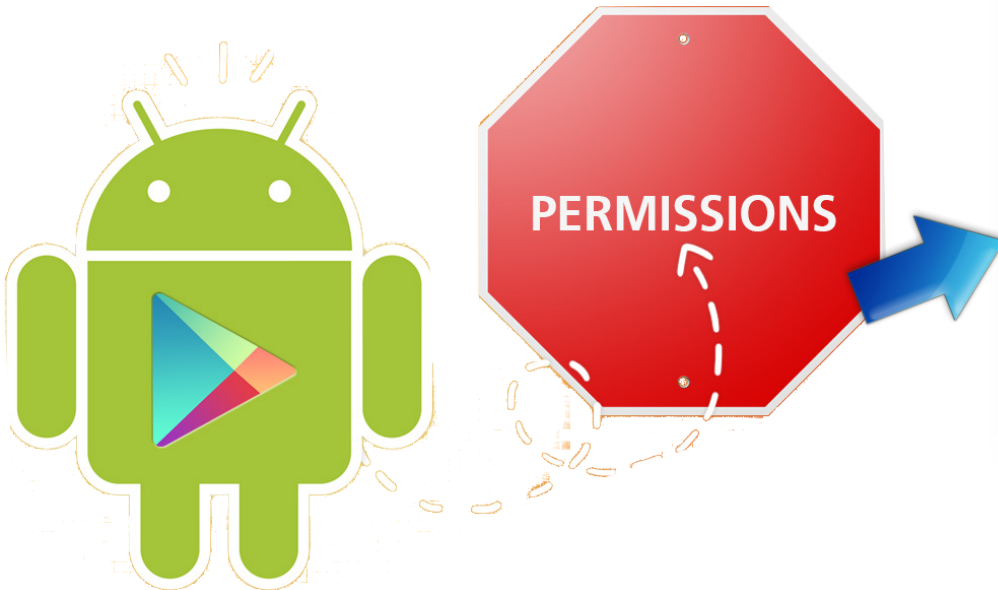
Sinfonier



Tacyt



Faast



```
permissionName:"android.permission.GET_ACCOUNTS" permissionName:"android.permission.INTERNET"  
permissionName:"android.permission.READ_EXTERNAL_STORAGE"  
permissionName:"android.permission.READ_PHONE_STATE"  
permissionName:"android.permission.ACCESS_NETWORK_STATE"
```

## *Tacyt Demo 3:*



Sinfonier



Tacyt



Faast

## *Profiling Attack – Clicker*

## *Examples: Research and clusterization*



- *We can correlate data and cluster apps:*
  - *From an app, we can include the person or company who made it and correlate it with other developers in which account they hide.*
  - *We can detect anomalies: developers uploading 50 apps in a row? Developers sharing exactly the same files in their APK? Developers sharing images? APKs with just a second of developing time?...*

## *Tacyt Demo 4:*



Sinfonier



Tacyt



Faast

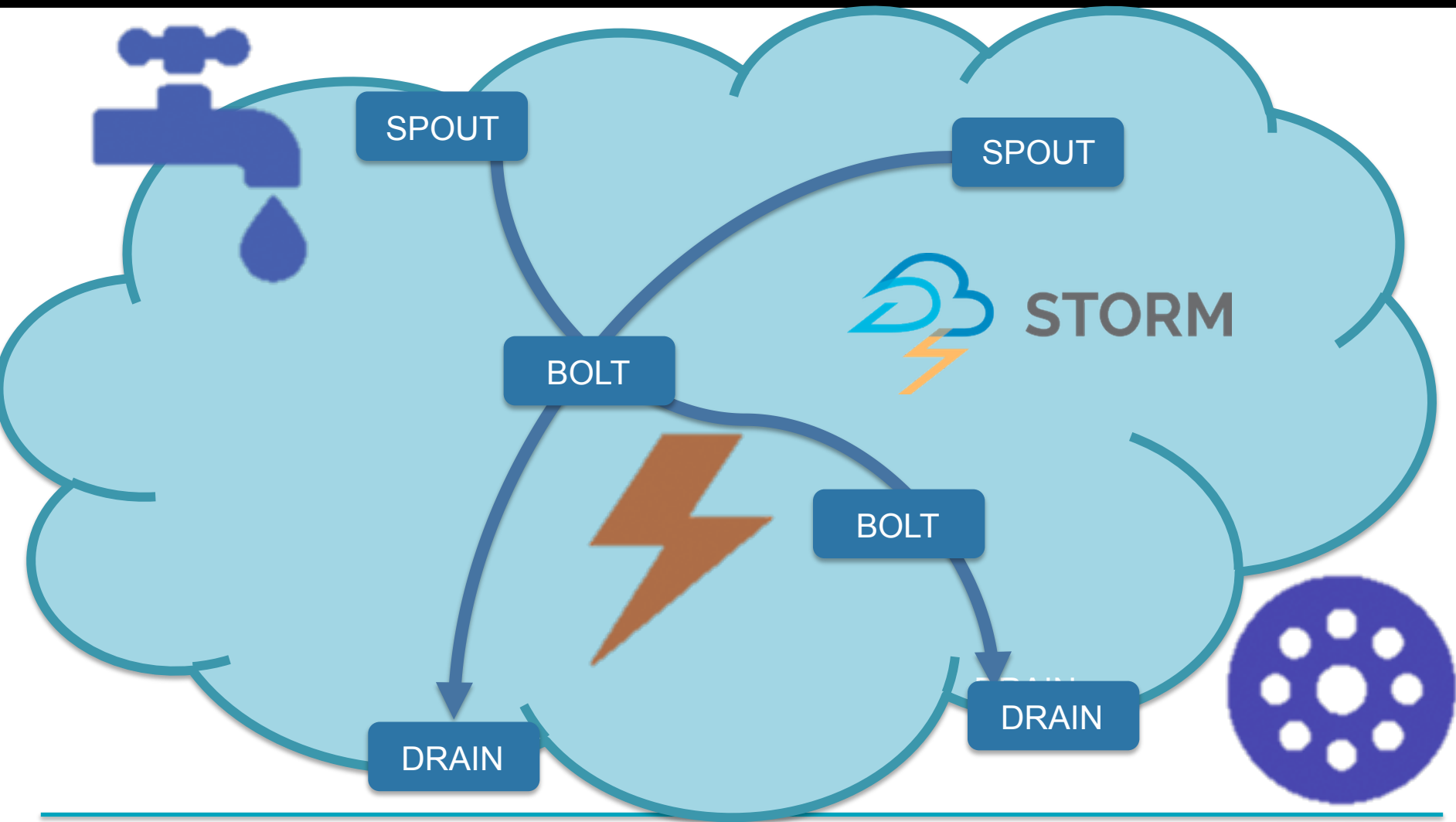
*IS Dialers*



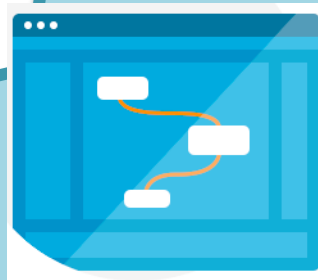
- *Allows to correlate data and detect*
  - *Anomalies*
  - *Singularities*
- *Helps to search quickly in a Big Data of apps*
- *Helps to avoid code in detecting cybercrime*
- *Provides an API to be an OSINT and integrate with other tools.*



*“Apache Storm is a free and open source distributed realtime computation system. Storm makes it easy to reliably process unbounded streams of data, doing for realtime processing what Hadoop did for batch processing. Storm is simple, can be used with any programming language, and is a lot of fun to use!”*



# How It works



Drag & Drop  
Interface



Automatic  
Deploy API  
(Nightly version)

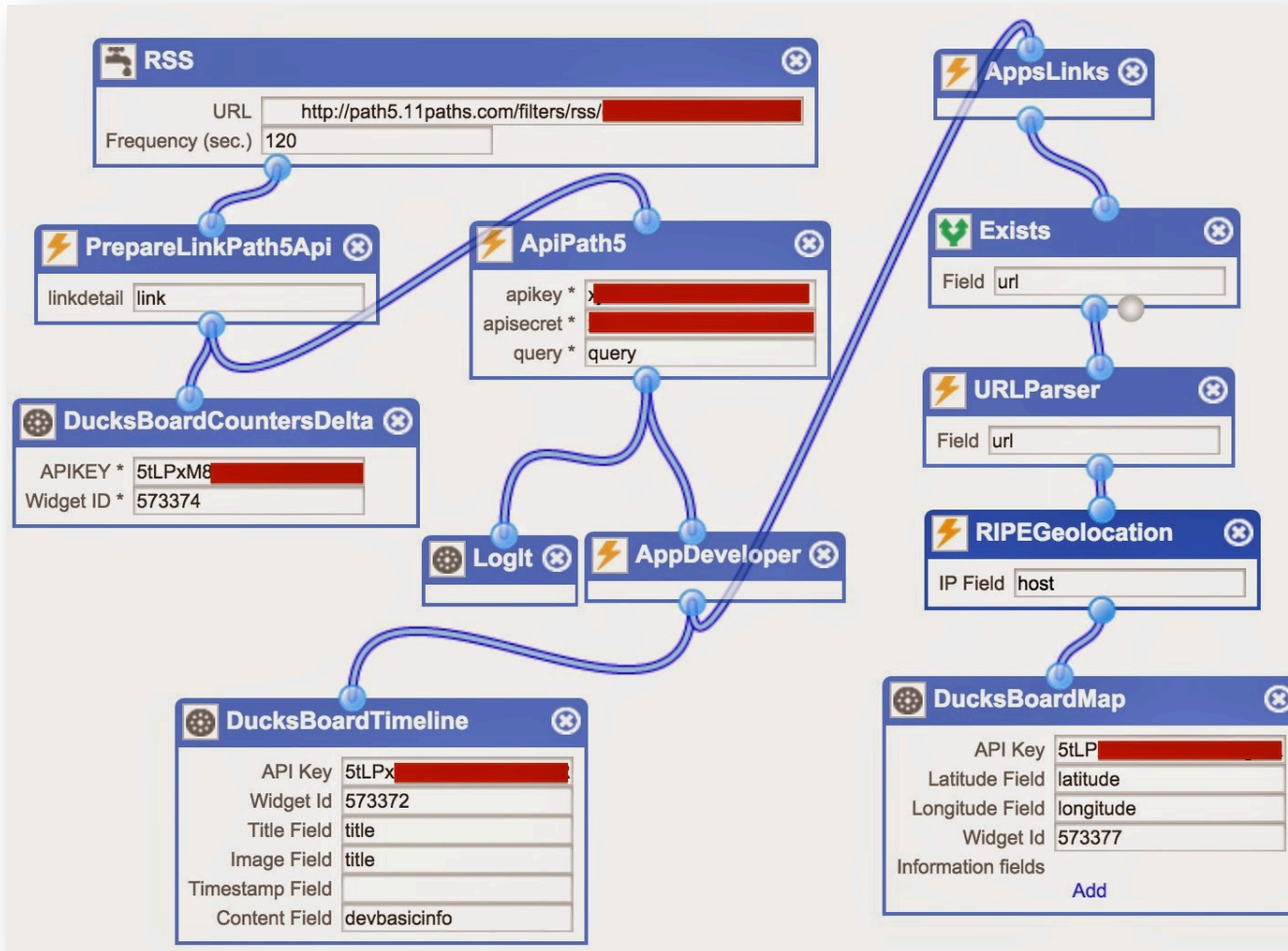
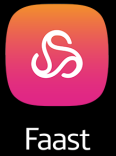


Storm  
Cluster



Sinfonier

# Sinfonier Topologies



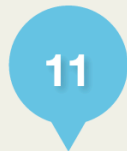
# Tacyt + Sinfonier



## APKS



FEED ORIGINAL



NUEVAS APKS DETECTADAS

## EMAILS DISTINTOS DESARROLLADORES

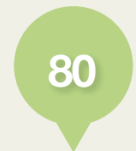


EN EL FEED ORIGINAL

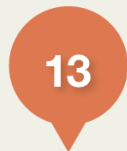


EN LAS NUEVAS APKS DETECTADAS

## DETALLE "PATHS" ENCONTRADOS EN LAS APKS



TOTAL ANALIZADOS



SINGULARES

## "PATHS" ANALIZADOS

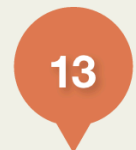


"paths" singulares

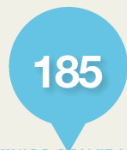
## "PATHS" SINGULARES MÁS UTILIZADOS

PATH	Nº APKS
/FT/COMMENTINNER.FB	53
/FT/FILE.FB	53
/FT/UPCMTATTACH.FB	47
/MGW.HTM	38
/DNS/PUBLICIPS	31
/REG/REG_MOB2_RETAK...P...	13
/REG/REG_MOB2.JSP	8
/XCHINESE/APPSKYOUT.PHP	6
/VPBX_RONG/CHINESE/APPC...	6
/API/ACCESSTOKEN	6

## DOMINIOS QUE UTILIZAN PATHS SINGULARES



"PATHS" SINGULARES



DOMINIOS CON "PATHS" SINGULARES



## DOMINIOS SINGULARES RESPECTO AL TOTAL ANALIZADOS



dominios singulares

# Faast (Vamps)



## How it works

### Monitoring the status of vulnerabilities

- Dashboard that makes management easier
- Detailed and validated monitoring reports on tests conducted, vulnerabilities found, solutions, and development of the vulnerabilities

### Scheduling

Agreement on domains audited, assessment slots and processing capacity

### On-demand, real-time queries

- Vulnerabilities detected and corrected
- Assets discovered by changes in the infrastructure

### Persistent test execution

- Asset identification
- Asset analysis
- Vulnerability exploitation
- Vulnerability verification
- Remediation plan definition

Powered by  
**Faast**

# Conclusions



Sinfonier



Tacyt



Faast

- *Cybercrime in Apps is huge*
- *Research in Google Play is not easy*
- *Tacyt allows to*
  - *Discover and Investigate anomalies & singularities*
  - *Cross-Market*
  - *Cross-Time*
- *Synfonier helps to*
  - *integrate other sources*
  - *Automate Intelligence Generation*
- *Faast help us to reduce security Windows*
  - *Managing vulnerabilities in a persistent way*





tacyt : THE TOOL FOR APP  
CYBER INTELLIGENCE



Fonier



Tacyt



Faast

## *Questions?*

- If you want give a try to TACYT, contact me!
- <http://www.elevenpaths.com>
- Chema Alonso  
[@chemalonso](#)
- [chema@11paths.com](mailto:chema@11paths.com)
- <http://www.elladodelmal.com>

