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 " ToxicPanda "
Numéro de Référence	59612512/25
Date de Publication	25 Décembre 2025
Risque	Critique
Impact	Critique

"ToxicPanda" est un malware bancaire conçus pour les appareils Android, spécialisé dans la compromission d'appareils mobiles à travers des techniques d'on-device fraud (ODF) et de prise de contrôle de compte (Account Takeover, ATO). L'infection par ce malware se produit principalement via le téléchargement d'applications malveillantes en dehors du Google Play Store (sideloading). Les victimes sont souvent trompées par de fausses mises à jour de navigateurs ou d'applications populaires.

"ToxicPanda" abuse des services d'accessibilité d'Android afin d'obtenir un contrôle étendu sur les appareils infectés. Une fois déployé, le malware peut exécuter plusieurs commandes à distance, lui permettant notamment de simuler des actions utilisateurs telles que les clics, le défilement ou la saisie de texte. Il est également capable de déployer des superpositions frauduleuses imitant des applications bancaires légitimes, d'intercepter les frappes clavier et de collecter des identifiants sensibles. Ces capacités permettent une automatisation complète des interactions avec les applications financières directement depuis l'appareil compromis.

Les risques associés à cette menace sont élevés et incluent la compromission de comptes bancaires, des pertes financière et atteinte à la confiance des clients via l'exécution des transactions frauduleuses entièrement automatisées et le contournement des mécanismes de sécurité, y compris l'authentification à deux facteurs (2FA).

"ToxicPanda" intègre des mécanismes avancés destinés à renforcer sa résilience et son efficacité. L'utilisation d'un Domain Generation Algorithm (DGA) permet de rendre les infrastructures de commande et contrôle (C2) plus résistantes aux tentatives de démantèlement.

Le maCERT recommande d'intégrer les indicateurs de compromission (IOCs) ci-dessous au niveau des moyens de détection et d'alerter le maCERT en cas de détection d'une activité relative à ce malware.

Actions recommandées :

- Interdire l'installation d'applications via sideloading ;
  - Désactiver l'option « Installer des applications depuis des sources inconnues ».
- Installer les applications Android exclusivement depuis le Google Play Store ;
- Activer et maintenir Google Play Protect ;
- Mettre à jour régulièrement :
  - le système Android
  - les applications installées
- Sensibiliser les utilisateurs aux fausses mises à jour (Chrome, navigateur, sécurité, banque) ;
- Éviter de cliquer sur des liens reçus par SMS, messageries ou emails non sollicités ;
- Surveiller les communications suspectes vers des domaines générés dynamiquement (DGA) ;

Indicateurs de compromission (IOCs):

Domains :

dksu.top	bingx.sbs
mixcom.one	d.dblpap3.top

fgta.lol	vfam.top
dpds.lol	jpnapp.com
freebasic.cn	smet.top
cgtp.lol	ayte.top
atnp.lol	smuw.top
dblpap1.top	dubelog.lol
dblpap2.top	daraz.digital
dbltest.top	tbva.top
dblxz.lol	download.tw1988.link
bnwu.lol	msda.top
dbltest6.top	ctrl.dksu.top
cpt.lol	bauw.top
dbltest8.top	patm.top
unk.lol	aykn.top
99spedmart.me	down.tw1988.link
mwscg.top	qhte.top
kmpct.top	sakd.top
ckysp.top	kaqp.top
aerodromeabase.com	mvfa.top
bentonwhite.com	sajw.top
bplnetempresas.com	ctrl.sakiwmk.top
chalnlizt.org	ewjh.top
check-googlle.com	saywe.top
cihainlst.org	kadb.top
comteste.com	fbr.digital
cuenta-ntflx.com	ctrl.bbf02eec73.top
qwneoa66666.top	itvpndownload.top
d7472ad157.lol	kaet.top
38.54.119.95	kmba.top
ctrl.mixicom.one	

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

Hashs :

- a4e272db5b6a0ca7707d280e33b4619aa5b779cc9ec590c9c94f34a808b0cf0c
- b1bdc1efad145e516e759655b8ae19d4fbed245f5b1d0b2d76f280424332c64f
- efeea4534e32a8549bab06823b2941d3b36cae77f21a181b94fbe1a62dc4329f
- d201a9d4f7ad2f413dc8574ad7a61ef0e825ebc4e2a668b7509fd7c22cf2099e
- 2e3b153ce4fc78c2c79579941cac114a2274f6d1d4da28d37a27b3eb0769fa75
- 2220fbac9036343ce344f260169c9063ec018c9e5143cf384a1dcaac5ac61e67
- 857d676411d4fa847d62631ad94e7e0a
- c68f166f53afa7232ea6e404ea4e80e6733bb096e9f09d94a250ca6bf4e2bcad
- 87b80f81c7adf545875a80b46b2ffe16a3c025daa1b803863ba2915e880983e2
- 314cbc4b68cf28fc01a30c31901e74dc9046117907961c91d74e7dd9223ba776
- c81634316d0bb19bffa029a70296fbe778f5fc698aefa124b991b3257f3c7a21
- 221ba7298e94d22d33d446ef5add2cb3cf4c18886ee1b6a188ac365e88228538
- 56bc71fd19f6d0738fc1c9c7869bcd7533d6114f6c6d7140e58365521eb6d85c
- 14df744881e33d344b20851098c61d2371afe18b31747b307a46ff51fa78c17a
- 82c12f29aa41bbb9813fb9a24a891c2454c58c97d7cc2e0d7922f12ad011cf4a
- 69310dff6e0c934e845ce129e5919266f90a398afa1a46b6321e0e20517c984a
- 115e8f80f83ee75d85bafd04c8cbda06de3acaa461389c755d777004468606c2
- cca9353b4c322d0ba6bd633a86946c832718f7000e2037803f45d7a269acdb5f
- 9449ea5319473f4eac4896a3d9e095ac9780e9994158824af13cfd1f1bade475
- 11d926b4e7068914d27200e1aebcbc5e255088ae588a50a1f8f0520771bb6b15
- 16cfe2e74cca2dfdc42f50643f7b32a1f661d5f6ecb8bef8a33125a7f3124070
- fd1a5f6a8b5474a950510d687188b76f6a76fb25423c0e5bc80beeef296f4d39
- b51a18d93969632972dccab0c24534992649154b43fc91d6c8bf163407722e58
- bee3ecaeaa7925c229b58053533581f760e409d0d9f583c30964612423064911
- 181353a8725695703d7f84006f63c1f8443b731a3be09c6b24269897b2f7566b
- 1ad6dadfcf052a5a0997b323734c23b2f2676fcb0c5e0ca7cca964cb5ea95f85
- c0050dcf8783a9573cc23fc5381e28c80cc316362a71ab13ec757dcee4e34648
- 520d7902587dfc26a058e1ef5a7e6b9946bb668d03a41ee153ea54492e77f660
- 159a7af39c0d6c2334df77088fe2d545a96d591dbf2b85c373a4a45377f492c4
- 158bfa63e745e4d5b05f2c63fca5a002c3080843d0b814b6497b150e4bb5f43e

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