

Sketchware 기반 악성코드 분석 보고서

A asec.ahnlab.com/ko/91275

ATCP

November 27, 2025



1. 개요

안드로이드 OS 스마트폰 이용자의 증가에 따라, 개발자가 앱을 개발하는 데 편의성을 제공하는 서비스도 발전하였으며 대표적으로 Sketchware가 있다.

Sketchware는 앱 개발 시 어려움을 느끼는 사람들을 위해 공개된 도구로, 단말기 내에서 간단한 기능의 앱을 제작할 수 있도록 지원한다.

그러나 이를 악용하여 악성 앱을 제작하는 사례가 지속적으로 발견되었으며, 대표적으로 Arsink 악성 앱이 있다.

이 악성 앱은 Sketchware를 통해 제작되었으며, 관리자 앱 내 APK 파일을 조작하여 사용자 단말에 설치할 악성 앱을 제작할 수 있다.

현재 Arsink 악성 앱을 변조한 악성 앱들이 텔레그램을 통해 활발히 유통되고 있으며, 본 문서에서는 그중 하나인 “Spider-Rat” 악성 앱 분석 정보를 포함한다

2. Arsink

Arsink 악성 앱은 안드로이드 기기를 대상으로 하는 악성 앱으로, 원격 제어 및 개인정보 탈취를 목적으로 한다. 최초 수집은 2023년 8월로, “Arsink4Rat”이라는 앱이다.

원본 악성 앱을 개발한 것으로 추정되는 개발자는 [그림 1]과 같이 유튜브를 통해 Sketchware를 통한 앱 개발 방법 및 악성 앱 관련 영상을 게시하고 있다.

해당 앱은 자사 및 타사 안티바이러스 제품에서 Trojan/Arsink로 진단하고 있다.

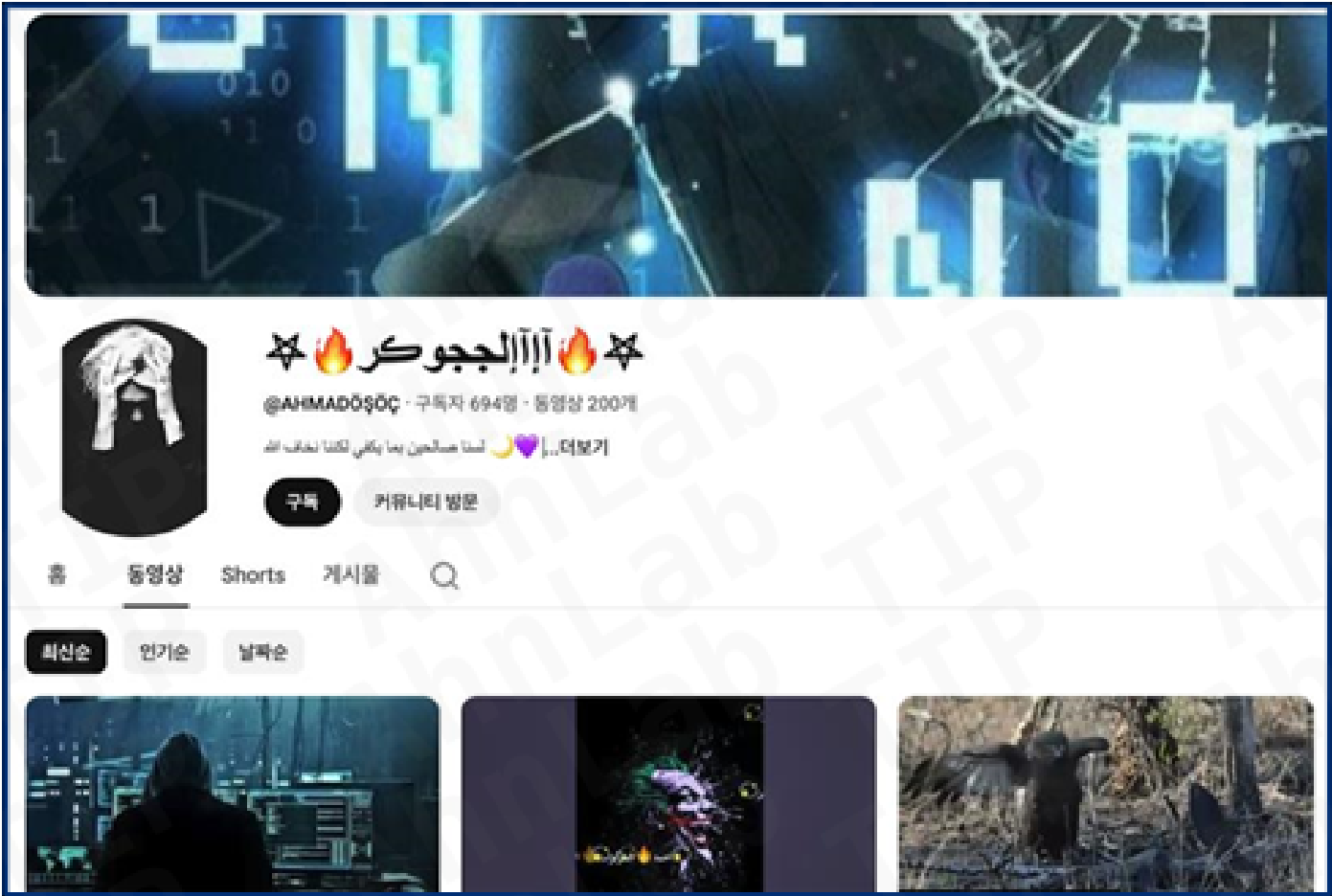


그림 1. Arsink 제작자로 추정되는 유튜브 채널

Arsink 악성 앱을 비롯한 Mod 앱 등은 [그림 2]와 같이 아랍 국가의 해커들을 대상으로 텔레그램 채널을 통해 공유되고 있으며, 이를 통해 다양한 악성 앱이 제작되고 있다.



برلامجج و شروخالت جولاكير ،
5797 Messages



Pinned message #3

GRIM 🦴 🔴 مع معلومات واختيار نقاط الضعف يمكنك استخدامه ع...



AH_army

اختصار

Arab Hacker Army

بعد البوتات التي قد تساعدك

🔧 مصنع بدون حقوق او اعلانات
عربي // English

🔧 @Black_Hisoka1325BOT

🔧 بوت متجر الهاكرز
🔧 @Black_Hisoka1103BOT

🔧 اكبر بوت قواعد بيانات لكل الدول
🔧 @AHDDataBot



그림 2. 아랍 국가 텔레그램 채널

MD5

37877e5d60e2778a311ba86a7a53a1dd

948152cac017e993aeb0e8d2568e7818

cf092628a3f35b82ceb053f562a3b35e

f014a794cf90f3be499485fdbdea3e28

f185dbe27c00c8812d135f406b44cfb3

추가 IoC는 ATIP에서 제공됩니다.

URL

<https://kimo-rat-ee056-default-rtdb.firebaseio.com/FirebaseDB1>

<https://silly-souffle-876668.netlify.app/>

<https://soft.cr3zyblog.com/?p=46>

<https://t.me/+T3aaSxhqymliMjBk>

