



NOTE DE SECURITE

Titre	Andromeda Malware
Numéro de Référence	58611911/25
Date de Publication	19 Novembre 2025
Risque	Critique
Impact	Critique

« Andromeda » est un malware modulaire qui a la capacité de vérifier s'il est exécuté ou débogué dans un environnement virtuel à l'aide de technique anti-machine virtuelle. Il télécharge d'autres logiciels malveillants à partir de ses serveurs de contrôle, souvent dans le but de voler des informations sur les systèmes infectés.

Ce malware est distribué via des campagnes de phishing, des pièces jointes de courriers indésirables, des logiciels illégaux et divers kits d'exploitation. Des recherches ont révélé que ce malware présente de nombreuses similitudes avec le code source de « zbot/zeus, Gamarue, Wauchos ».

Le maCERT/DGSSI 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):

Domain:

- xjpakmdcfuqe.biz
- pacifista.ru

- xjpakmdcfuqe.nl
- xjpakmdcfuqe.in
- xjpakmdcfuqe.com
- xjpakmdcfuqe.ru
- restless.su
- devicesta.ru
- imageshells.com
- restless.su
- amnsreiuojy.ru
- trishnaseeds.com
- morphed.ru
- sonic4me.com
- wertdghbyrukl.ch
- rgtryhbgddtyh.biz
- gfaghrtehxxvdfsquaj.zapto.org
- sonic4me.com
- morphed.ru
- trishnaseeds.com

Ip :

- 218.54.47.74
- 112.175.88.207
- 112.175.88.209
- 112.213.106.187
- 188.165.132.183
- 218.54.47.76
- 188.190.114.20
- 218.54.47.77
- 103.246.115.238
- 112.175.88.208

Signature malware:

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: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma

- Win32/Botnet.Andromeda.HwcBEpsA
- Win32/Botnet.Andromeda.HxMBTvsA
- Win32/Botnet.Andromeda.HxMBUWMA
- Win32/Botnet.Andromeda.HxMBXkA
- Win32/Botnet.Andromeda.HxMBZrkA
- Win32/Botnet.Andromeda.HxQBEpsA
- Win32/Botnet.Andromeda.HwMAEpsA
- Win32/Botnet.Andromeda.HwMB6q4A
- Win32/Botnet.Andromeda.HwMBWAUB
- Win32/Botnet.Andromeda.HwMBXwA
- Win32/Trojan.Andromeda.bfzadz
- Trojan.Win32.Andromeda.dhzcid
- Trojan.Win32.Andromeda.fahhol
- Trojan.Win32.Andromeda.dhijuk
- Trojan.Win32.Andromeda.crqzdv
- Trojan.Win32.Andromeda.crhyex
- Trojan.Win32.Andromeda.bxpfjk
- Trojan.Win32.Andromeda.dhtwxi
- Trojan.Win32.Andromeda.cjopuv
- Trojan.Win32.Andromeda.cuulms
- Trojan.Win32.Andromeda.dggbzf
- Trojan.Win32.Andromeda.dhymqz
- Trojan.Win32.Andromeda.dgwulj
- Trojan.Win32.Andromeda.eazfro
- Trojan.Win32.Andromeda.cwhlwt
- Trojan.Win32.Andromeda.dgojbq
- Trojan.Win32.Andromeda.cjtgoa
- Trojan.Win32.Andromeda.cjfcqk
- Trojan.Win32.Andromeda.cqhqaq
- Trojan.Win32.Andromeda.cbkgfo
- Trojan.Win32.Andromeda.bfnvkf

- Trojan.Win32.Andromeda.cjbyed
- Trojan.Win32.Andromeda.cqhqdo
- Trojan.Win32.Andromeda.bhjqjcq

Hashs :

- 36039f56d19bd4b13a09eb9078ab6dc1a19d88868132069c5f6ec8a9c8763179
- 50558a486e9710fceaa9f744aa76208a1c8d43dac1d75278f626a00539ce8f38
- 6018c2338f105a8322c950a5aba682c287b85d0ac84ddd473593a85d1ac18d60
- 7bcfc75f235a910a60e3f86227a93206410098c25be10369eaac16a79ed3110c
- ba9101ff22cde35f4e3d1d4c4cacf9eedc8ddca37efafb054e349df84797c01a
- d45385afae8015f9a3c778a353559153fa555e3274b467a9c8f52577b316da57
- f916756f327e70c669faee656d03f9bd190e7a57459caaed678cf0c290c01862
- 000e26d45d7541b69db28952cec14083b831a234b16899c5f4db6cb5e004fdc7
- 0057afd186b369763989ec2d0527fbee13a3536eae0652fd0aff648fe20ba60c
- 00e961029f12410ed41ffef0aec0dfa6133812e039bd055660214a4b1ef4a181
- 0540de3ca3f32817196fe6806e1ac17c9150c152dcbbb9a09842619bf6d66f45
- 058c383466f2d51258e903ba5b54b235ea7baa0c4ae808083d7abd4beb83481f
- 0816a11508d8de2d97837e17c14f42964553b7f12f065b69ab76e08c32b2c2a1
- 0eb67c1d9e4b28c4b2b2762310ac04ac15129fe79d8351751c604d0fe42ba672
- 0f189f708332142a965450faf99812b1f2f2d8e4bebfa419415f10a42da2495b
- 1107ab3e4637b7abaa469c59f9dfb25eee70084ff9a2b132b33e145f2c6c1690
- 1773317faef6ac5cc7a615e53dd65c517519d285ea106b2dd69ae50e87a7c471
- 17e519f50e18348a8a949fa835363c33e972e97be90232dcdbd762edafa335846
- 190ed83c69a29ed2b79a7946b0b6cc5b13c34bb417dfdef367c3759dc75ac331
- 19b94ae85adae5679cfc9ab5d4700be13d1df9c70f798a81c78e11c0fb667966
- 1b555c6214060fe0b0404026fdeb27c8650d108ffab7fc4d55bc594bc8db25df
- 1bc4f112a39f8c10eea6622bf7c8ec379090c3aa2d0c64dec7d44a79e239cde9
- 1d4dc1574b91a9a07900c33b0efdc5f1b98b07ec2634af3b0f50acefe792c1ea
- 1d718a2c3923ae18f40ba2870dd7239c6bad0739a5c49a01ad75007fb24e38e0
- 1de2cdd8b7c7d50d728d3bfb6a3badcc394b29036e8b5296f14c2e8b220f6a3
- 1ff0a30e2400b0922c3a16d4b5f2c39a7d3e5c7c13f8b9977879037051303a7d

- 262c343d09f21d44c8a8a6da8a97c063d5b41ce462f43225c9e6ab5253678f70
- 34e21a8be6484a48677d485207b1b8454bc9f8b639a4b77a263522916efa90d6
- 34efac655858497278cbd2d86d75c5fa63ba9b8c49c3d6e1fa6a733a97aa1802
- 36c012e1d6ef6c6c77b3820d287e5214abdd7b48218834027dc26d39aa52bc78
- 36e9f118aad1b76fb7df310715b17d3f1ad1c5232fce77157e6088f1b62c75e6
- 39abb91637cbcb34b1b13214a4443176e23fe6aea1d8003c712501ca6d2309a1
- 3a3b671d9874baa8b76080ebf4a47042d76b9c3d07bae7e23b852eb5f439f3a9
- 3ec7ce04a9968011620b6fb339234d9397b89d122cb8224e08a40db8d768686d
- 40effea520d00b6b7d70f858d3e69e6a937f5587828525d3d4dc5ad0893f7ff3
- 42626d33dbfd99710aa5bcb43156cd259110e1d7f3081134467003ade0ba0ea
- 45fdb14864540fb446e98504089f67ba320433490969e3eda87a8e40fbc8f6f1
- 48274b9397879ae18b08f8fd78104a7215fa87fbb10319749e6a901bc153752b
- 4af6959b039f798e8ee6dc111f50289e12ce5e626df5066be758dfe9b77755e1
- 4b2c71e3e62743ce07efa05a3954b3323ef63227235cdf406edcb11656347cfa
- 4d5ecb2ef3cf2f6f90a1eebdb1690bb8ffa889bce6a0586cbf2c651fc8dfab5a
- 517c6f71a4d5bba393266d2185edd3b2186ff1f760b36db9cceb2a3f9aaf7654
- 51ba4eed230dc3ca5ef1ffe1ce3318a88dab034ff5cf3d28796d8c77c56e8527
- 58815f01ca028dbdda3441cb2ad743d63f5685e12d7a51ae3bb4017484b9584e
- 59bdb64068804f4f038cb2b34d62852118aff79b07038fc83097474a372602f6
- 5b21a69d58e2eaf75e9f64065521f1131da5216b75893a63e66774aa79563cc4
- 5bf9b7c146aed14d82aa28b2b41b6a10a36b5e0cf924cab725c6b77f8ebc1ca0
- 5e9cd81327ce5249df34e3ae610516f7d95ad87f130e51ddea67f03e74c79c0d
- 5f0c0366cf84c9f73f93e333eb0a116c1c9d7e126e29f88d6beb7f9c0f1d196c
- 5f39387b1141042dd13c37098fa68b4480eb802b75aad3831ac9e32981d764a4
- 5f6a01af24459a73a9bb35175b4f1f2356e4faa80e129a55b254e46f49606958
- 60feafaaf5fbd23f61af0a0017eeb0230e9c6c21fa2fe7d8098ad5a1fad04340
- 61a801c93b9795384ad56927f6c8052047306e98655d4d5a97451fd721b68cb3
- 67115bb88c6479525748d95f8c870696b9da6c78116bee4cc62e8721d5fc3c1b
- 6b5fd93d430111c3b2d95b407018773b11075f1dd945b40535153d679144f275
- 70bd2fbdf3c0287c959597b2a5001290614ee8556b81c18dff43efdaf515de7
- 717df60135ac736145237b75a2c2d0454406be1aa5970156be1a3979674d8862

- 7245691f4698571673dfe6f47b42c0afb9f1d7b38cfcfbf18c22cf40351a23219
- 730f310a5d10b3bcabaccb7a2fd2d389a990e96688e123843398c601b9046427
- 78204b5009349094ee543f3e6443926e17045c3d7b1ffc975d2be30276cb708d
- 792fa5ba370c1d2f5ba124f9ebbe91b1279d1caa1be08a9d5da8d55e9f435bc2
- 7b6acfb64d8d3d843db3e89eac28affacbf8ada71ffaefeb0b86b3a7c92948b0
- 7bfc128387849160ce69d66e55b9007e05d16f4877af921d15596687ea04bb2e
- 8077de2efcbbcf83f74849da1e0d5f5528722fb79115a83b8b14840e63d07bdd
- 81a0c263cb7cab72687a846668f48f86cc4dd8ceffb10e6134339b809cc8960a
- 82c7c85c35be70a3255f5552acb2a1e3bc7c68487879d3cf1b75f80083f9e696
- 83a1335d868eb81fc5cddfc9569f0c02702b94d545a025c8e78ecef08c0de938
- 8608394ba6c4137ac4cfdd08989ca038b929a85d781d78b5973e2880a6c45ac1
- 88ca57578651d22ef28c2efe32503edd5a34d4e1455be2aaae009d4beaf8e5e6
- 8d7d4648ed2f06e9c063491b4ab20ba228bba8d207476471b7c9b5cf1518d5b8
- 8e785428f9a6d1fd268c169c40471eceb1e8fba37cf809908ca94bdf2a74b80
- 8fd8c1009f101bda76c11a5a812a49b6c4bf167e44a4af13c1084103ec01b713
- 90c5a96ccc7a2d44511deb531aaeaa05d2d692d228c47dfad0c40ba0900258cf
- 95b0d057a6516306610d7319d0380506c069f4a4068cf5da8e9807744b24643a
- 973db89c0c1d37abf960a165da59d49e30c56d9d8bb3e968e529e2e08ddedeb6
- 99df1bb762cfc3b24e444543f22f6b5576cb2a9496c579e61fa0c0ff2d7d1425
- 9bfe5bf4eddd4aed79a239512b811374d4faa78d7b66aa7e5bf8e1e1083a316a
- 9cd999527b3fc963ba4fbb8e7fa58f35826b270d0405e31b5b9ea18948fa6d27
- a178bcd674947b2c91d73595381842ce44d84fbc88a4daad6345994bcbfd58fc7
- a1feb29bc93e9d366419fd3de1d6a1f61671f5c979a3459722b5c6059d0160ae
- a23daadd50453a5c374c23870a5b6990b7c9fc16c92d0a488a2078cdb19006b6
- a37e9dd572aeb7950cde950fa5aaa53fac6c31c9dce2b335ea170f77ec4797c9
- a554c59a6d744d2ab6eb8a1410b2ccb1b0bb2badf5db50811858b1b9c5463049
- a87de23b6aa1bd44a428585795e468b8af9c8867f835ad4a0cd6d8b685bb25d5
- a9e584179f570c5d6f6d7407b79a5878cafef530d49f19ec8d7f8db1d4272043
- aa2e7b331920da491cc275d52c07982a419619bbee5cab5a1c6500363216f15f
- aaea75d5e376ecd38f51913aeb4833a4ca343651afd699ab94256e37662a0609
- ac7f49ff307ae7af4c3d3dd787ad183247eb6f523db1edcacdb606232ed6ce7f

- acfda4b665b56d940c72d9186867a786c8b88a1f1d0ee70c3ee5eb8b2bf0698a
- b20066de9551afc5534162c33b381d486eee6561dad3f60e1104c034775a1a08
- b3d72a8272e4f0279628c117879b19005560bcc9ee5850ff1c1b4d349cf3bec8
- b5868cd68a475bfcffae62b25d0f597db51e6268f48676bd4b7907a8dda117d
- b62af0f168dc38f1294b2320f9f67e509fa794378011cfffbec1c5b55ed1e63f
- b86df41d94727831f721e8d5f4860ab243d322757b336db6f7e771c76d8427de
- b942d1823291a732e7c62850c039fef5507eb186ebe86a60c35497ce2bef5c79
- b9fdf34d62857b07da12a52573b8ff7de661186a5e24a761a3065acef39670f9
- c4c8ede1afbdc58c42676e48572111864a680198a2a60acb5665ad57efc3219
- c81044ae014c8728425758b09a8a5b1cb614c4f10fa9d1ecf630a18d10578e6d
- c86a41b92451bfe4b80af1fedaf73ae5f0bee3db3fce95cd5e7b94b59e8cd735
- c9792e7efffaa5500bf3c4de7a3efa9db17138f778446cddd95f4ad6eed500ed
- cb2bca6de9eae862a41a33b50b64520d2c4b3ed326c7ac5e1ce40f5840447e7a
- cc37fa3cfc561864a4bf71a5f962ef8f1034d97c6e8433232e840e1bc7521c0e
- d0cde564968562585a69144c513231e98dc5790ef312d604360caaef294a3e32
- d25ada4b5f98bcb1b1d6cc4f8775ff16518078bde899baf79f7b472ad6056163
- dc61da7b6e50eefc67e0f4b1c010f1dedcea0eed0f803e84096c7c7598cadb49
- de628fa2e08a6fd1d29ebf29888dd6f22f42cbae58623dd801dc5d940ec6891b
- e0352363028c91e1ace885ee9615fbcaed07f55aab9b89c6e2c1e465c177bacc
- e0c65a5df7511969f6fef22969c694970234bef8c1f8f6dc3bddaf50df7ea5e2
- e371c3418e25b8c56ac997d7d0ac233adb990aed2fedaf9d9455d24d6a748aa8
- e591e6ba8ed9c818bf2f8e008014366c8c42be84d4aee53e23ff2aea0b0eb4d5
- e82ed0c3858765b03df8b58dce62035f7596d6141efdba90a83b8a4dc9ed7b0f
- e83dd0c8fcc437de18c9d7884f4ee2f7b47b64b5cceac12ece6140b0f1e587f5
- e8462df4a5a2b73000b72b15f76f8a19a403b94893e988918a9bb83ea0c463e8
- e87c773b9c0d401e55ccf584403f34f6abec359f9cf2377bf6e5569869ba9912
- ebd28d7458474284a801691af0bfc1edb5cf14fbf94eee2216127e03ff2340b8
- ee38c5cb5c72b61500143b3170156fe9c7243221189ee750248ef7cb53bbdbdd
- f01403951dd132718d25b85107116aca8c2d621d36169063d3dec2af7058314b
- f0e4b6f2822e145902884b7e2189e096ee33b5f729220cf699ad69938a44b537
- f10cdd91a7640b634e3058e7db5264c5d456b8596a2cc03c0c259e1fdc4a2101

- f3b7ee1a8d1e0ec7dd8fda276f79d1795bfec55b6a169743b20a989ba6507732
- f4617ca8a1f8110570d3f5952911258b20a0c11aca7e578a819e711a710bc38a
- f675a9ec18fd353af41b6878b5424bbe1324572f0b20ebd895ad6f6a3e0a7fdd
- f84f64ea9d6c155ab49e571c9b462ee11e9d9335112184d2913c460cf66ef434
- f983a591da65c598e8eb6a090c72fa2b7cec854d7956fd48719e4b3f3b864959
- fb1ca88f0c0f3461506ef27f445a7484ad543c9c8a6f4bd2272942ffab61d543
- fb2fce8fd697a160cae800b2bc6190e82d6ec4adf85d4d86ab43e502ea287b2d
- fdb6f4d325770223606400b85050231a6e39140c89787d7cd7ed45aa24e11ae7
- ff6391a88059d57be6f776849342d01c17e888e6d3e191470311bacb775dd1e2
- ffdcf54a7cb33f0e1a39108f169cc749d6ba22f1026c2966dc1fb9f1705df23