



NOTE DE SECURITE

Titre	Malware “ Nymaim ”
Numéro de Référence	61151702/25
Date de Publication	17 Février 2026
Risque	Critique
Impact	Critique

”Nymaim” est un malware de type downloader, dont la fonction principale est de télécharger et d’exécuter d’autres logiciels malveillants sur le système infecté. Le mode de propagation le plus fréquent demeure le phishing ciblé, où des e-mails frauduleux incitent l'utilisateur à ouvrir une pièce jointe (souvent un document Word ou Excel) contenant des macros malveillantes. Parallèlement, Nymaim est connu pour son utilisation intensive de kits d'exploitation (Exploit Kits), qui scannent silencieusement les vulnérabilités des navigateurs web ou des plugins obsolètes lorsqu'une victime consulte un site compromis. Enfin, le malware s'appuie sur le malvertising (publicités infectées) pour rediriger le trafic vers ses serveurs de téléchargement, transformant une simple navigation web en un point d'entrée pour l'infection.

Une fois installé, il récupère des payloads supplémentaires depuis des serveurs C2 contrôlés par l’attaquant, puis les déploie et les exécute automatiquement sur la machine victime, compromettant ainsi davantage le système infecté. “Nymaim” possède une architecture modulaire qui lui permet d’être enrichi par des plugins ajoutant des fonctionnalités spécifiques. L’un de ces modules est notamment conçu pour intercepter les identifiants d’accès aux comptes de messagerie et aux programmes FTP, puis transmettre ces informations aux serveurs C2, facilitant ainsi le vol de données et la fraude financière.

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 :

- 86198c44fcff1eacc8b13a96ae93e2736c37783c81226e3ca28853777d6e9770
- 1a48e956b6f78067c23081873a9c03b9c4e2a16289b2685e451ed2c4a3ee96d8
- e7c620fb4cfbc881f984628147e46ef883a14d6f54c91adf7c87fa0950fd4f5f
- 792fac17ee074eaf3d5c70899e0bc4f6f9b24565e3e63e211cd7165afd2d9fc8
- d96d920ad3dfbc67bedf5cd2ce5fe3a3838c5dba443dfaaf1f170e1c65c1be8
- ab7a28eff7527fb4241ea20359f6dd817ca31c009db6347d891b140acc30a48a
- 6b4a536aaf805cdd8d37aa7a324efd0a4b0e7ee31131467ca28c6b48cfe3ce07
- 540cedcd8517f292cdc61224f99c7b3ed132ac6ec5ff0c9bbe8ee47235b69ca6
- dada13ccb513d9f7aa4145114752ea4c36c2712c807f216ba23afa659cdcc27a
- 5d26aa67c57c87b710e8b02f16cb75d0a99844ec69f0eab0bf029703913f2078
- b5aa63de7d9691c2a973f54db8196d35a0ea1889816cd6820b849e523d8076fd
- a518759dedbcb0b75a1f652a9b592a1c596ea64c27869ddbc6aa939f4df64c88
- f81ae510dae047e4216a13fb003dcd2161ab161e03c02f09f4c23abfd0144c5f
- 3ad211c56a4809ba2864521c6b983f1c0950eb94ecaa590732f29a1f43b75698
- 71fd4442a33454d704c2e857887669fbb76fad97c3f5543d76d2482889c6b218
- 3a11ba5354a15fa159f3b41e768638f65ad3e4ca98a2ab66d6a14fc3fe9de602
- 08c7701b837b72ccf68a1d6e4669546532f7391e58da71df7f57617bafbe5336
- b0a0f44e00ccd438df95ae2e240fd0de13794d1a58091edb275b36273ea98745
- 020700b43ac301a9fc26fe29cf8bd37449ea9f24cbba7f513f7596f0c9c2ec8b
- 977ec3c1c3eb1aded1880ceace4c40eedc9a486ab06f9c7c55ed29d2e0b8ea00
- 65f95ddd70aa6b8bf09ac5ca6ca6d9c8e6af50778c4d08c99b3b50539c695dcc
- 2b6b70bae80392d3ab139876a8434a0bef01acb5c22e11f250c5d9d200908e42
- 317742d4e747697201f66b9abf2a67184f4857feea00eb596a5a0e4677828c0d
- 7daea674c0044434d1fb836b530ae3d4873e1b2df63d1cf3dd1fecc8fb6ac8ba
- d282b63274868bab6d45dd82588c74572dcf0fd61d0692605866ca87e421bdcb
- 68d2564892dbd541cbd155e15be3e84fc4cf1731bfdc01c4f75a1b3eb8206561
- 3bcf540a39a50c83eee39c21f51adbdf560b0fe0ea4a643d7017fb3f215b39bd
- c571c7e5aeb5984a40346573680fa386bd9749384fc9c77f36a1214694683b41
- 0dbf4a02aa9d9cbbcfcc934e12c008a33a9420c3f1163370e30f570e6055d40f
- 701307b86a3ff77b15816d3d51eb7901e3c48b385937a11e038a6a61e3854ccd
- 84a2a216e58fc402bd3b25a89d4aabb1a26c99ad5c000491e98d2c5ff1fbf78e

- cee16c01b408006185f548b5363b86b45bb97e8878628cdac4ee4a552d77071a
- 00b0d34b3aa0a1786cd5327c0d5c9e56d8f7442fb6c0a9ff257c2e39599b9de6
- 8ec324e298d51c661d472cfaa93e2f1d5e6f824ef3a44bfe20131f981b1ef0c4
- d6abc9c2f15c380e489de88d653a8a8409613296b3f666f57a3e54151a2c3565
- 946deec750ca2d319adf6a5663f817cb3a8f222bc2149598163585de357faa3b
- f0c4696e869c17f690ce11d688da98b43454dd6435d8d56533c1593b4952e5d7
- 3b07bc058e8fd1dd60d9a04ff759c5980b0442aecb4e25cdca030a1baa1ac009
- 4d7104b2c85a305e0d7bf293a38427e8e8413fd07bfa89a502a6d774f2d8de4f
- 249c41af31dcedb3645e37168d3976f8913788040781aac8f9100dd261d6bd2c
- 39639dba0e9c01460d918aa21f680de09c87bf05b316a9de14b9507c15e41f46
- 48897d658dc17c4d075978aa656190424b61abee29fc2c500390dbf5757a4647

IP :

- 116.131.57.65
- 151.101.1.91
- 151.101.65.91
- 151.101.193.91
- 92.63.197.221
- 208.67.104.97
- 171.22.30.106
- 107.182.129.235
- 104.18.38.233
- 188.119.66.185
- 31.214.157.206
- 188.119.66.185
- api.aria2c.vip
- aria2c.vip