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

ars technica

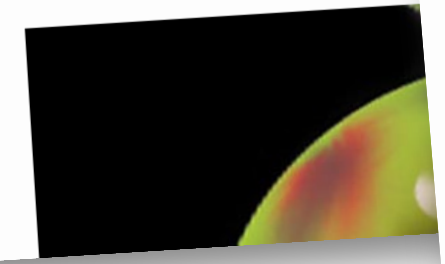
MAIN MENU MY STORIES: 0 FORUMS SUBSCRIBE JOBS

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 CNET TV How To

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

PM PDT

More +

Comments

Home > Security

News

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

Share 17 g+1 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.

Eleven Paths

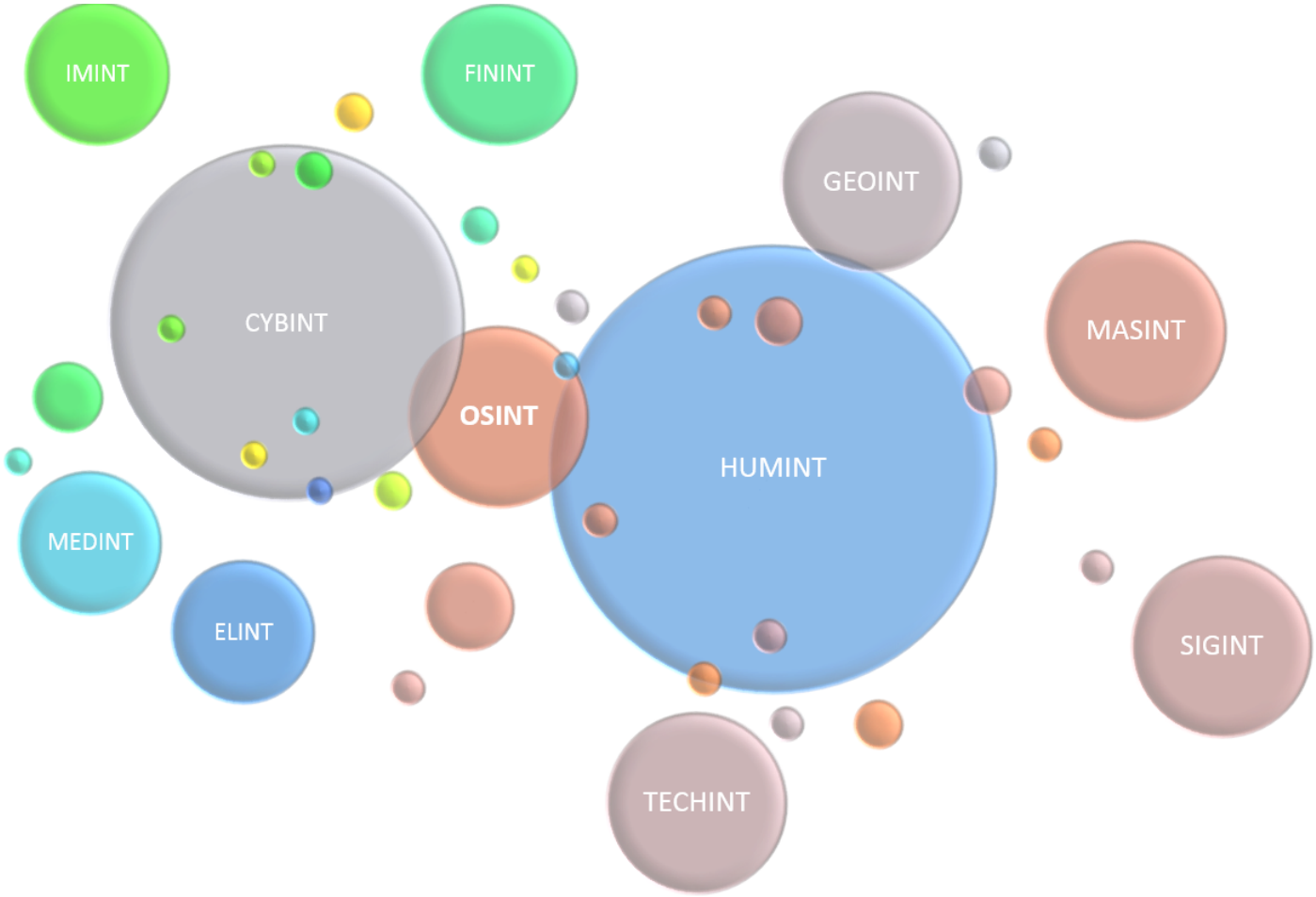
Problem: Cybercrime in Google Play

Sinfonier Tacyt Faast

Eleven Paths

Intelligence & Security

Sinfonier Tacyt Faast



Eleven Paths

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

- 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

Tacyt

- 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

PlayDrone

Sinfonier Tacyt Faast

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-

Eleven Paths

Tacyt

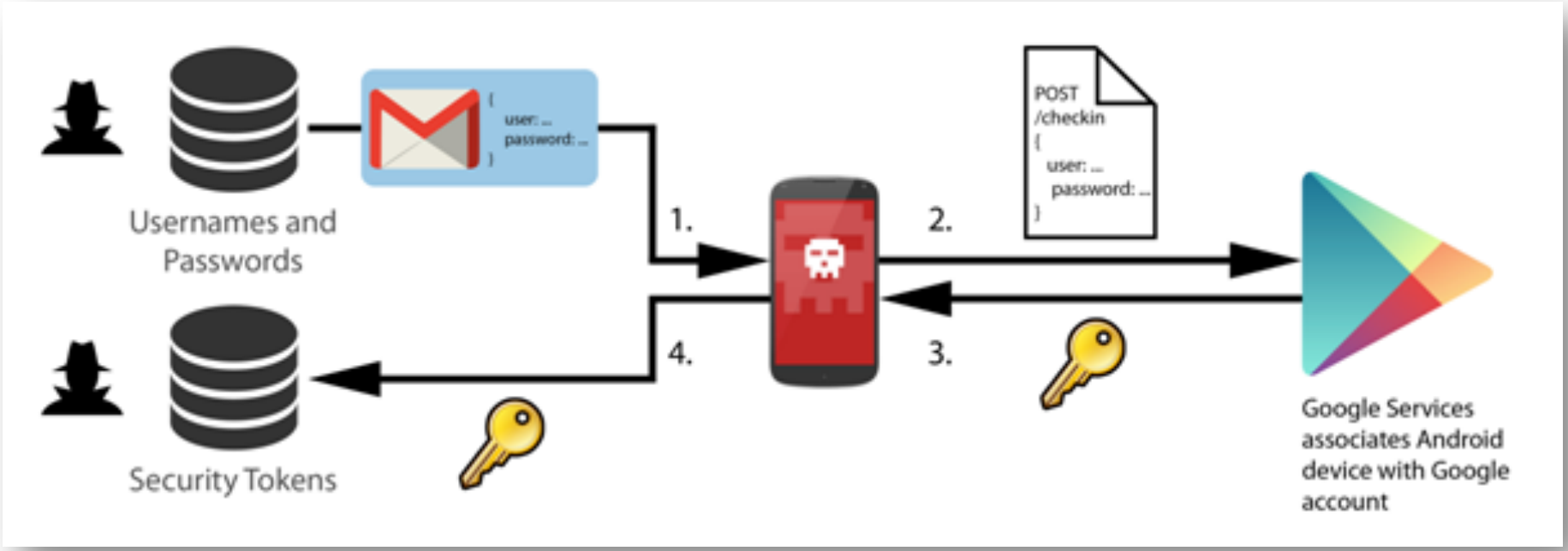
- Real Time integration of apps
- Real Time processing of filters
- Interactive Console
- Cross-Market analysis
- Cross-Time results (Dead apps)
- API

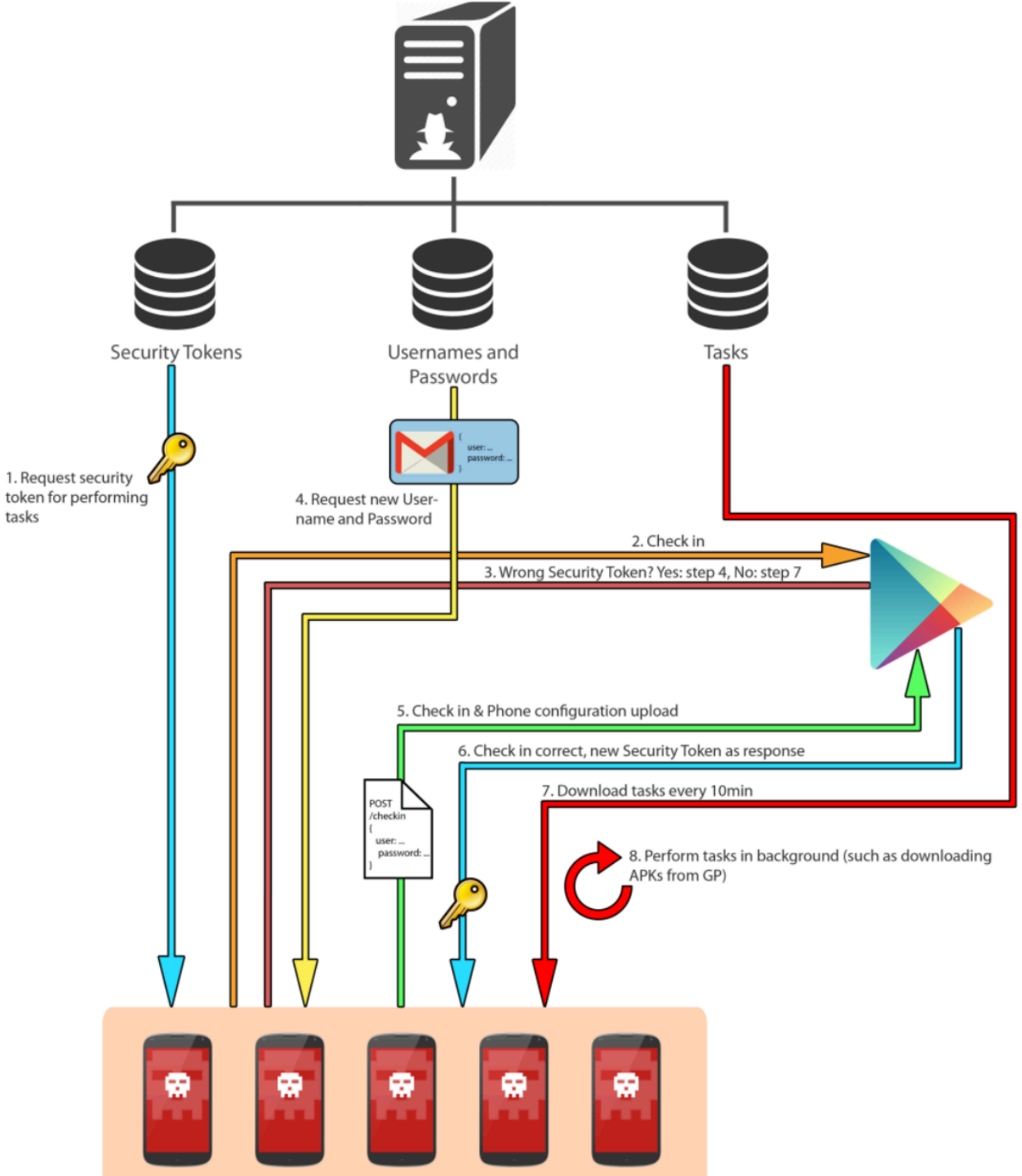
Tacyt Demo 1:

Fake Apps + Fake Devs

Shuaban Botnet

Sinfonier Tacyt Faast





Shuaban Botnet

Sinfonier Tacyt Faast

ACCOUNT

ID	用户名	密码	创建时间	设备表识	地区	操作
10661	stcloudbv29@gmail.com	*******	2014-11-06,23:32:10	7005fa5fca[redacted]	巴西	修改 删除
10662	amandacq92@gmail.com	*******	2014-10-29,18:26:43	bf81f80f7d[redacted]	巴西	修改 删除
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

Eleven Paths

Tacyt Demo 2:

Shuabang Botnet

Security Solutions

Sinfonier Tacyt Faast

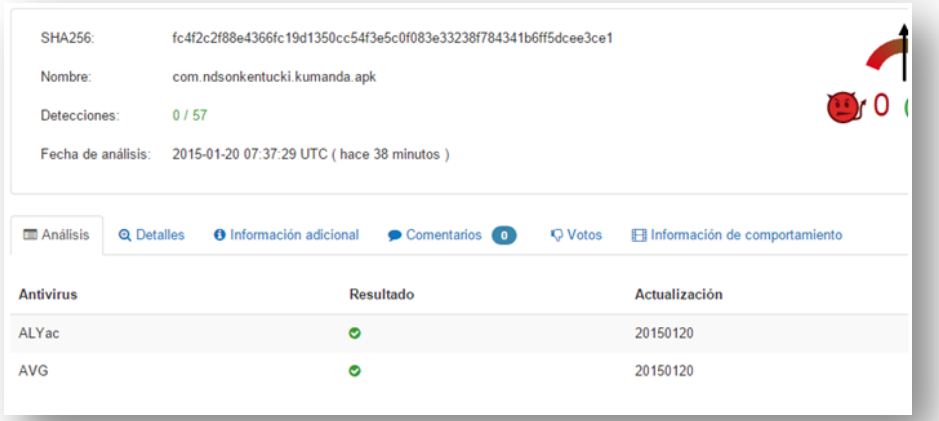
- Antivirus
  - They do they work well, but are good detecting, not discovering
- Reputation
  - Voting, users, opinions
- Automatic Report
  - False positives
  - False negatives
- Sandboxes
  - Slow, bypass, Slow


celularis ANDROID APPLE HTC NOKIA SAMSUNG SONY OPINION

Los antivirus en Android no sirven para nada

30 Twittear 607 +1 73 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.ndsonkentucki.kumanda.apk

Detecciones: 0 / 57

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

Análisis Detalles Información adicional Comentarios 0 Votos Información de comportamiento

Antivirus	Resultado	Actualización
ALYac	✓	20150120
AVG	✓	20150120

Eleven Paths

Reputation Report

Sinfonier Tacyt Faast

Threat Report of Android App

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

- Summary
- aviours Details
- eral Info.
- Permissions
- Activities
- Services
- Receivers
- Libraries
- ELF Files
- s
- tification
- ential Risky
- ngs

com.originalsongs321

Risk Status: Safe

Risk Score:

0 /10

App Summary

App Name	com.originalsongs321
MD5	522A750170F42863121F6B2ACCB09965
SHA1	ECFC861666A94CAD19E15389D77997F87CEFC754

Eleven Paths

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

Eleven Paths

Tacyt

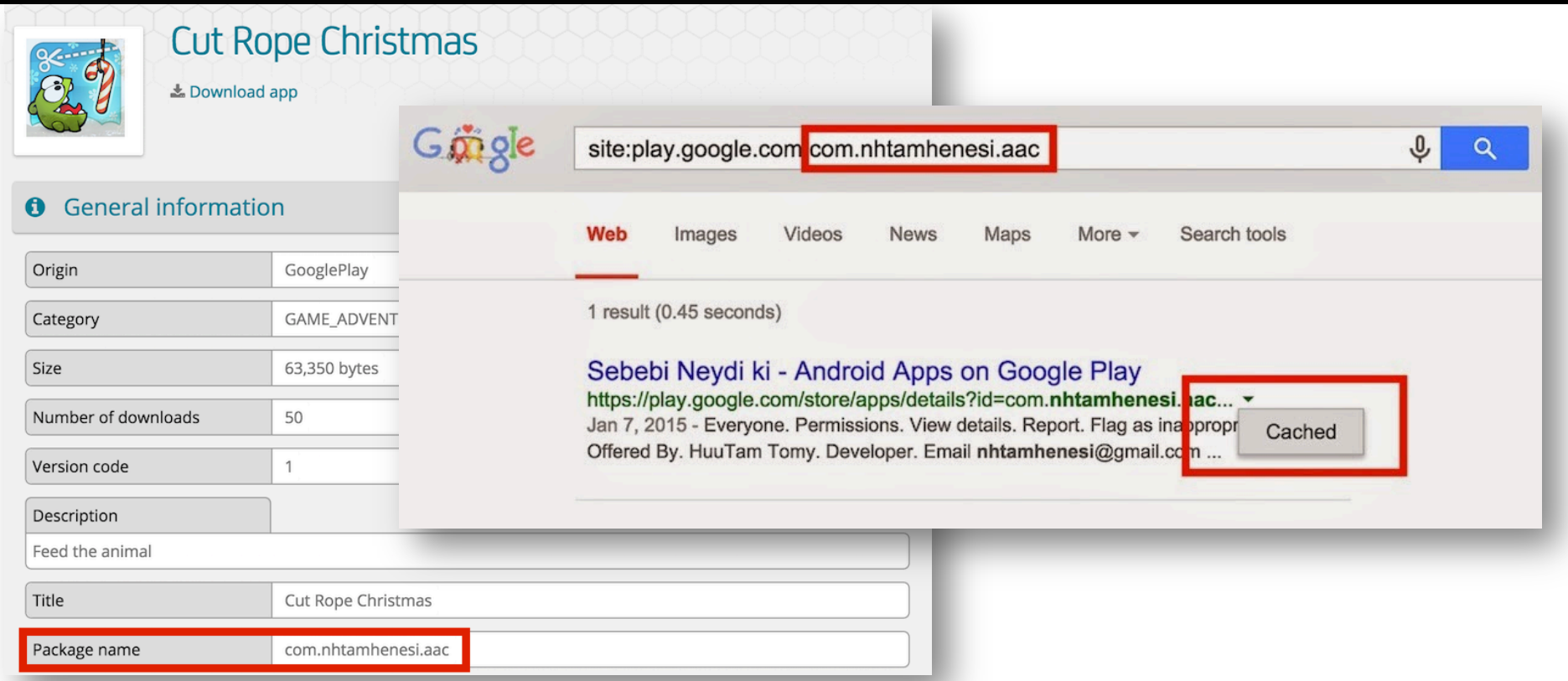
- Apply some intelligence to **the way attackers work** on Google Play. Anomalies & Singularities.
- Do not concentrate on DETECTING, but on CORRELATING data. Detecting is difficult, but once you know your enemy and with the right amount of information and data, correlating is easy.
- We try to find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

Tacyt

- **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

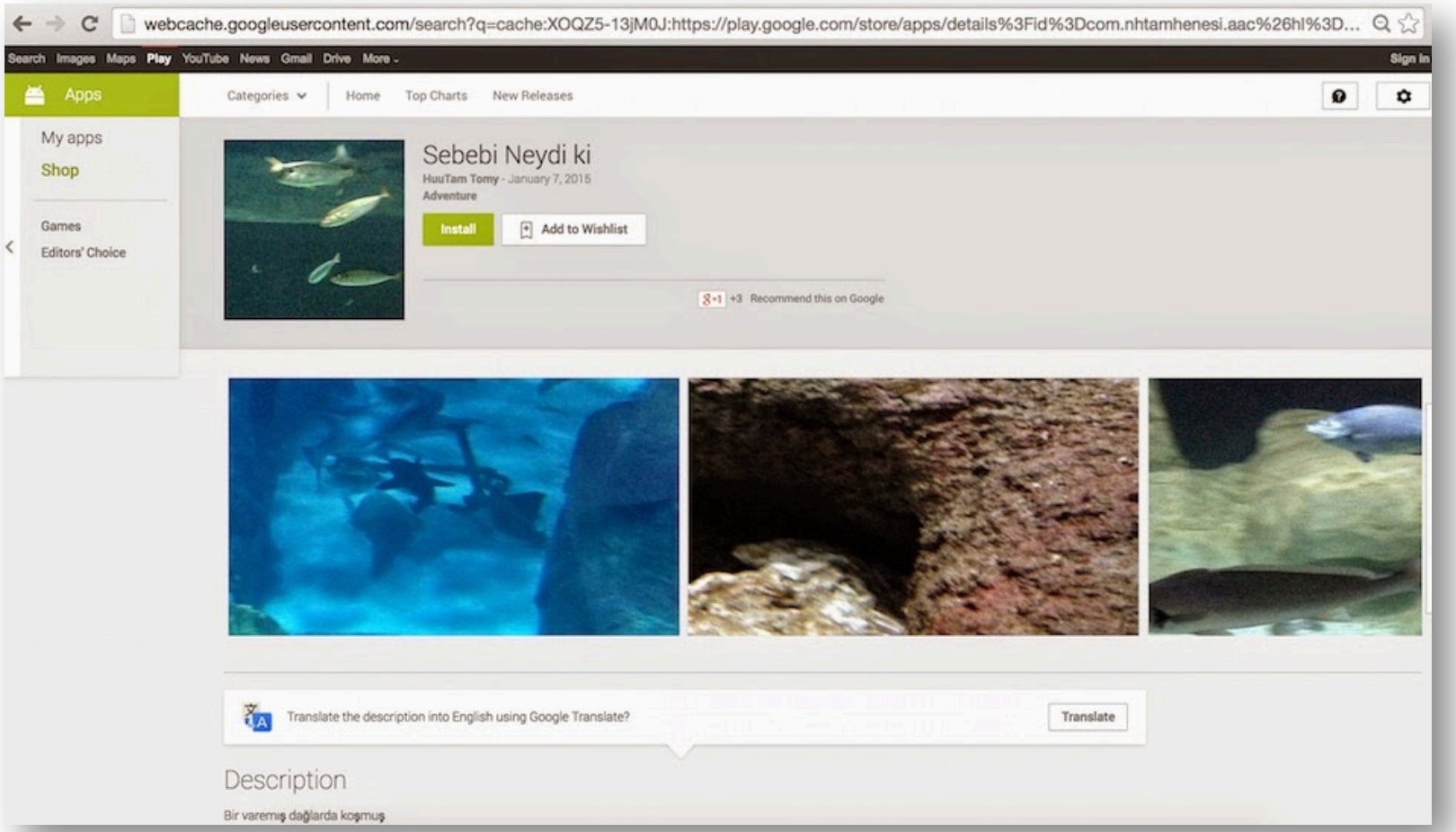
Sinfonier Tacyt Faast



Eleven Paths

Gremlin App

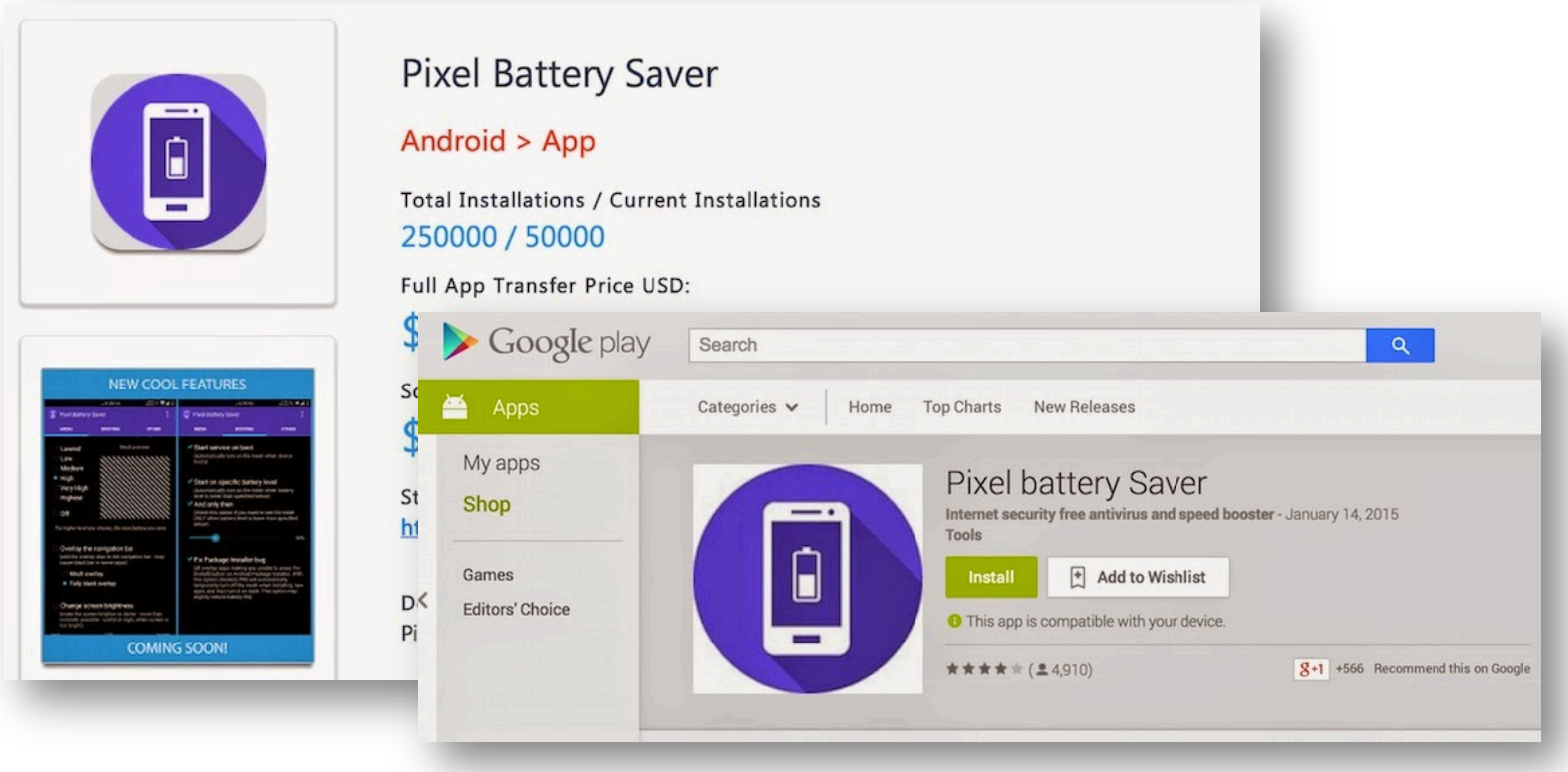
Sinfonier Tacyt Faast



Eleven Paths

Buying Gremlin Apps

Sinfonier Tacyt Faast



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

Eleven Paths

APT Providers: Gremlin apps for targeted attacks

- 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

Sinfonier Tacyt Faast

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!

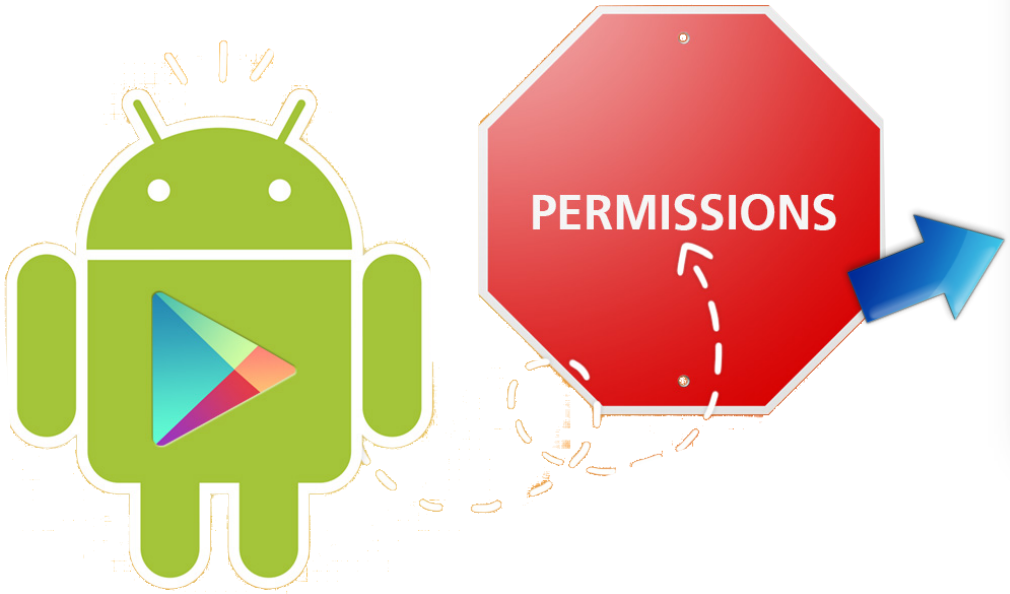
Military Mobile

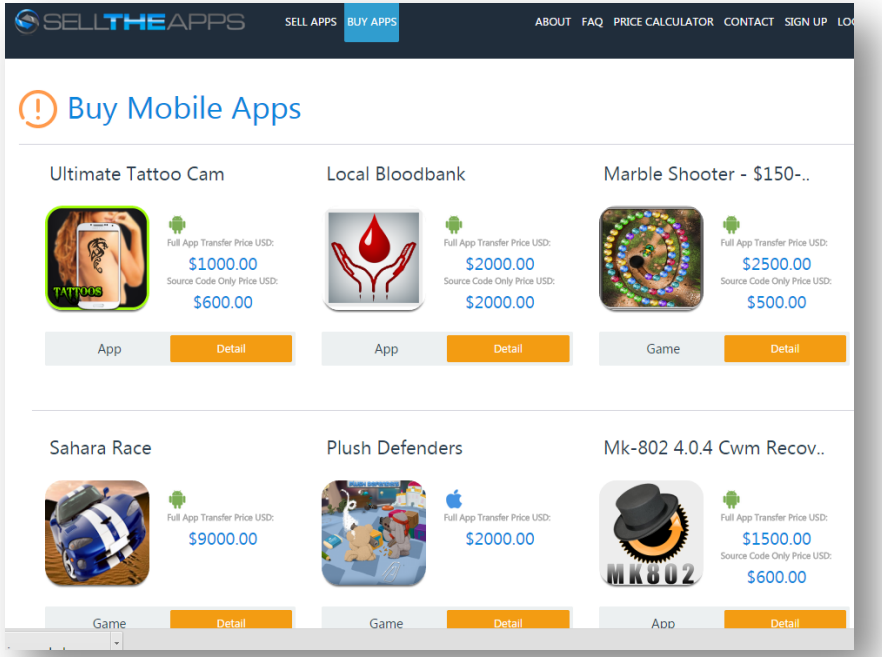
This app deploys with Military Bases, Military Ranks, Military Ribbons, Military Quizzes, a unique and integrated Deployment Tracker, and a rich set of social features. The perfect reference for US Soldiers.

- 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

Eleven Paths

Tacyt Demo 3:

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?...

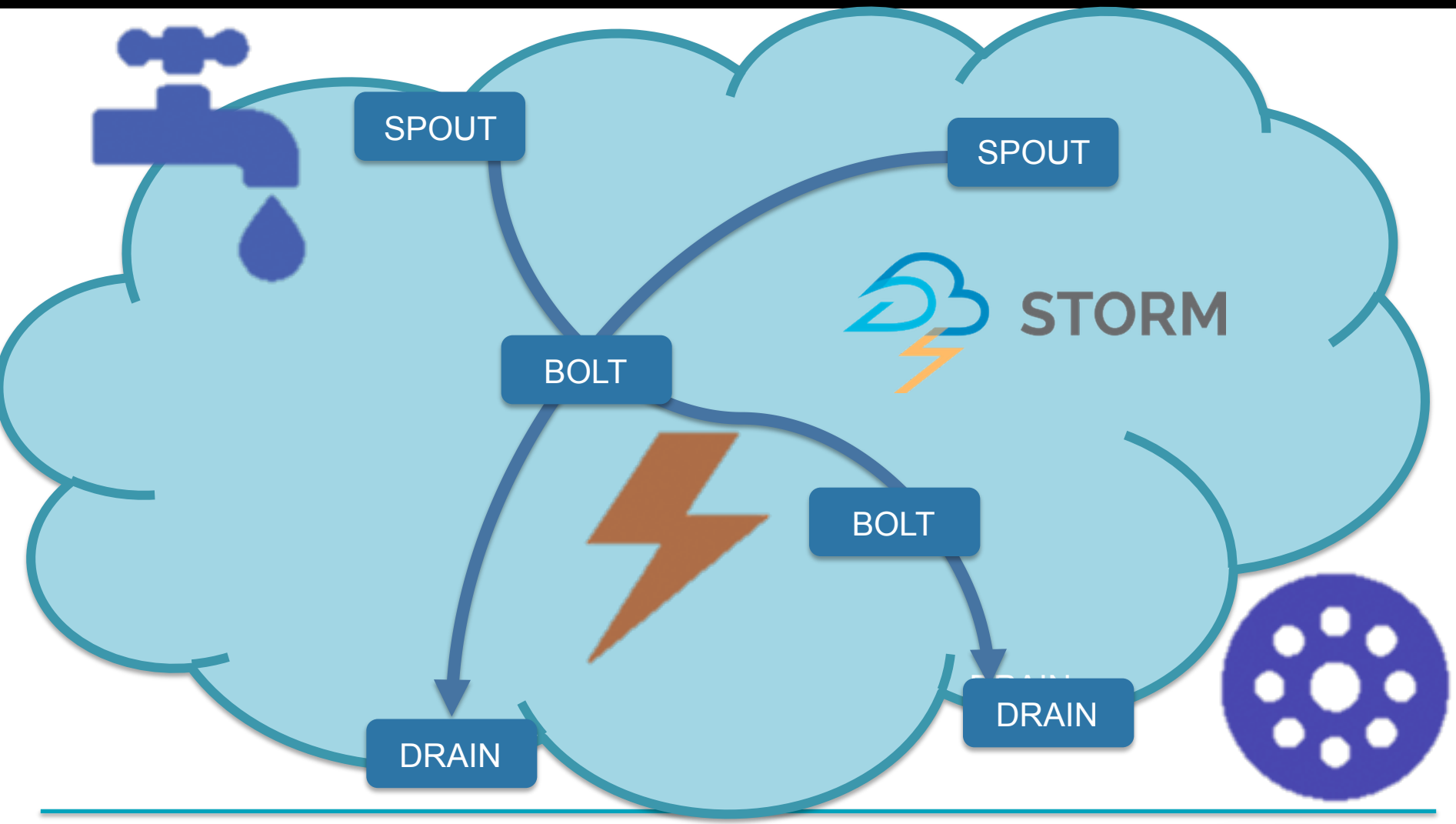
Tacyt Demo 4:

JSDialers

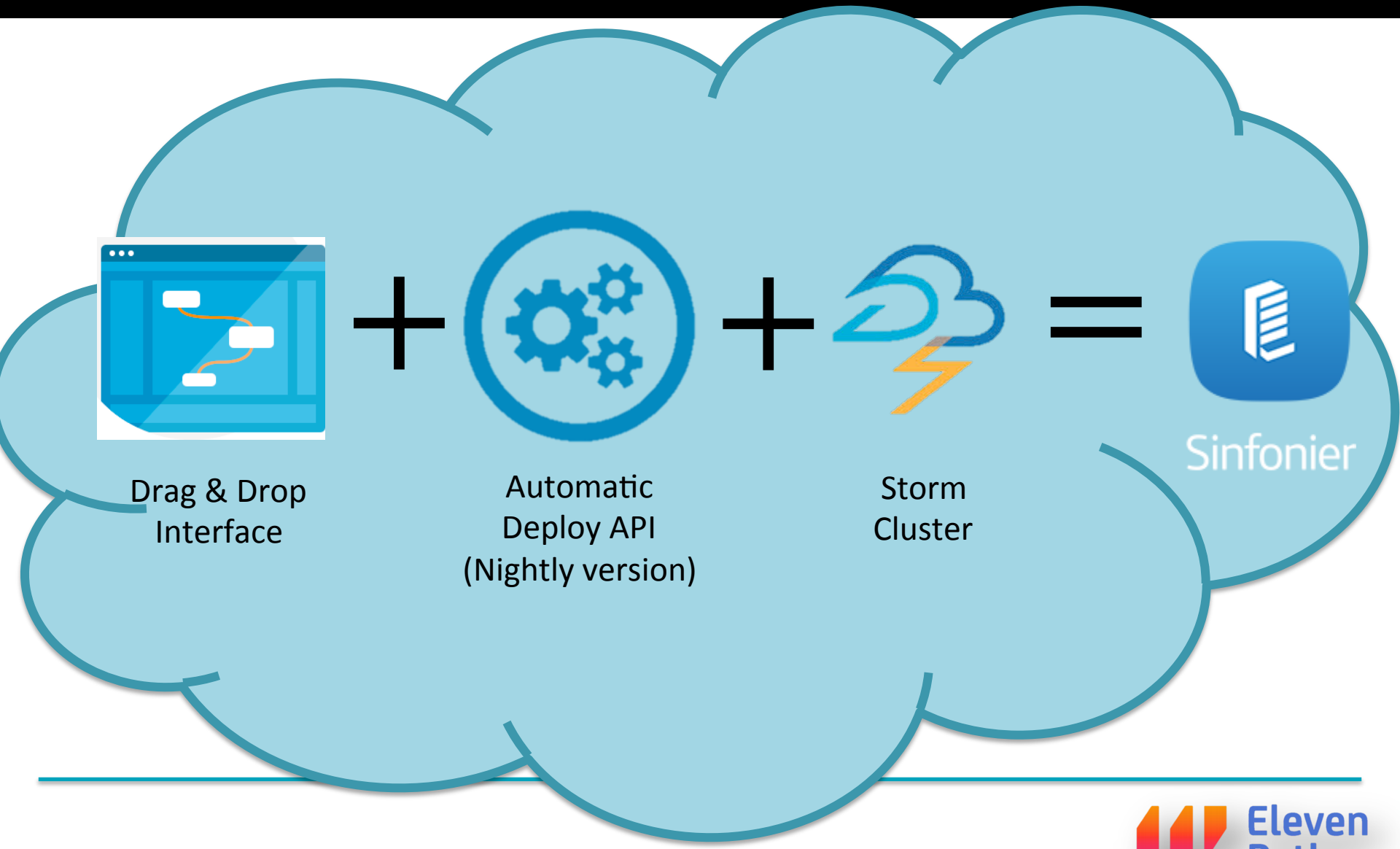
Tacyt

- 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! "


SPOUT
SPOUT
STORM
BOLT
BOLT
DRAIN
DRAIN

How It works

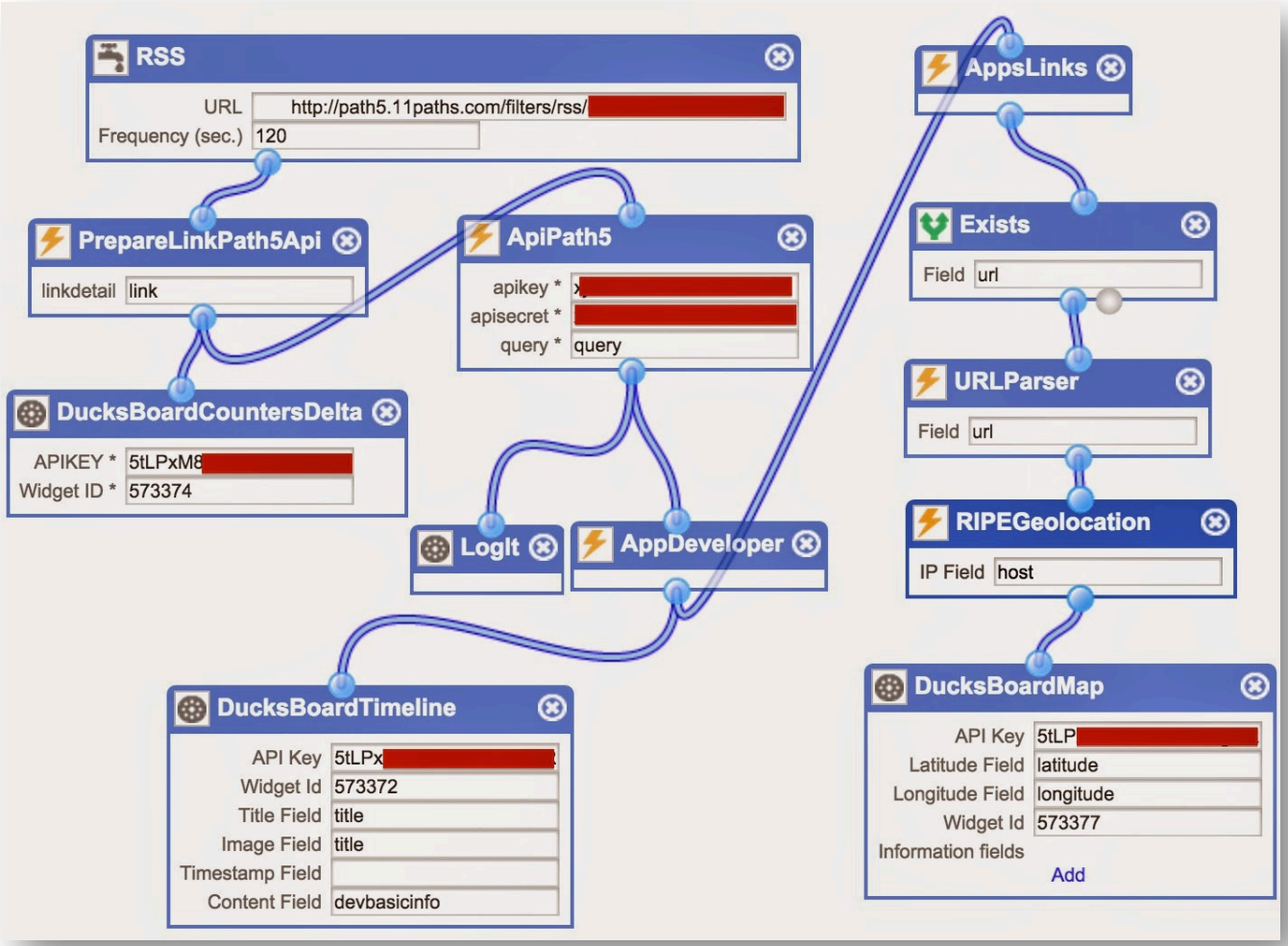


Sinfonier Tacyt Faast

Eleven Paths

Sinfonier Topologies

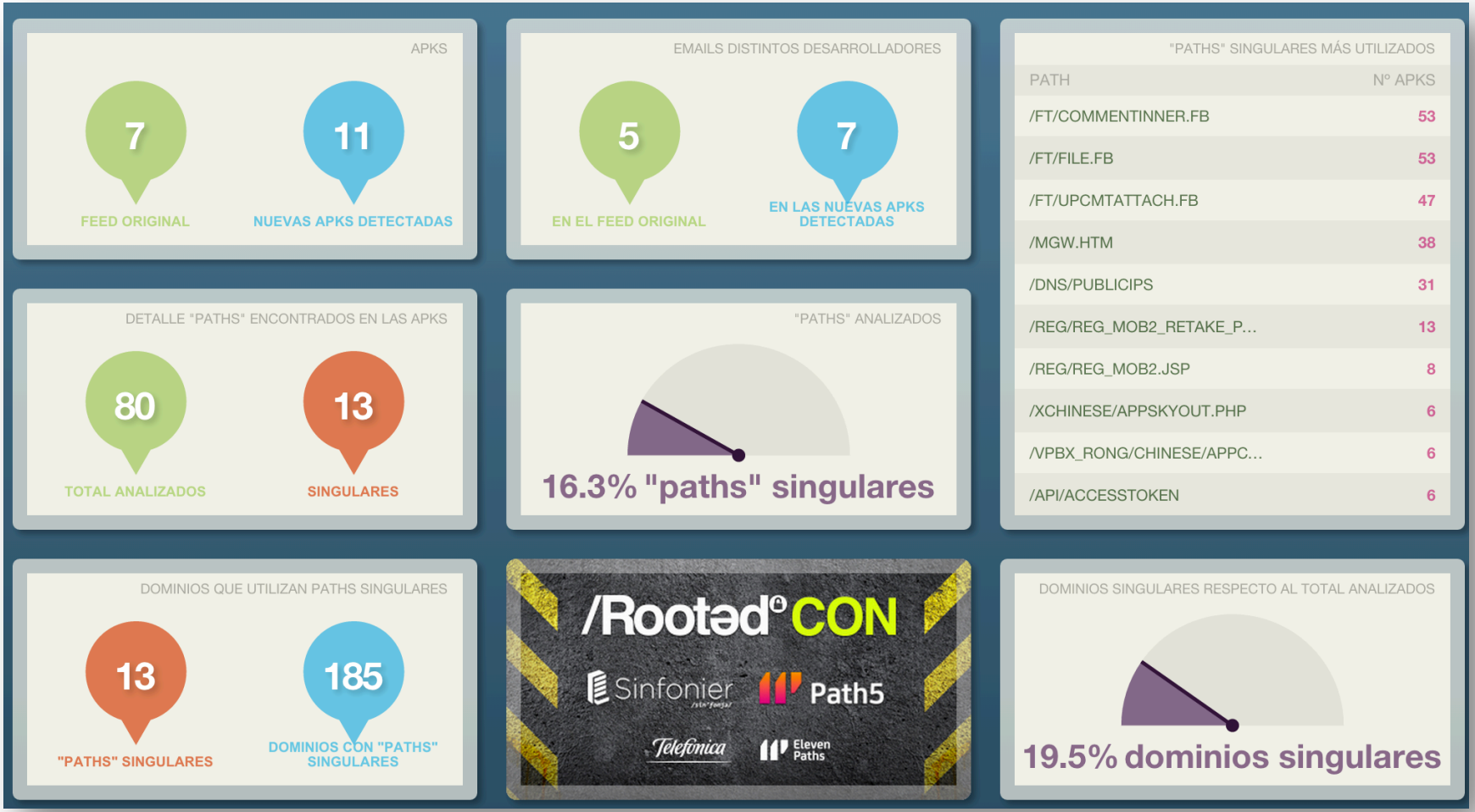
Sinfonier Tacyt Faast



Eleven Paths

Tacyt + Sinfonier

Sinfonier Tacyt Faast

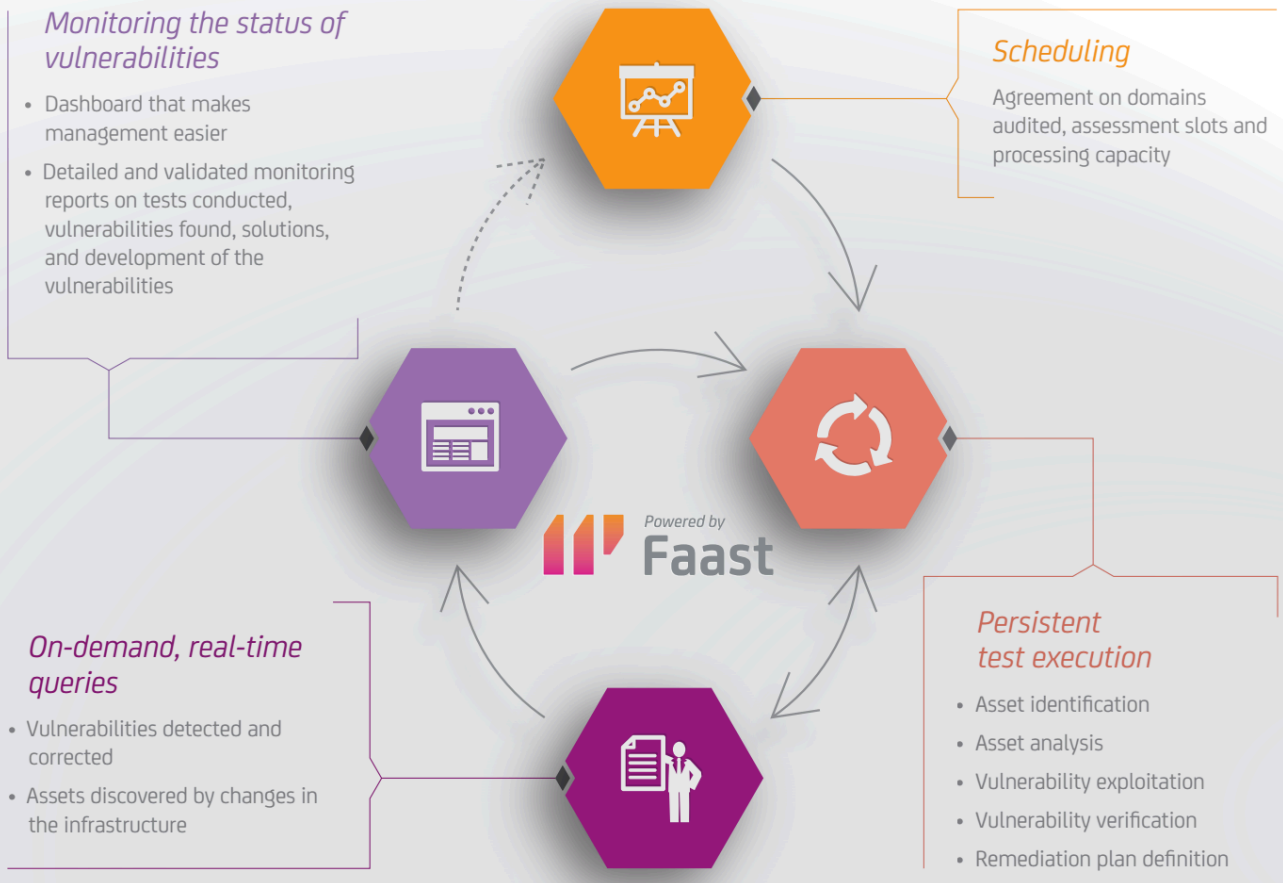


Eleven Paths

Faast (Vamps)

Sinfonier Tacyt Faast

How it works



Eleven Paths

Conclusions

- 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 vulnerabilites in a persistent way

Questions?

- If you want give a try to TACYT, contact me!
- http://www.elevenpaths.com
- Chema Alonso

  @chemalonso
- chema@11paths.com
- http://www.elladodelmal.com