

침해된 정상 사이트를 C2 서버로 사용하는 AI 기반 난독화 악성 앱 분석 보고서

A asec.ahnlab.com/ko/91077

ATCP

November 17, 2025



1. 개요

국내 유명 택배 회사를 사칭한 악성 앱은 이전부터 꾸준히 유포되고 있으며, 유포자는 Anti-Virus(AV) 탐지를 회피하기 위해 다양한 기법을 사용하고 있다.

대표적으로 난독화와 패킹 기법이 활용되고 있으며, 현재까지도 이러한 기법이 적용된 악성 앱이 다수 발견되고 있다.

최근 AI 기술의 발전으로, 기존 난독화 및 패킹 솔루션에 AI를 접목해 악성 앱을 제작·유포하는 사례도 발견했다.

특히 정보 탈취 후 데이터를 유출하는 과정에서 공격자는 정상 사이트를 C2 서버로 악용하고 있는데, 이는 해당 사이트가 침해되어 관리자가 인지하지 못한 상태에서 외부 프로그램을 통해 C2 역할을 수행하고 있음을 추측할 수 있다.

또한 공격자는 국내 포털에서 운영되는 블로그에 C2 서버 주소를 하드코딩하고, 앱 실행 시 이를 불러와 C2 서버로 활용하는 방식으로 탐지를 더욱 어렵게 만들고 있다.

본 보고서에서는 AI를 활용한 Proguard 난독화 사례와 C2 서버 확보 방식, 그리고 데이터 유출에 대해 분석한 내용을 소개한다.

2. 분석

2.1. APK 정보

분석 대상 APK의 메타 정보와 주요 기능은 다음과 같다.

항목	내용
앱 이름	한진택배
패키지 이름	com.golfpang.golfpanggolfpang
크기	1,098,850 bytes
MD5	d42a2c80e486c763b310237bef115ef3
SHA1	d14f20abeae95d9ed29ea7cb17545fd0a3f70c6f
SHA256	6c99fed293a7b23cae5d6e746d1272a24e28dcce6db2942ae47372726d9f12a7
특징	SMS 정보 탈취 갤러리 정보 탈취 단말기 정보 탈취 국내 포털 사이트 블로그 활용 C2 서버 은닉 침해사고 추정 사이트 활용 데이터 유출

그림 1. 악성 앱 메타 정보

2.2. AI를 활용한 Proguard 난독화

AndroidManifest.xml에서 명시한 컴포넌트 외 사용되는 클래스, 함수, 변수 정보가 의미 없는 한글 8자리로 구성되어 있으며, 리소스 이름이 변동이 없는 것으로 보아 Proguard를 활용한 난독화가 적용된 것으로 추정된다. 또한, Proguard 난독화 적용 시 사용한 문자열의 경우 8자리 의미 없는 한글로 설정했음을 추측할 수 있다.

```

package com.golfpang.golfpanggolfpang;

import android.app.Activity;
import android.content.Intent;
import android.os.Bundle;
import android.os.Handler;
import androidx.activity.저소코쳐나기구부;

public class shtextiles extends Activity {
    public static final int 서키코다누지차루;

    @Override // android.app.Activity
    public final void onCreate(Bundle bundle0) {
        super.onCreate(bundle0);
        this.startActivity(new Intent(this, namucpa.class));
        new Handler().postDelayed(new 저소코쳐나기구부(4, this), 15000L);
        this.finish();
    }
}

```

그림 2. 변수 이름 한글 난독화

```

public final void 부추추러노누조가() {
    Intent intent0 = new Intent(this, sungeunpnp.class);
    if(Build.VERSION.SDK_INT >= 26) {
        this.startForegroundService(intent0);
    }
    else {
        this.startService(intent0);
    }

    new Handler().postDelayed(new 기기히거라어타소(this, 2), 1000L);
    new Handler().postDelayed(new 기기히거라어타소(this, 3), 2000L);
}

```

그림 3. 클래스 이름 한글 난독화

- >  android
- >  androidx
- ▼  com
 - ▼  golfpang
 - ▼  golfpanggolfpang
 - >  gddfsder
 - >  namucpa
 - >  shtextiles
 - >  sungeunpnp
 - >  가어추포마도두티
 - >  고시푸보나저누두
 - >  기기히거라어타소
 - >  러아허쿠사바주타
 - >  소어치버니바가저
 - >  수오코주저노디차
 - >  수터푸마라사우고
 - >  어바리구러초티더
 - >  처소코처나기구부
 - >  커바누가사호치머
 - >  투히푸구저디키바
 - >  포마나소타비수토
- >  kotlinx
- >  okhttp3
- >  retrofit2

- ▼  가투바처라미모러
 - >  고시푸보나저누두
 -  기기히거라어타소
 -  러아허쿠사바주타

그림 4. 클래스 및 함수 한글 난독화

2.3. 정적 분석

권한이 허용되면 앱은 무작위로 생성한 운송장 번호를 기반으로 실제 배송 조회 사이트에 접속한 화면을 띄워 정상 앱처럼 위장한다.

```
case 2: {
    namucpa0.getClass();
    try {
        Random random0 = new Random();
        int v = random0.nextBoolean() ? 10 : 12;
        double f = random0.nextDouble();
        Intent intent0 = new Intent("android.intent.action.VIEW");
        intent0.setData(Uri.parse(("https://www.hanjin.com/kor/CMS/DeliveryMgr/WaybillResult.do?mCode=MN038&schLang=KR&wb1num=" +
        intent0.addFlags(0x10000000);
        namucpa0.startActivity(intent0);
    }
    catch(Exception exception0) {
        exception0.printStackTrace();
    }
    return;
}
```

그림 5. 랜덤 운송장 번호 조회 페이지 접속

2.4. 동적 분석

앱 실행 시, 악성 행위 수행을 위해 필요한 권한을 사용자에게 요청한다.

그림 6. 권한 요청

MD5

46a05b40410e26998b617240c1cc054e

52cd352cd52189ff202dc2af5c113c81

7b80a53b40a377d95e3f61d60c5de9fc

8223ec9a2a9236efaca2ffb5812bd560

96076a7576ed55b2f5d057f7f73ce799

추가 IoC는 ATIP에서 제공됩니다.

URL

[http://dhct\[.\]co\[.\]kr/](http://dhct[.]co[.]kr/)

[http://mlsm\[.\]or\[.\]kr/](http://mlsm[.]or[.]kr/)

