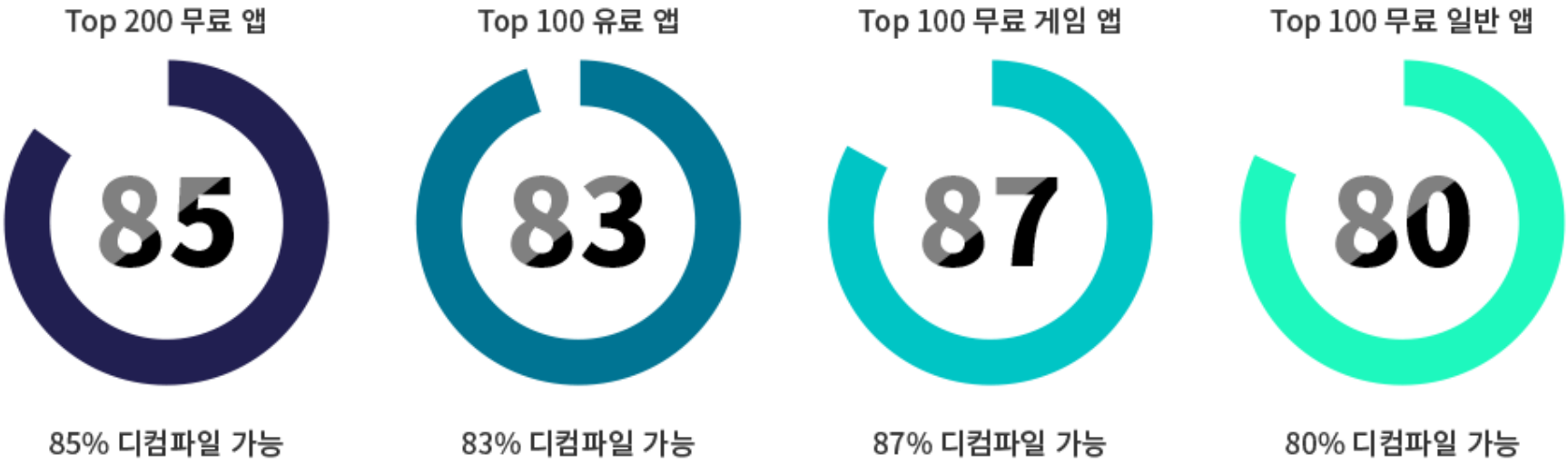
모바일 앱 해킹에 대한 방어의 필요성

조민재(Johnny Cho, johnny@se.works)
SEWORKS, Inc.

WHY? WHY!

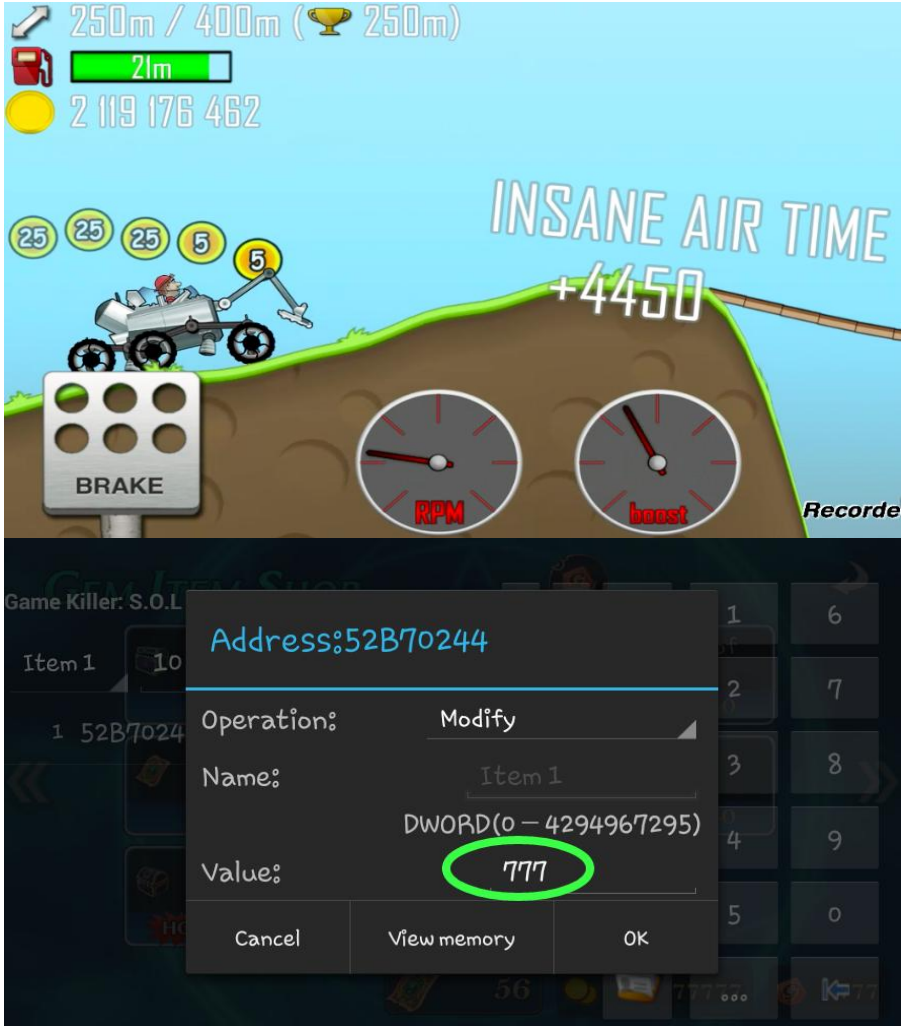
앱 해킹 위협

SEWORKS가 행한 구글 플레이 앱스토어의 내부 리서치 결과



1. 메모리 해킹


20 Found
Level:0-1
$:5
Score:0
score: 0
events_allocated: 9
fast_fwd_counter: 0
enemies_allocated: 1
health: 20
Score: 0
Change Game Speed


250m / 400m (250m)
2 119 176 462
INSANE AIR TIME
+4450
BRAKE
RPM
boost
Address:52B70244
Operation:
Modify
Name:
Item 1
DWORD(0 – 4294967295)
Value:
777
Cancel
View memory
OK

2. 소스코드 난독화

Unobfuscated Code:

```
C:\DashOProEval 4.2\samples\tapasya\src>javap
Section
Compiled from "Section.java"
public class Section extends java.lang.Object{
    public Section();
    public static void main(java.lang.String[]);
    public static void printStudentInfo(Student);
}


C:\DashOProEval 4.2\samples\tapasya\src>javap
Student
Compiled from "Section.java"
class Student extends java.lang.Object{
    Student();
    public void setStudentName(java.lang.String);
    public void setStudentID(java.lang.String);
    public java.lang.String getStudentID();
    public java.lang.String getStudentName();
    public void setScore(double, double, double);
    public double getMathsScore();
    public double getEnglishScore();
    public double getHistoryScore();
    public double calcAverage();
}
```

After Identifier Renaming:

```
c:\DashOProEval 4.2\samples\tapasya\output>javap
Section
Compiled from ""
public class Section extends java.lang.Object{
    public Section();
    public static void main(java.lang.String[]);
    public static void a(b);
}


c:\DashOProEval 4.2\samples\tapasya\output>javap b
Compiled from ""
public class b extends java.lang.Object{
    public b();
    public void a(java.lang.String);
    public void eval_b(java.lang.String);
    public java.lang.String a();
    public java.lang.String eval_b();
    public void a(double, double, double);
    public double eval_c();
    public double eval_d();
    public double eval_e();
    public double eval_f();
}
```

3. 바이너리 난독화

Official Version (Tap Titans)

Starting Point

Pirated Version (Tap-Tap Heroes)

Starting Point

4. 암호화 키

What is this magic encryption key used by any and all Snapchat app?

M02cnQ51Ji97vwT4

You can find this (in the Android app) in a constant string located in com.snapchat.android.util.AESEncrypt; no digging required, it is quite literally sitting around waiting to be found by anyone.

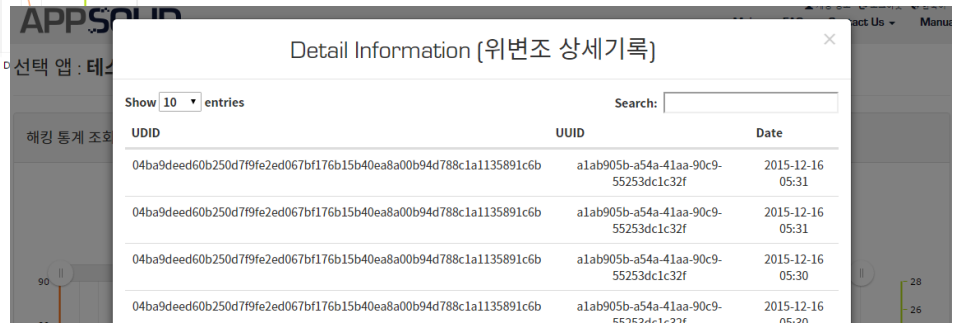
On a more positive note (perhaps), in the 3.0.4 (18/08/2013) build of the Android app, there is - oddly enough - a second key!

1234567891123456

Again, this is just sitting around in AESEncrypt waiting to be found. These two static keys used for encryption lead us on to our big topic under encryption.

출처 : GibsonSec
http://gibsonsec.org/snapchat/snapchat_gibsonsec.txt

5. 실시간 모니터링



4th SNC

APP SOLID.

모바일 앱 해킹 대응 A-Z

- 개발
  - 메모리 해킹 방지
  - 소스코드/바이너리 난독화
  - 앱 위변조 방지
  - 암호화 통신
  - 서버 측 검증 >>>> 클라이언트 측 검증
  - 암호화키, 토큰, ID 등을 절대 하드코딩하지 않는다!
- 운영
  - 앱 해킹 커뮤니티 모니터링
  - 보안에 도움이 될 적절한 파트너를 찾으세요!

Thank you!

조민재(Johnny Cho
johnny@se.works