ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité
des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

NOTE DE SECURITE

Titre	LANDFALL: Nouveau logiciel espion Android cible les appareils Samsung
Numéro de Référence	58191011/25
Date de Publication	10 Novembre 2025
Risque	Critique
Impact	Critique

Palo Alto Networks a publié un rapport détaillant la découverte d'une nouvelle famille de logiciels espions Android baptisée « LANDFALL ». Cette menace exploite une vulnérabilité critique, référencée « CVE-2025-21042 », affectant la bibliothèque « libimagecodec.quram.so » utilisée par les appareils Samsung Galaxy sous Android 13, 14 et 15. La faille permet une écriture hors limites (out-of-bounds write) lors du traitement d'images au format « DNG » (Digital Negative), ouvrant la voie à l'exécution de code arbitraire et à la compromission complète du terminal. Samsung a corrigé la vulnérabilité « CVE-2025-21042 » dans ses correctifs de sécurité d'avril 2025, mais de nombreux appareils restent exposés faute de mise à jour.

Selon les analyses, la campagne « LANDFALL » est active depuis 2024 et cible principalement des utilisateurs situés au Moyen-Orient. L'infection débute lorsqu'une image « DNG » malformée est ouverte sur un appareil vulnérable. Cette image contient un fichier ZIP malicieux. Une fois exploitée, la vulnérabilité permet le déploiement de deux modules principaux : « b.so et l.so ».

Le premier module, « b.so », collecte des informations sur l'appareil, puis établit une communication chiffrée via HTTPS avec des serveurs de commande et contrôle (C2). Le second module, « l.so », se charge de modifier la configuration de « SELinux » afin d'obtenir des privilèges élevés, de maintenir la persistance et de permettre le chargement de modules additionnels. Ensemble, ces composants permettent au logiciel espion de surveiller et d'exfiltrer des données sensibles, notamment des fichiers, des messages, des enregistrements

audio et des médias provenant d'applications telles que WhatsApp. Des mécanismes anti-analyse et de nettoyage des traces sont également intégrés pour compliquer la détection.

Le maCERT/DGSSI recommande d'appliquer les mesures préventives ci-dessous et de l'alerter en cas de détection d'une activité relative à cette attaque via « incident@macert.gov.ma ».

Mesures préventives :

- Intégrer les indicateurs de compromission (IOCs) ci-dessous au niveau des moyens de détection.
- S'assurer que tous les terminaux Samsung Galaxy disposent de la dernière version logicielle disponible.
- Désactiver ou restreindre le traitement des fichiers DNG non nécessaires dans les environnements professionnels, particulièrement lorsqu'elles proviennent de sources inconnues.
- Surveiller les connexions HTTP/HTTPS afin de détecter les communications suspectes et les comportements anormaux.

Indicateurs de compromission (IOCs):

IP adresses:

- 46.246.28.75
- 194.76.224.127
- 45.155.250.158
- 92.243.65.240
- 192.36.57.56
- 91.132.92.35

Domain Name:

- projectmanagerskills.com
- healthyeatingontherun.com
- hotelsitereview.com
- brightvideodesigns.com

Hash:

- b06dec10e8ad0005ebb9da24204c96cb2e297bd8d418bc1c8983d066c0997756
- 29882a3c426273a7302e852aa77662e168b6d44dcebfca53757e29a9cdf02483

- c0f30c2a2d6f95b57128e78dc0b7180e69315057e62809de1926b75f86516b2e
- 9297888746158e38d320b05b27b0032b2cc29231be8990d87bc46f1e06456f93
- b45817ffb0355badcc89f2d7d48eecf00ebdf2b966ac986514f9d971f6c57d18
- d2fafc7100f33a11089e98b660a85bd479eab761b137cca83b1f6d19629dd3b0
- a62a2400bf93ed84ebadf22b441924f904d3fcda7d1507ba309a4b1801d44495
- 2425f15eb542fca82892fd107ac19d63d4d112ddbfe698650f0c25acf6f8d78a
- ffeeb0356abb56c5084756a5ab0a39002832403bca5290bb6d794d14b642ffe2
- 211311468f3673f005031d5f77d4d716e80cbf3c1f0bb1f148f2200920513261
- 384f073d3d51e0f2e1586b6050af62de886ff448735d963dfc026580096d81bd
- b975b499baa3119ac5c2b3379306d4e50b9610e9bba3e56de7dfd3927a96032d
- 69cf56ac6f3888efa7a1306977f431fd1edb369a5fd4591ce37b72b7e01955ee

Composants:

- b.so
- l.so

Références:

- https://unit42.paloaltonetworks.com/landfall-is-new-commercial-grade-android-spyware/
- https://www.bleepingcomputer.com/news/security/new-landfall-spyware-exploited-samsung-zero-day-via-whatsapp-messages/
- https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=04
- https://security.samsungmobile.com/securityUpdate.smsb