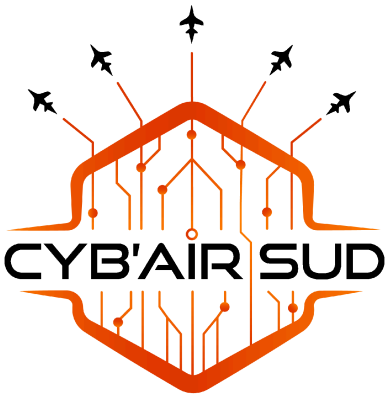


The Kill Chain for Android Malware: Delivery

Abstract for CFP 2025

Speaker: Thibaud PERRARD

Short Description

How does malware reach a phone? This session analyzes modern Android infection vectors: infiltration of official marketplaces, phishing campaigns (smishing), and exploitation of vulnerabilities (0day), persistence.

Detailed Abstract

This presentation offers a technical analysis of delivery vectors that determine the success of an Android compromise. Focusing exclusively on the "Delivery" phase of the kill chain, we will map offensive strategies from large-scale social engineering to pure exploitation of vulnerabilities.

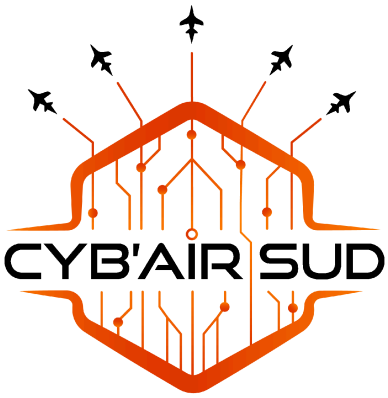
We will first examine the challenge of infiltrating official marketplaces, a tactic relying on bypassing automated scanners (like Play Protect) using minimalistic droppers. These droppers do not contain the payload but retrieve it post-installation via dynamic code loading (DCL), often coupled with app store social engineering to build trust.

In parallel, we will analyze social engineering campaigns (phishing/smishing) aiming to force APK installation outside the store (sideloading), circumventing Google's security perimeter. Finally, we will address the top of the pyramid: vulnerability exploitation. This includes '1-click' scenarios, where minimal interaction triggers an exploit chain targeting an exposed component (e.g., browser renderer), and '0-click' threats, typical of spyware, targeting non-interactive attack surfaces (like multimedia library parsers or messaging protocol stacks) for stealthier injection.

This taxonomy of entry vectors provides an essential strategic view for understanding the current mobile threat landscape.

Additional Information

— Language: French
— TLP Classification: CLEAR
— Recording: yes



The Kill Chain for Android Malware : Delivery

Résumé pour CFP 2025

Intervenant : Thibaud PERRARD

Description concise

Comment un malware arrive-t-il sur un téléphone ? Cette session analyse les vecteurs d'infection Android modernes : infiltration des marketplaces officiels, campagnes de phishing (smishing), et exploitation de vulnérabilités (0day), persistance.

Résumé détaillé

Cette présentation propose une analyse technique des vecteurs de livraison (delivery vectors) qui conditionnent le succès d'une compromission Android. En nous concentrant exclusivement sur la phase "Delivery" de la kill chain, nous allons cartographier les stratégies offensives, de l'ingénierie sociale à grande échelle à l'exploitation pure de vulnérabilités.

Nous examinerons d'abord le défi de l'infiltration des marketplaces officiels, une tactique qui repose sur le contournement des scanners automatisés (comme Play Protect) par l'usage de droppers minimalistes. Ces derniers n'embarquent pas la charge utile, mais la récupèrent post-installation via des mécanismes de chargement dynamique (DCL), souvent couplés à une ingénierie sociale d'app store pour générer la confiance.

En parallèle, nous analyserons les campagnes d'ingénierie sociale (phishing/smishing) dont l'objectif est de forcer l'installation d'APK hors-store (sideloading), contournant ainsi de fait le périmètre de sécurité de Google. Enfin, nous aborderons le sommet de la pyramide : l'exploitation de vulnérabilités. Cela inclut les scénarios '1-click', où une interaction minimale déclenche un exploit chain ciblant un composant exposé (ex : renderer du navigateur), et les menaces '0-click', typiques des spywares, qui visent des surfaces d'attaque non interactives (comme les parsers de bibliothèques multimédia ou les piles de protocoles de messagerie) pour une injection plus discrète. Cette taxonomie des vecteurs

d'entrée offre une vision stratégique essentielle à la compréhension de la menace mobile actuelle.

Autres informations

— Langue : Français
— Classification TLP : CLEAR
— Enregistrement et rediffusion : Oui