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	Malware Keenadu
Numéro de Référence	61590303/26
Date de Publication	03 Mars 2026
Risque	Critique
Impact	Critique

"Keenadu" est un backdoor Android sophistiqué qui se distingue par sa capacité à s'implanter à différents niveaux de l'écosystème Android, allant d'applications téléchargées sur Google Play jusqu'à une intégration directe dans le micrologiciel (firmware) de certains appareils via la chaîne d'approvisionnement.

"Keenadu" est principalement utilisé à des fins de fraude publicitaire. Les appareils infectés sont exploités comme des bots capables d'ouvrir des pages web invisibles et de générer des clics sur des publicités, permettant aux opérateurs malveillants de percevoir des revenus frauduleux. Toutefois, certaines variantes de "Keenadu" agissent comme une porte dérobée offrant un contrôle total de l'appareil compromis.

Dans les cas les plus graves, notamment lorsqu'il est préinstallé dans le firmware, le malware peut exécuter des commandes à distance, installer des applications supplémentaires, collecter des données sensibles et surveiller l'activité de l'utilisateur. Les informations exposées peuvent inclure les messages, les fichiers multimédias, les identifiants bancaires, la localisation et d'autres données personnelles. Cette implantation au niveau de la chaîne d'approvisionnement rend la détection et la suppression particulièrement complexes.

D'autres variantes ont été découvertes au sein d'applications systèmes préinstallées, bénéficiant de privilèges élevés. Bien que ces versions présentent des limitations par rapport

à la variante firmware, elles conservent la capacité d'installer des applications secondaires à l'insu de l'utilisateur. Dans certains cas, le malware est intégré dans une application liée au déverrouillage facial de l'appareil, ce qui accroît les risques liés à la confidentialité et à la sécurité des données biométriques.

Par ailleurs, plusieurs applications distribuées via Google Play, notamment des applications destinées aux caméras domestiques intelligentes, ont été identifiées comme vecteurs d'infection. Ces applications, téléchargées plus de 300 000 fois, permettaient l'ouverture de navigateurs invisibles au sein même de l'application afin de générer du trafic frauduleux.

Au regard de ces éléments, "Keenadu" doit être considéré comme une menace hybride combinant fraude publicitaire industrielle et capacités avancées de compromission. Son implantation potentielle dans la chaîne d'approvisionnement Android constitue un risque pour les particuliers, les entreprises et les administrations utilisant des appareils mobiles non maîtrisés.

Il est recommandé de :

- privilégier des appareils provenant de fournisseurs reconnus et certifiés ;
- maintenir les systèmes Android à jour ;
- surveiller l'installation d'applications non autorisées ;
- déployer des solutions de Mobile Threat Defense (MTD) ;
- appliquer une politique stricte de gestion des appareils mobiles (MDM) en environnement professionnel ;
- intégrer les indicateurs de compromission (IOCs) ci-dessous au niveau des moyens de détection ;
- alerter le maCERT en cas de détection d'une activité relative à ce malware.

Indicateurs de compromission (IOCs):

Hashs :

- 0c1f61eeebc4176d533b4fc0a36b9d61
- 10d8e8765adb1cbe485cb7d7f4df21e4
- 11eaf02f41b9c93e9b3189aa39059419
- 19df24591b3d76ad3d0a6f548e608a43
- 1bfb3edb394d7c018e06ed31c7eea937
- 1c52e14095f23132719145cf24a2f9dc
- 21846f602bcabccb00de35d994f153c9
- 2419583128d7c75e9f0627614c2aa73f
- 28e6936302f2d290c2fec63ca647f8a6
- 382764921919868d810a5cf0391ea193
- 45bf58973111e00e378ee9b7b43b7d2d
- 56036c2490e63a3e55df4558f7ecf893
- 64947d3a929e1bb860bf748a15dba57c
- 69225f41dcae6ddb78a6aa6a3caa82e1
- 6df8284a4acee337078a6a62a8b65210
- 6f6e14b4449c0518258beb5a40ad7203
- 7882796fdae0043153aa75576e5d0b35
- 7c3e70937da7721dd1243638b467cff1
- 9ddd621daab4c4bc811b7c1990d7e9ea
- a0f775dd99108cb3b76953e25f5cdae4
- b841debc5307afc8a4592ea60d64de14
- 4c4ca7a2a25dbe15a4a39c11cfef2fb2
- 912bc4f756f18049b241934f62bfb06c
- ba60d29da7fd4794b5c5f732916f7d5c
- ca98ae7ab25ce144927a46b7fee6bd21
- d840a70f2610b78493c41b1a344b6893
- f0184f6955479d631ea1b1ea0f38a35d
- c57de69b401eb58c0aad786531c02c28
- 07ec44371bf3ecf490c84a074deb477e6cd5ba4f
- 129dbfef5ffa59f829bb606ee410c75dbb6e77fa
- 17d3db0a69f9fa851d3d1a3e453514b5fe645eeb
- 26927304bdfaa2211523b12db42ffb92a4d6831c
- 2de681d196a0ad0452688127887c2d10df6e02a6
- 74e4aa22a80f721a56922e8e3fb10fbe8b354d81
- 77a1bf82d10503be47c805e3af73d1d6db38ffb4
- 7db58b72a3493a86e847c3685eca74c690d50b55
- 9a6e603b52f95f463241009d06124e1b226fa4c2
- 9e245048a6032a5e74fe83a1b9627e5193a1f93d
- 9fefd87be0b6b9ec4932b49d3eec13bffbc425d6

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- a0c4628f00e78bbce8fc2e7a8cf47920a09ca6e2
- a76d18d7fe9093f65814de13d2f9b76d33039209
- b9975c8f8f4b7ebd3a0b2148ecbb5bb66dc9e369
- c93390cb4aada8610336b9a874016e7dd8a258f0
- d0875d13452358892e3a145524a6b4adfe41fe26
- d1ed605893e8be2daa2fc0dba2f247ae4223d54e
- e272f4f6f514f3f9e0e17eca713f3d6667d9d354
- e395114ada50d2ca9ac731a24173b06f906ca6df
- e431819435fd9ba16199388fc1b6309bc8be207c
- efe62d3fe25ccf445b74516de12354f04987a5ad
- 10c69555d2f2cfa6771e44c10fd7761205b6faab
- 5467ce4030d9b9aca7944d8df5e23146fd251df9
- 0010001fae2a41185565d6ea7ff34ee13fd4c77d0fbd48c3e0c1213f0065f26f
- 0ea744f4ac3b970c1135fb63f1bd3b8a0fc47227b344b5cd6692e5fb6237f8c6
- 163c42b00f2db2930f8da2e75095c8578477cea623f3b3825e110ff49e517cbe
- 2a604f85b748e4e687627fb4919053d577095c59cd323c52c0bdf801090b48ad
- 305b87b4df93d31722d603ad5751e66e03c40613c2b44941e40d4dd29a4a5d44
- 312d9596139cf64915adc8c3892e92be2ec5bd6ae1935fc5967d87cbe0797f96
- 496bd073ae894a4b1fc1a7caf48a93702d3d96d064cec484c338878b50a3a4c6
- 4def1b1fcec0700bf45659287a0153b5294a520fcedfec3fad02fdb72ac61b37
- 52db1f284a0dccbb750314cf765131a17a8284a2aeea04701a2b71f35fb9d9ee
- 571349bece467e4a5b06b13c1f41df56067b3a103086d8faca57feb0aeb2ae21
- 62ff9ebd3f0bbac404336c4756324cd5331ea6cc4d38760878f34e23e122f41e
- 862775e9d9b522f4534717127a53bfb4e81ee3c974dd23807438ee77fcfccc52
- 877f627a55df4a4dccf34d5359f713e5c55d413eb2342cdf51dfb0bb5c40b214
- 9e302d473fe20d9adcef23657fc18fcf701e8439af537ac12aacce3378b5d78d
- a18375596659d465efe7594eedc63ddd371da51f14473f5b6d3ce88e3a60253a
- a294ccb85d7cd8adf14e6869ca36d6addfd2caa914ade3884b7d9760e4bc0499
- a5d594c8de979074f2d22b37bb01b04fd738295a9388862141252201e028813e
- f74647f29cab8e55c94816f622068015cc387d93342bde1104cee3db368c3d20
- f7d62a7a744346f55b96a31da9f5788da26e7ab4c8fecf897fb38c2ca3652882
- fa1c4ca0a93748754db776d6777c1a30691f28e53489a6abd2f9b4cae53600ff
- feaf9714b00bf3d882d96ccee4d312923f29e668db7aeef0a4189aba47b0f20b
- f3cc6d7f5b5f7da62334b3eb7fabd0b0a5dcde0bfebc58c47f7f7e91dc266b20
- f3ef68b406840fe9ba028ebbf5e4f502f6c3615fd7b20a8bdbc8a343351aa229
- 26971fdd34cda3ea13f5473b4ed49c6b9600b7e8e9222e9f6f778ec3f0725c09
- 3c2091a18d0ecbcc69517138173262420ab01bb25de74c99672fa1349b8e7c87
- 6d806746e42c268bcbf616115b5a44be46584c9bae38e1d97e1ed6419c010767
- 862775e9d9b522f4534717127a53bfb4e81ee3c974dd23807438ee77fcfccc52

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- f325201bc8a9ed91b7eb577ae5964876fa3884ca38ed5a3516ee3cb64f29c4a5

IP :

- 110.34.191.81
- 110.34.191.82
- 67.198.232.187
- 67.198.232.4

Domaines:

- dllpgd.click
- proczone.com
- fbgraph.com
- sliidee.com
- glogstatic.com
- uscelluliar.com
- gmsstatic.com
- ytimg2.com
- goaimb.com
- gsonx.com
- gstatic2.com
- keepgo123.com
- zcnewy.com
- aifacecloud.com
- gvvt1.com
- keepgo123.com
- fbsimg.com
- newsroomlabss.com
- playstations.click

Référence :

- https://securelist.com/keenadu-android-backdoor/118913/