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
Numéro de Référence	49793009/24
Date de Publication	30 Septembre 2024
Risque	Critique
Impact	Critique

XWorm est une famille de logiciels malveillants multifonctionnels, couramment utilisée comme cheval de Troie d'accès à distance. Il exécute généralement des attaques en plusieurs étapes, en utilisant souvent des tactiques d'hameçonnage impliquant des fichiers LNK malveillants et des scripts PowerShell pour se déployer via des outils légitimes. Il permet aux cybercriminels d'obtenir un accès non autorisé à des appareils, de voler des informations sensibles telles que des identifiants et des mots de passe, voire d'installer des ransomwares et de lancer des attaques DDoS. Cette conception modulaire fait de XWorm un logiciel malveillant sophistiqué et hautement personnalisable.

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.

Indicateurs de compromission (IOCs):

Hashs :

- 04ce543c01a4bace549f6be2d77eb62567c7b65edbbaebc0d00d760425dcd578
- 06e3abeed1bc98ed56d5587e9732c9d39ea41879c250dff68ce8815953fcf7ad
- 09505b5cf1541b783f14b1bf1403b918fae70f049d72f47439bd068a43ed8e0a
- 09505b5cf1541b783f14b1bf1403b918fae70f049d72f47439bd068a43ed8e0a

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

- 096e33b9b0b4f843a7ea0259f75b4370f00ab90f3807eb89d5f0117da762900d
- 0d16de10ce708b990d1b0ae26ac12792c91864426c88a8c73a475f7f33db014b
- 15f54e2562a9c6f51367327e9f19c11282f21a2de6687f73f0483e6fe3164973
- 17dc38bd4e01496a91d82e6de763df6fd94c00eb1e90e0cccd7f07f84b549f43
- 2951e41d8573c6631e3385eb5242c3fe9e1713fbeaf9c268f7f30c59cb54515f
- 2f5304b657b07839525d7d3ef50f192cde2bcab15b8fde2a6ff264f6412290df
- 38dea3732044129bd99314de582ba3d58a649c8967fe12b98cd867ca6e349ffe
- 40041c3240eaa39da781a68f6a60f93577f1b0bbdaee5a0297d7fe329c073baa
- 40041c3240eaa39da781a68f6a60f93577f1b0bbdaee5a0297d7fe329c073baa
- 41356db4670449f02766c8a51bba8dd70f4f1a6819c8a686a56d6a891b591585
- 444986ba74685fde34afbbf6a6963c5f35f12a1a65a705e5184c545a18c080c6
- 47e238a43f9cc38f2d4e449c7d8a557b990e60773ad02820717a634c22b609be
- 47e238a43f9cc38f2d4e449c7d8a557b990e60773ad02820717a634c22b609be
- 5a47b18066d8dcd0fbc524f529002cf0a270d8394de928e8426fa06959a82704
- 5a47b18066d8dcd0fbc524f529002cf0a270d8394de928e8426fa06959a82704
- 64519b4e63dbedc44149564f3d472c720fa3c6a87c9ad4f07d88d7fd1914f5b9
- 6f981f255cebe8a27629426577b8896d9f9208f7e24771ae861f62efd2616458
- 7860a6e7264839c59506d5d69e40311e0c1e6af11b2351ccffe8d9b09acde9a3
- 7ddb331b1930f9cd3fd7e6de43119db0bbcb20bf6d23b1fbb60db12b0d983c2f
- 814187405811f7d0e9593ae1ddf0a43ccbd9e8a37bee7688178487eeef3860c6
- 8a399e51bdcd4b8d0a041236e80b3094987a80674bda839351fef1585c8c921b
- 8cfefc291d9088ef0b3ab7dd59d8ff672e73d333c8d18bd1dff4c7695ae8af83
- 8f9fff88c0c636c80ca0a4cfa37d3fb620289579a1ecae9ba1d3881235b482ee
- 904343ba2502d390b36403181e77192a62f31e98c87eb91906fbae27019b4c0d
- 98ab2fc44063d4e00f221e502419d9cca598fafb9e1e00352149327267604bc1
- 98ab2fc44063d4e00f221e502419d9cca598fafb9e1e00352149327267604bc1
- 98fcabe279d4001b29949d980aa9ae8396b352ef7c4a90b9dbe07650a7d4b797
- 9a5c05cce53b21e5f745c2b494a6fbc818dbd1ca5bca366eddf73fd037a86c7b
- 9ce4e79962ec3e5a307282afcb72b4da39c4a2aace29f3f85c060d8c07cf3905
- 9ce4e79962ec3e5a307282afcb72b4da39c4a2aace29f3f85c060d8c07cf3905
- ac1984f835b8bc2cf366ef77e5b6e759baf1a41920897896928dfc9d5d843c13

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

- b09bf46468d9ed8b1957246f4cf7fd15679212fe9e5df7df6101179e0594cae6
- b26144c6e42601f1f1be09ece7c7fcb127637db3b953065648d1b1f371da7e8a
- b26144c6e42601f1f1be09ece7c7fcb127637db3b953065648d1b1f371da7e8a
- b54a4f92b1081f0c10a41c2404d51ed340181c485751efb974113a5cf401ad9c
- b9a9ae029ca542aadea0b384e4cfb50611d1a92c4570db5ddc5e362c4ebe41b4
- bf5a2450f5287f775c2427590c29c27e28e3662c2f68296c64cdacdb639f3b97
- c4e613ee1365d8561be02525896c095c8a3fda3199f2f615ab32a644f3d90451
- c4e613ee1365d8561be02525896c095c8a3fda3199f2f615ab32a644f3d90451
- ca0efb6da9edbe627ab206a7f494adb42f8483da1d574ddb8f723c1ddfeaecc4
- ca0efb6da9edbe627ab206a7f494adb42f8483da1d574ddb8f723c1ddfeaecc4
- caf141712e9ceaf7a0c6c0e93410edd1acb942a5c8999162265882cd1c1d6020
- d7e684fe7f3729edd70e2855528af3e634789155d687ed98911d1d2f0200d2a6
- d815e32b7998d3927792e579d4ad8430792ca1043b3570f0ee73855529516d21
- d938cb8accbc51046158350155f1af9248fc8459ef2b92be752b93dae77504a6
- dd8377e9c3620d0732bededcd0d219f77f7bcffbc49470a9b7ff22db33fe4a185
- dea780f228acbd536b5cbb35efe1a41d18771f6ed987c9d19b175de44f1d566c
- dea780f228acbd536b5cbb35efe1a41d18771f6ed987c9d19b175de44f1d566c
- e314b233b41a5688a4e43f876ccb10718351d3f396b4df623b4ebb0a093be7e0
- f44e495e1301866188a62916859075ed73d13193823c69884312f04785707279

Ip :

- 185.216.68.142
- 81.19.139.19
- 81.19.139.62
- 85.209.134.253
- 88.151.192.128
- 95.214.27.17

Domains :

- churchxx.ddns.net
- eu-central-7075.packetriot.net
- freshinxworm.ddns.net

- liouas.ddns.net
- plunder.dedyn.io
- plunder.jumpingcrab.com

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