

Malware Analysis of Pokemon Go “with droidjack”

@bunseokbot

이거 개중요

droidjack 3.x 버전이 공개되었다



개이득 (by /bin/bash)



그래서 약간 분석해봤다

깊게하긴 귀찮다.. 시간되면 하겠는데






같은 인증서가 사용된 앱

Apps signed by this certificate:

	Name	Package	Version Code	Added
	Happy Street	com.godzilab.happystreet	1004006	2013-10-16 13:55:01
	TATA Dialers UAE	com.revesoft.mobiledialer.voip_souk.tata_dialers_UAE_33003	303004	2014-08-28 13:17:33.576129
	iGO	com.navngo.igo.javaclient	235654	2014-09-25 07:01:19.970057
	WiFiKill	me.paranoid.wifikill	2020	2014-05-06 10:45:34.340432
	Angry Birds	com.rovio.angrybirdsstarwars.ads.iap	1220	2013-10-16 14:23:02
	Europe	com.tomtom.europe	132	2014-08-02 16:18:54.271971
	ORDO Pro	com.free.alpha.manager	131	2013-10-16 14:19:08
	Drag Racing	com.creativemobile.DragRacing	83	2013-10-16 14:27:06
	Drag Racing	com.creativemobile.DragRacing	81	2013-09-26 13:34:25

<https://www.androidobservatory.org/cert/ECE521E38C5E9CBEA53503EAEF1A6DDD204583FA>









왜 이렇게 같은 인증서가 많은가?

 apktool.jar	2014년 8월 10일 오전 4:16	8.2MB	Java JAR 파일
 certificate.pem	2010년 5월 5일 오전 8:51	1KB	프린트...아카이브
 key.pk8	2010년 5월 5일 오전 8:52	633바이트	도큐먼트
 SandroRat.apk	2014년 9월 22일 오전 3:49	216KB	도큐먼트
 signapk.jar	2008년 11월 5일 오전 8:14	7KB	Java JAR 파일

자체 Signing할 인증서가 있어서 같은 인증서가 뜬거였다

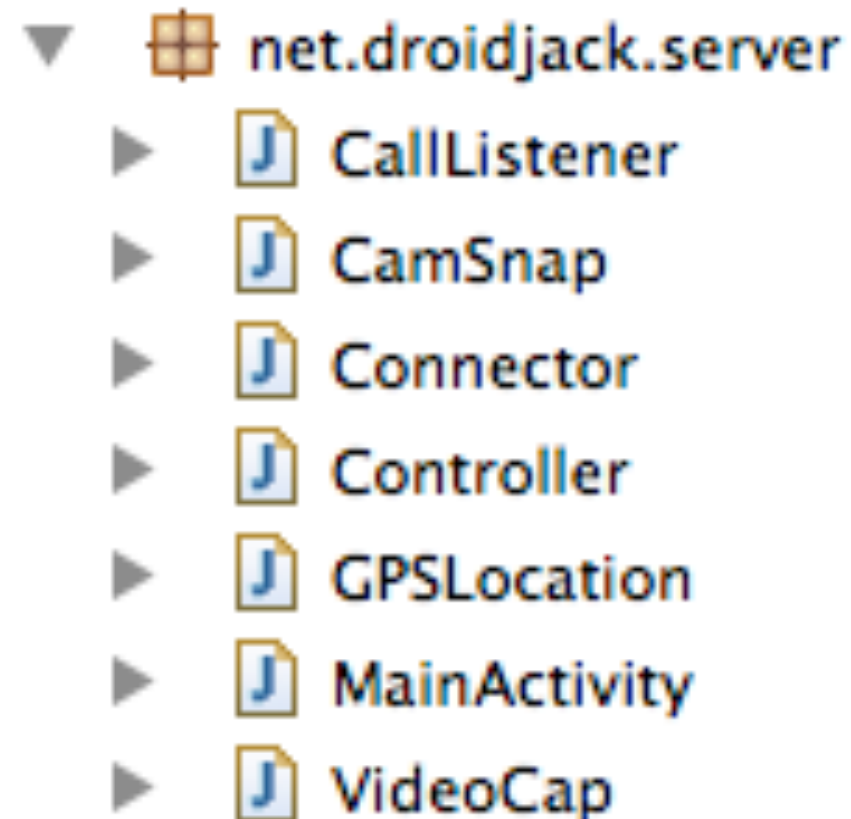
발견된 악성코드 내 package

in Pokemon Go malware

- ▼  net.droidjack.server
 - ▶  CallListener 휴대폰의 전화 상태 (수, 발신) 정보를 가져온다
 - ▶  CamSnapDJ 전면, 후면 카메라
 - ▶  Connector 부팅이 완료되면 Controller 서비스를 시작한다
 - ▶  Controller GPS, Call, Camara, Video를 실제 조종한다
 - ▶  GPSLocation 네트워크 정보, 위치 정보, 단말기 정보를 전송한다
 - ▶  MainActivity 실행되면 Controller 서비스를 활성화시킨다
 - ▶  VideoCapDJ 전면 카메라로 비디오를 촬영한다

droidjack 에서 Inject 하는 APK

SandroRat.apk



버전 차이때문에 일부 다른건 있지만 똑같다 허허

통신 서버

```
public class br
{
    protected static String a = "pokemon.no-ip.org"; C&C 서버 주소
    protected static int b = 1337; C&C 서버 포트
    protected static byte c = -1;
}
```

Domain Whois Information

IP Address	8.23.224.110
Country	US
Registrar	VITALWORKS..
E-mail	<u>domains@no-ip.com</u>

<http://whois.domaintools.com/no-ip.com>

Server Information

IP Address	88.233.178.130
Country	TR (Turkey)
Netname	TurkTelekom
description	TT ADSL-TT net_gay

<http://whois.domaintools.com/88.233.178.130>

현재 no-ip.org 에서 차단되어 '<http://blog.alzac.co.kr/711>' 내용을 참고하였음

앤 어디서 나왔는가

App Name: 앱 이름

File Name: 파일명

Dynamic DNS: DDNS (무려 알아서 생성해준다)

Port Number: Default Port

Bind with another APK

File: 원하는 다른 APK와 bind 하게 해줌

☐ Bind?

스텔스 모드 (프로세스에 안뜬단다)

☐ Stealth Mode

droidjack 제공 기능


Android Remote Administration Tool


+ Inbuilt APK Tool
+ File Voyager
+ SMS Trekker
+ Call Manager
+ Contacts Browser
+ Remote Eyes
+ Remote Ears
+ Browser
+GPS Locator
+ Message Toaster
+ App Manager
+ Detailed Info
+ More


- 정상 파일에서 Injection 하는 기능
- 기기 내 파일 내용 제공
- SMS 쓰기, 읽기, 원격 삭제
- 전화내용 녹취, 삭제 등
- 연락처 내용 읽기, 쓰기, 삭제
- 전, 후면 카메라 이용 촬영 & 녹화
- 브라우저 북마크 읽기, 브라우저 원격 호출
- GPS 위치 추적
- 기기에 메시지 출력 (Toast Message, AppPush)
- IMEI, MAC Address, 통신사업자 정보, 루팅 여부 확인
- .. 등등


실제로 모두 제공할까?


과연..?

Devices 

Generate APK 

Theme 


About 

Lounge 

Country	Phone Number	Model	Manufacturer	Version	IP Address	ID
그러하다						

Port:

Status: Not listening for new connections

Reception  Off

DroidJack says:

Wanna suggest/report/comment anything? Write to me! :)

동작 방식

- no-ip.org 무료 DDNS 서비스는 아예 생성할 때 부터 자동으로 생성해준다
- 심지어 기능별 세팅과 스텔스 모드에 대해서도 설명되어있다.
- 내가 bind 하고싶은 앱이 있다면 [ex) 스미싱몬..] 원하는대로 해준다
- 그리고 기능같은 경우에는 SandroRat.apk 라는 앱에서 알아서 생성되어있다.
- Generate를 누르면 합쳐진 APK가 생성된다.
- Injection할 때 에는 apktool을 사용한다.
- 앱을 Signing할 때에는 signapk.jar을 사용한다
- 이 droidjack 만의 인증서를 가지고 있다.

사실

- 실제 테스트이랑 소스코드 분석한것도 올리고 싶었는데 넘나 귀찮아서 안했다.
- 절대 못하는게 아니라 안했다
- 사실 하긴 했는데 올리기 좀 그런게 많아서.. ㅈㅈ
- 그리고 이거 합쳐서 돌려봐야 요즘 백신에 다 걸린다고 한다
- 결론 : 코이먹고싶다

End

@bunseokbot