

# IRATA 악성코드 분석 보고서 - ASEC

A asec.ahnlab.com/ko/91274

ATCP

November 27, 2025



## 1. 개요

모바일 시장의 성장에 따라 안드로이드 플랫폼을 대상으로 한 악성 앱의 수가 증가하고 있다.

이에 대응하여 Google은 Google Play Store에서 악성 앱을 탐지하고 차단하기 위해 AI 기반 악성 앱 탐지, 개발자 계정 규제, 앱 심사 강화 등의 보안 기능을 지속적으로 개선하고 있다.

그러나 일부 국가에서는 국가 제재 및 정부의 인터넷 통제 정책으로 인해 Google Play Store 접근에 제한이 있었다.

대표적인 사례로 이란이 있으며, 미국 중심의 경제 제재로 인해 Google Play Store 접근이 제한되었고, 이란 내 인기 앱들이 자주 삭제되는 현상이 반복되었다.

이러한 환경에서 사용자들은 공식 스토어 대신 서드파티 마켓이나 외부 사이트를 통해 APK 파일을 직접 다운로드하는 방식으로 앱을 설치하게 되었다. 그 결과, 악성 앱이 쉽게 유포될 수 있는 환경이 형성되었다.

이에 따라 비공식 앱 설치 경로를 이용해 이란을 대상으로 한 악성 앱이 다수 보고되고 있다.

그 중 IRATA 악성 앱은 스미싱을 통해 유도된 피싱 페이지에서 다양한 앱을 가장하여 유포되고 있다.

본 문서에서는 2025년 기준 수집된 IRATA 악성 앱에 대한 분석 정보를 포함한다.

## 2. IRATA

IRATA(Iranian Remote Access Trojan)는 안드로이드 운영체제를 대상으로 하는 악성코드 패밀리이다.

초기(2022년) 유포 방식은 정부 기관을 사칭한 문자 메시지를 통해 이루어졌으며, 현재는 도박, 성인 게임, 포르노 콘텐츠, 대출 서비스 등 다양한 목적의 앱으로 가장하여 악성 앱을 배포하고 있다.

실행 시 가장한 앱의 피싱 페이지를 제공하며, 설치 후 피해자의 민감한 정보를 탈취하거나 원격 제어 기능을 수행한다.

B4A(Basic4Android) 라이브러리 기반으로 개발되었으며, 현재까지도 동일한 개발 환경을 유지하고 패킹 및 난독화 기법을 적용하여 안티 바이러스를 회피한다.

## 3. 앱 실행 화면

IRATA 악성 앱은 [그림 1]과 같이 성인 콘텐츠, 도박, 쇼핑몰, 사법부 관련 앱 등 다양한 형태로 가장한다.

앱 실행 시 SIM 카드에 저장된 국가 코드를 확인하며, 이란이 아닌 국가의 경우 [그림 2]와 같은 “해당 앱은 이란에서만 이용 가능합니다”라는 알림 메시지를 표시하고 즉시 종료한다.

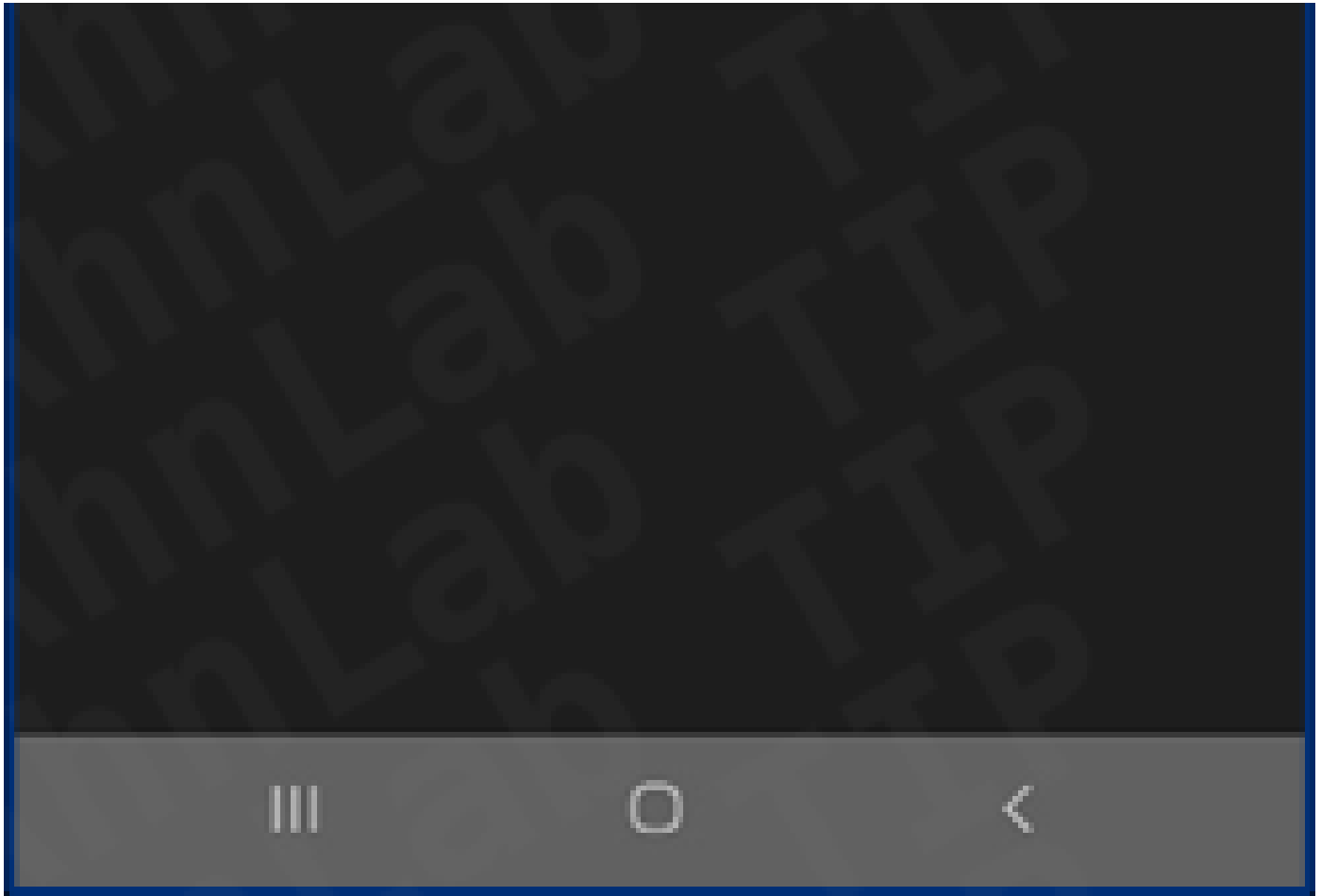


그림 1. 악성 앱 아이콘

خطا

برنامه فقط در ایران قابل اجرا میباشد.

OK



## 그림 2. 타 국가 실행 시 사용 불가 문구 및 종료

이러한 방식은 특정 국가를 대상으로 한 악성 앱에서 동적 분석 회피 목적으로 자주 사용된다.

단말기의 국가 코드를 이란으로 설정하면, 악성 앱은 [그림 3, 4]와 같이 피해자에게 악성 행위 수행에 필요한 접근 권한을 요청하고 피싱 페이지를 표시한다.

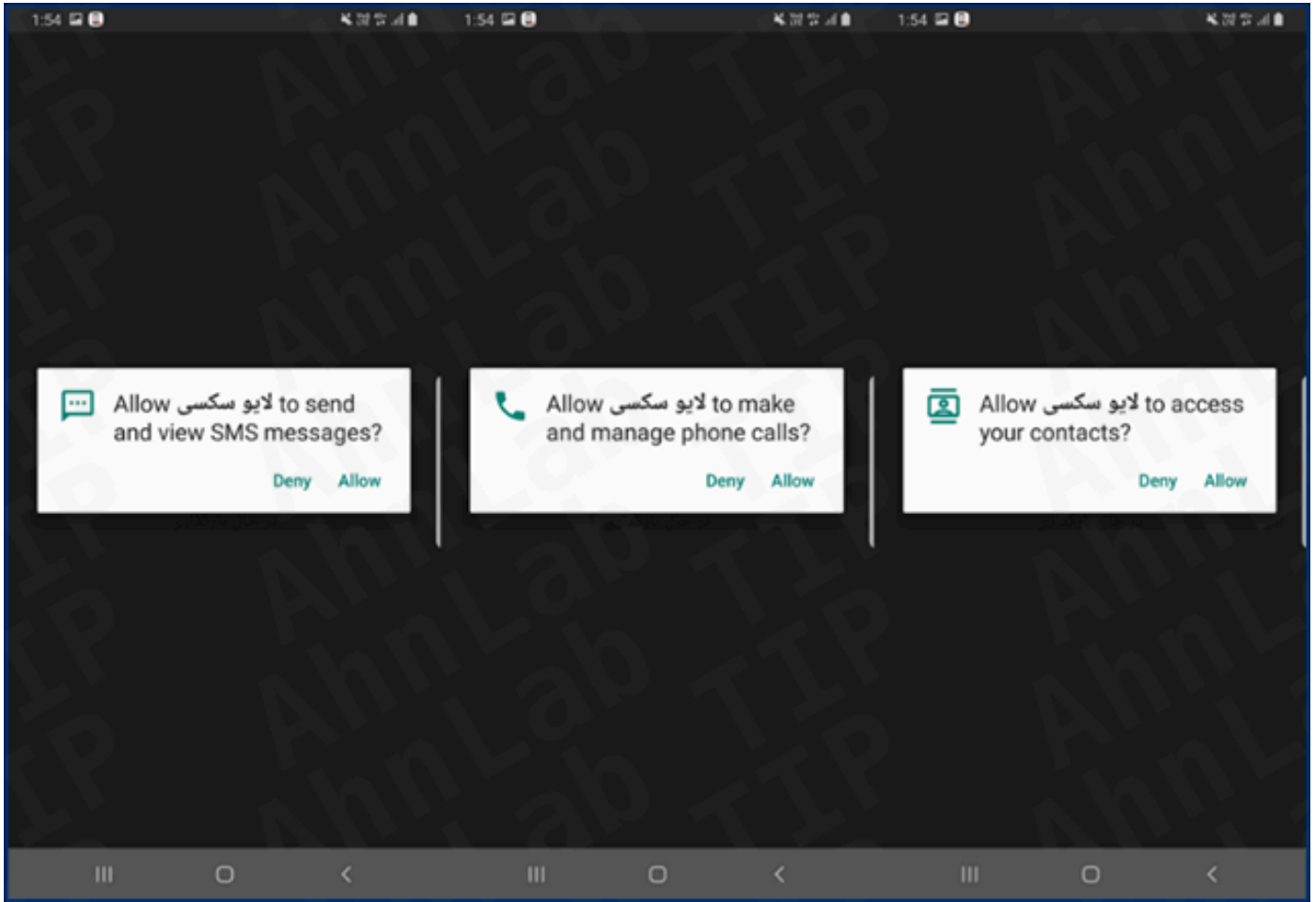


그림 3. 개인정보 탈취를 위한 권한 요청

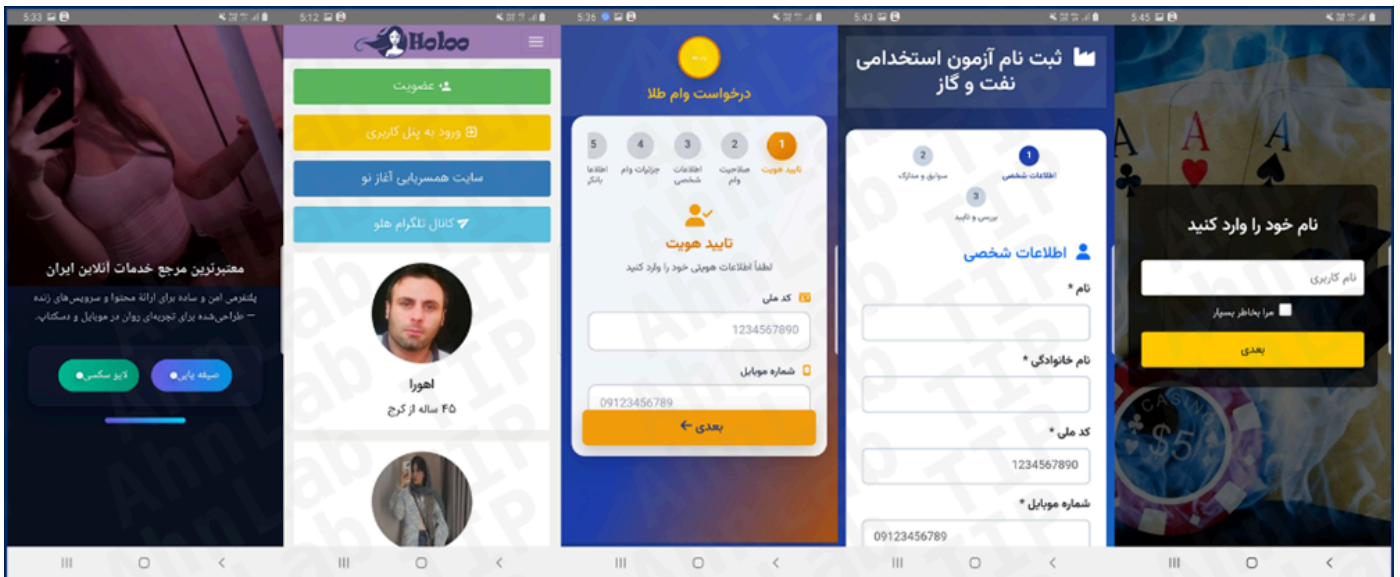


그림 4. 악성 앱의 유형별 피싱 페이지

피싱 페이지는 피해자에게 콘텐츠 이용에 대한 결제를 요구하며, [그림 5]와 같이 Cloudflare 기반의 HTML 페이지인 결제 피싱 페이지 URL을 로딩한다.

```
[+] Entered: com.xnotice.app.main._dwc_overrideurl  
arg[0]: https://gfez.space/g%E2%80%8C%E2%80%8C%E2%80%8C%E2%80%
```

### 그림 5. 결제 피싱 페이지 로드

결제 피싱 페이지는 [그림 6]과 같이 이란에서 공인된 전자결제 서비스 제공업체인 “Behpardakht Mellat”를 사칭하며, 금융 자격 증명 정보를 입력을 유도한다.



پرداخت اینترنتی به پرداخت ملت



## اطلاعات پذیرنده

نام پذیرنده : رایان ارتباط

شماره پذیرنده: 2374783

آدرس وب سایت: <https://www.rayanertebat.ir>

مبلغ قابل پرداخت : 500,000 ریال

## اطلاعات کارت

زمان باقی مانده : 08:41

شماره کارت



شماره شناسایی دوم (CVV2)

تاریخ انقضای کارت

سال

ماه



그림 6. 결제 피싱 페이지

이후 피해자가 앱을 종료하거나 일정 시간이 경과하면 앱 아이콘을 은닉한다([그림 7] 참조).

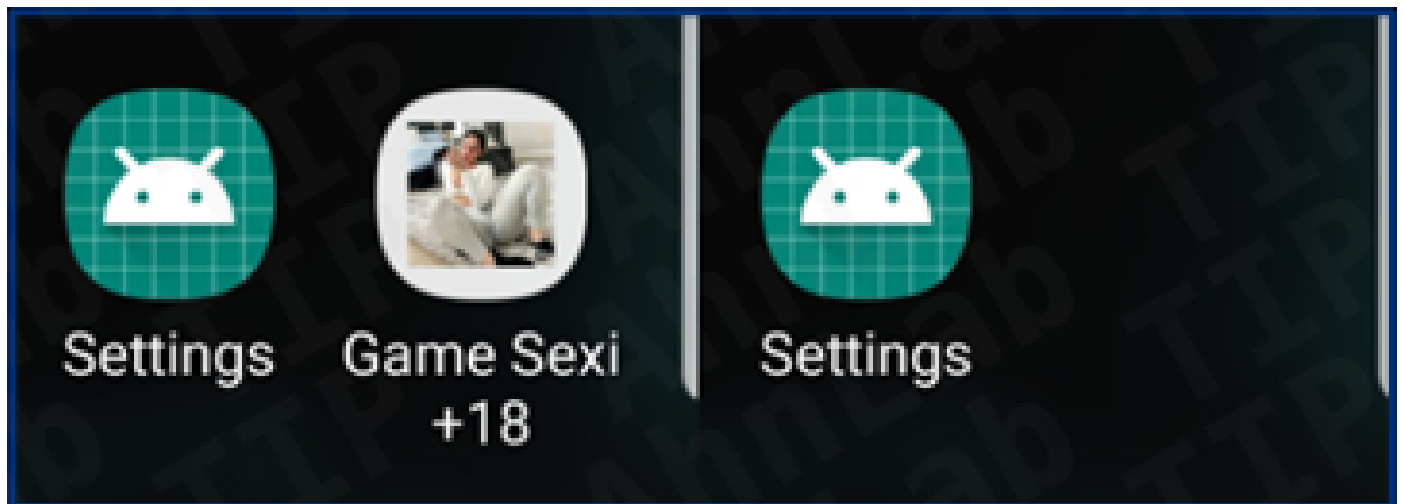


그림 7. 아이콘 은닉

금융 자격 증명이나 개인정보 등 목표한 정보를 탈취한 이후, 피해자 단말기에 저장된 연락처 목록 및 통화 기록을 대상으로 스미싱 문자 메시지를 유포한다([그림 8, 9] 참조).



그림 8. 단말기 내 연락처 및 통화 기록을 대상으로 스미싱을 유포

وام خرید طلا

مزیت ها

- ✖ غیر حضوری
- ✖ پشتیبانی 24 ساعته
- ✖ بدون نیاز به پیش پرداخت
- ✖ تأیید صلاحیت وام با احراز هویت شما در لحظه
- ✖ پشتوانه ای محکم برای آینده شما و عزیزانتان
- ✖ اقساط انعطاف پذیر تا پنج سال

♦ برای مشاهده اطلاعات و درخواست وام به سایت زیر  
مراجعه کنید ♦

♦ سایت معتبر وام اسپیس: 

## 그림 9. 스미싱 내용

MD5

4cc054a0455504f95174af880915588a

590cd2d654bb955066f381d9d7ad003f

5aa6d5f023b2b441ad4d48e25fccaa93

a0b1c0a462ea52371209a23f3aed5b7e

a2c419cf3856c06fc2ada10bdd4c09d5

추가 IoC는 ATIP에서 제공됩니다.

URL

[http://road0\[.\]duck-jsuv\[.\]com/X\[.\]php](http://road0[.]duck-jsuv[.]com/X[.]php)

[http://road0\[.\]sand-acdr\[.\]com/X\[.\]php](http://road0[.]sand-acdr[.]com/X[.]php)

[http://road1\[.\]sand-acdr\[.\]com/X\[.\]php](http://road1[.]sand-acdr[.]com/X[.]php)

[http://route0\[.\]rain-hoya\[.\]com/X\[.\]php](http://route0[.]rain-hoya[.]com/X[.]php)

[http://route1\[.\]rain-hoya\[.\]com/X\[.\]php](http://route1[.]rain-hoya[.]com/X[.]php)

추가 IoC는 ATIP에서 제공됩니다.

