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	AVrecon malware
Numéro de Référence	62432603/26
Date de Publication	26 Mars 2026
Risque	Critique
Impact	Critique

« AVrecon » est un malware ciblant principalement les routeurs et les équipements de type Internet of Things (IoT). Il est utilisé par des acteurs malveillants pour compromettre des équipements connectés à Internet et les intégrer dans des réseaux de « proxies résidentiels », permettant de dissimuler l'origine de leurs activités malveillantes.

Ce malware est généralement déployé après l'exploitation des vulnérabilités connues, notamment des failles de type exécution de code à distance (RCE) ou injection de commandes, sur des équipements insuffisamment mis à jour ou en fin de vie. Une fois installé, AVrecon permet aux attaquants de maintenir un accès distant au dispositif compromis et d'utiliser celui-ci comme relais pour leurs opérations.

Les équipements infectés sont ensuite exploités comme proxies résidentiels, ce qui permet aux cybercriminels de mener diverses activités illicites. Le malware peut également agir comme loader, en téléchargeant et exécutant des charges malveillantes supplémentaires sur les équipements compromis.

Lors de l'infection, AVrecon met en place des mécanismes de persistance variables selon le type d'équipement. Dans certains cas, le firmware de l'appareil est modifié afin d'assurer l'exécution du malware à chaque redémarrage, rendant la compromission difficile à détecter et à supprimer. Le malware communique ensuite régulièrement avec son infras-

tructure de commande et contrôle (C2), notamment via des échanges périodiques de type « PING/PONG » afin de recevoir de nouvelles instructions.

Systèmes affectés:

Les appareils suivants ont été identifiés comme étant les plus représentés parmi les dispositifs infectés par AVrecon :

- D-Link
  - DIR-818LW Wireless Router
  - DIR-850L Wireless Router
  - DIR-860L Wireless Router
- Hikvision
  - DS-2CD2020F-I IP Camera
  - DS-2CD2420F-IW IP Camera
- Netgear
  - DGN2200v4 Wireless Router
  - AC1900 R7000
- TP-Link
  - Archer C20 Wireless Router
  - TL-WR840N Wireless Router
  - TL-WR849N Wireless Router
  - WR841N Wireless Router
- Zyxel
  - EMG6726-B10A Router
  - PMG5617GA Home Gateway Unit (HGU)
  - VMG1312-B10D Wireless Router
  - VMG1312-T20B Wireless Router
  - VMG3925-B10A Wireless Router
  - VMG3925-B10C Wireless Router
  - VMG4825-B10A Wireless Router
  - VMG4927-B50A Wireless Router
  - VMG8825-T50K Wireless Route

Recommandations

Le maCERT recommande :

- d'intégrer les indicateurs de compromission (IOCs) ci-dessous au niveau des moyens de détection ;
- d'appliquer sans délai les mises à jour de sécurité sur tous les équipements réseau exposés à Internet ;
- de remplacer les équipements en fin de vie;
- de désactiver l'administration distante lorsque celle-ci n'est pas nécessaire ;
- de surveiller les communications sortantes des routeurs et équipements IoT vers des infrastructures inconnues ;
- de segmenter les équipements IoT du reste du réseau interne afin de limiter les mouvements latéraux en cas de compromission.

Indicateurs de compromission (IOCs):

Hashs :

- 6501a2d2ed60b85b1080ac9edaf39b70
- efb8b73d59a805e1fd9ebf0d3540b0e8
- 06d491b70f369b2672fce5a7b59a5c93
- bf0183b2d18341c47576ba8e0d36fdff
- 126b1c224e8635d9571f9d769d7b55e2
- 22c5849855878f331d7bbf07e7ec7e41
- 1c8c17ef978bd4f03db672c0b2d51d00
- f74c8bd1701746cce8b4bad819cdd148
- 1f970f5eb9cbef8dba11e2aed72373ba
- f774fcbf889a8a629004f31e8b962b63
- 2a646682ee7f0f853605c78bb9126ed5
- ffaa0890eb9a38307477157c02f63583
- 327c1ca93321705027e0bf47658b5f53
- f81b9fceea2056ba2c3f261b56f577b1
- 32f1f238da09f1ebc1385317d50e94b4
- 8dcaf0e2a0baf54e65f46689b2a845ef
- 3bfc273e5592825443ded9c28f50cd5d

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

- 3ed1a6d57f00c1643cc85e049c82d1b4
- 6501a2d2ed60b85b1080ac9edaf39b70
- d5d63db439bb1dba080ab27555b03a2a
- 667ae41f4a6201071b8cc3f88e3e02c7
- de86b12800919ce8b213b51354d28ab8
- 6a389a89a6da7433210d9a52fc72589c
- ef7f3f7cb4f3f1a90a2028d44c4fe702
- 6a6619b4b9a53233ca0a56606c484f9a
- f0d1852065c498c3bdaec3de8e6cd626
- 6ec7063f03f95499b6c1821f90bda7e6
- f143b44d3b8d835c09bf2c346d90ec22
- 70c2317f40de5b28f42d640488910140
- f3cf4a369e5fb451db250c31776ba84e
- 74e5514cdd3ef6f703483700f04b5812
- c32ac3f6cba0772de7737da60f9170c0
- 7d4c60c77a7d74cc3d9af4dabbecdbb8
- c53397dc47ddc38a8c6daa3a02116518
- 8a978017496adb02eb368f3b28bc4ccd
- bb5e9faa666e6d96eb95e358524213b6
- 8ad3f40fd8fcf2c7ee04d1219017cfe3
- bd24f43084b33f13a835f661bf48b5e2
- 8fc84a03b66ceccd394c6a754bb513a6
- bd4a12d4de4e42c4d9246aa92ddb86b8
- 920534d235204ced7ad2c76c1af7b3f8
- 9dfba3b92850a74135925e524e7b4748
- 963354b60552af16408cf4d82a827832
- b1a32a442cdb34901f1f7ffbe47749f0
- 9752ac893640a027bea5a6df48ceb396
- b5ad7f7e10f5d0401a2ad6b737724ff6

IP:

- 188.138.125.163
- 176.120.22.67
- 185.163.204.198
- 62.138.0.10
- 85.25.100.30
- 62.138.14.209
- 91.245.255.112

- 62.138.0.211
- 175.110.114.65
- 188.116.22.153
- 213.202.230.95
- 38.180.91.47
- 176.120.22.67
- 77.246.106.198
- 45.137.213.88
- 91.215.85.178
- 37.77.150.19
- 185.162.128.133
- 37.77.150.77
- 5.149.254.109
- 5.149.250.54
- 79.141.160.92
- 5.149.250.171
- 212.118.38.30

C2 Domains:

- advstat.cc
- meterstrack.cc
- startsun.cc
- backdump.cc
- netjunk.cc
- zeroback2.cc
- critlan.cc
- plxz.cc
- zeroback3.cc
- zeroback4.cc
- atable.cc
- cleandone.cc
- evrc.space
- lups.cc
- dzero.cc
- r0ck.online
- regul.cc
- fpride.cc
- vdem.cc

- utcp.cc
- zerophone.cc
- zeroback.cc
- zorc.cc

C2 URI Path:

- lumi/config.php
- lumi/test.php
- lumi/ping.php
- lumi/track.php
- lumi/pride.php

Référence :

- https://www.ic3.gov/CSA/2026/260312.pdf