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	XWorm RAT « Update »
Numéro de Référence	63830505/26
Date de Publication	05 Mai 2026
Risque	Critique
Impact	Critique

XWorm est un cheval de Troie d'accès à distance (RAT) basé sur .NET, apparu en 2022, et qui continue d'évoluer avec des mécanismes de diffusion de plus en plus sophistiqués, ciblant principalement les systèmes Windows.

Selon des rapports récents d'avril 2026, plusieurs campagnes utilisent XWorm, notamment via :

- des packages npm malveillants,
- des emails de phishing contenant des fichiers Excel exploitant la vulnérabilité CVE-2018-0802,
- de faux jeux vidéo.

Le malware utilise des techniques avancées comme le process hollowing, permettant d'injecter son code dans des processus légitimes tels que « MSBuild ou Windows Explorer ». Il établit ensuite une communication chiffrée avec ses serveurs de commande et contrôle (C2) à l'aide du chiffrement AES.

Parmi les charges utiles fréquemment associées à XWorm, on retrouve notamment « Agent Tesla et Remcos RAT », ainsi que divers infos stealers. Ces malwares sont souvent déployés en complément pour maximiser l'impact de l'infection, en permettant l'exfiltration

de données sensibles telles que les identifiants, les informations bancaires ou encore les données de navigation.

XWorm repose sur une architecture modulaire particulièrement flexible, comprenant des dizaines de plugins capables d'étendre ses fonctionnalités. Cette modularité permet aux attaquants d'adapter le malware à leurs besoins spécifiques, notamment pour le vol de données, le contrôle à distance du système infecté, la surveillance des activités de l'utilisateur, ou encore l'exécution de commandes à distance. Cette approche rend XWorm à la fois polyvalent et difficile à détecter.

La période observée, allant du début mars à la fin avril 2026, met en évidence une recrudescence significative des activités liées à XWorm. Cette augmentation s'inscrit dans un contexte global marqué par des vulnérabilités persistantes dans les chaînes d'approvisionnement (supply chain), une montée en sophistication des campagnes de phishing, ainsi que des attaques de plus en plus ciblées.

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

Indicateurs de compromission (IOCs):

Hashs :

- 00ba60e32d969137df6b8efdd6551c29106486a7fea4ac36c15bf0b074f26302
- 00d4b7b6084a52e78fb67710f1710e2fa726a498edfc047ef2c6df000d3df5c8
- 09c36f481b5ffb903341266318af76e6951db3ceeb97fe0a004935092cb40e74
- 0fed4b6ae92342bee5ba201ea73ec665fdcbd84f4849865b434de41da24e367b
- 1577ff149db29ed8e6c7442e9d13c8cf4718b33ac6b16bbdf39e996fb22e538f
- 1d5638dc3d98a3e696edbb7c05709e611f51642124036990ca85dc45f8c6a0dc
- 253c28a87dd3dd911b80ef004c2fdcb05349e6d60bee68a86d06e671347c0b4c
- 253f27aad4b5e1f578499b2bc31d66466c91f85b9b3952b5e3906a72f7f2b550

- 2959afc3285daed5dfaa89bdebfcccaca367704af871b2a4e72fe7d27775084a
- 2eea097e689004e05f44f04ff22909c96d43d04fa7e5936f3709cf0d3a36c041
- 30052dbf5ccd3304c0fbeb9923d13fa7528f31e3cda210bb4fa111d024a5d532
- 3bae6eda4a5e540ab478b3d67a1a2b53e42eb2d5509504e027297e8ee4c0c759
- 463def540f254240a2ab4aaf11d5aa17eff2d57a16909a6cdd48fba75173f7ac
- 4d78efe6f619a81756db3aee2a83c7f1ac0c47628bd5ad100a71c82d445128e7
- 4dbf448c0f69df077a8e70531d00c7814e548f3cba38c50f3956d3e416596f45
- 4f978573add374e9e8f0846c274e4e6b745a8904710f470ff7986d9969e257e3
- 50299a2f4c1935435c715ea13343063c116248c46cb143c1c04f4f84d241012b
- 57dd8227d650fe16d7403ff87eb2fa917bf96917fdd454bc9ddcf80ba5619503
- 5feef4a3a61e7cb38abb3a59c3ed0d0e91e13958e72509c141e52a93fbcb639f
- 64f534e6af5dda57640011e684fbc4fccbead9ffee36c75a806681cb951e0166
- 6b8caec54162721f79f1b422ec44b75ef4e6649fa231a82c69e50b010420afff
- 6fa8d275fe8088eed53db568ffb9cf8c9c11d4e54a37d8986965d8053285bda6
- 6ffd1b8b7c4912b4fb0bdb1437371a1e761854092fb0c3e4934d32e9a30d9f38
- 72224fde333c4509fca14a48a1f31d71e6b00a85cc52423874bd27b278e79fb0
- 7ab98986f610a7341383733008c19dd4fabedb005a419574b31d31fed58f51ef
- 7bc432cbca6d578d75220f4d09a8c7ad1761e1d073d4b71927ca3dcc5682884b
- 816bb174626bcd225b71669970798a3afe4809ef76fd48752d64ca8862089c08
- 8a87aae368cd9817f313ece0e4bb52568017c01e245b7883b03db4bb03d80a1a
- 8edd7f6c70d33daa4a266af0b798ebea983302785bdd9030d2889bfa7b52cce1
- 919f4bc1a9f83cf679fe266beab946048de16084e0380429215013514aa17fc4
- 9843fbd378b1473199ad468ea9da5a606c271f09c2b2873206d32b69cb0988d0
- a1f47a553cf323808b04fadd3d1f009ff69bea3d81cdb051cd898ca937fe917f
- a3b32d655ec2781a743ef411da8ee030536c1a6113c80f2cfd1b51fd122e7241
- a5555c33bd6190465a0345cd80af96e2908c9a423fdf675c48e0a02d2bc5c90a
- a594f7f6b879cb11a418d8fdf2e33cba8987334edebf5964315347747eb3047b
- a69c53d749f3afd5249086d71ba9379b7284f1ec401343e7179ac5d5f40f4bad
- a6b5962e78e2eb7f62189265517e9f2eafd88694f212bd2114b4e59ab988448a
- ac725147767b4b4f50a65822c2b33bcd0a057a7a80113d567589e7e4f7caaba5
- b541745f453080d401484b9fba03bfa131cc5ce59d3631bd224e984168fafe3e

- b54f23074263b8a830d8b5867c4e30251d46e2967e6c10444d50c78744079db1
- b87c3e30fc09dde931196e43842b085b88f87953557eaf1b013bb1383b4d2475
- bad050d5390c95cfadd7177e8ccdd2bd2854c5279ed29eb9434267a6b910bbfa
- bcb06a36767e2debd376e810f2fa6068a2b0987fdd61998cdf73979987cc6c87
- cdbf6ed6994f287043d824780a51dfed3d7758214c2d3e5e2451948325dba0d8
- cf738c93501bb2ab3fd7d74a4bc291d3f037c13f32b0289d354bdf63e6398bfa
- cfbb294e146674f8c3d102f9bfef584d4239c103b170e1ff8bfe591a99fe2619
- d93fd38387669a6c3c80d06fdd62e890b9d40704541bf8fb83ae25aa54d0e690
- e0334171696aaeeb7dc50dacb80563f8d94ec463333d7fcf652db85103bd3be1
- e2eb4290336f01017569978111d61a6d874b6a0d330324dfd5dab55d7f9202e4
- e976409f3251e2be798ba4303d060771e0116e4b161e445b913de19c50835048
- edf4fad25760dee8930384909630dafa41de4d9bf872b3067323d19eaabf92cf
- f255f77d3530bbebee700dd07352d99162c11b936291e012724b4281826032ba
- f7e90b553bff2af4fa6fe63aaf4d2511fc5fe2514e402487b459c244b75416c0

Ip :

- 103.17.38.43
- 103.82.36.216
- 107.175.246.23
- 112.213.110.204
- 134.122.152.135
- 147.185.221.29
- 157.245.45.38
- 158.94.211.33
- 172.111.136.159
- 172.94.15.100
- 176.160.157.96
- 178.16.53.62
- 185.216.71.155
- 192.109.200.221
- 193.161.193.99
- 198.23.177.219

- 203.202.232.132
- 203.202.232.149
- 45.141.148.126
- 46.151.182.18
- 91.92.120.68

Domains et URL:

- kurkupa-rbx.ru
- 7326.info
- aferistin-41691.portmap.host
- tcp.cloudpub.ru
- promole5.ddnsfree.com
- 27.tcp.cpolar.top
- dsdsjksd-33267.portmap.host
- afafaf-61412.portmap.host
- ddaawww-57253.portmap.host
- arcania.fun
- okw36xvarg.localto.net
- portbuddy.dev
- 1.tcp.cpolar.cn
- 5.tcp.eu.ngrok.io
- afafaf-56808.portmap.host
- alm72rb-37531.portmap.host
- izjkc-144-124-196-92.run.pinggy-free.link
- k9f3sg-61848.portmap.host
- nj9gtedr4j.localto.net
- hebasix.duckdns.org
- 18.tcp.vip.cpolar.cn
- metrostroy-59371.portmap.host
- fsocietymrrobot-33709.portmap.host
- https://browsertools.shop

- https://gamedb.shop
- https://opencamping.shop
- https://unknowntool.shop

Référence :

Bulletins de sécurité maCERT/DGSSI du 30 septembre 2024:

- https://www.dgssi.gov.ma/fr/bulletins/xworm-rat/