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	" Prometei " malware
Numéro de Référence	63442204/26
Date de Publication	22 Avril 2026
Risque	Critique
Impact	Critique

Le malware "Prometei" est une famille des logiciels malveillants modulaire orientée principalement vers le minage de cryptomonnaie, le vol des identifiants et la compromission réseau. Chaque machine infectée rejoint un réseau C2, permettant aux opérateurs d'exécuter des commandes, de déployer d'autres payloads et de maintenir un accès persistant.

"Prometei" exploite principalement des vulnérabilités connues affectant des services exposés, notamment le Remote Desktop Protocol et le protocole Server Message Block. Parmi les failles exploitées figurent la vulnérabilité critique « CVE-2019-0708 », ainsi que des vulnérabilités affectant Microsoft Exchange Server telles que « CVE-2021-27065 et CVE-2021-26858 ». Le malware peut également se propager latéralement au sein des réseaux compromis en exploitant des identifiants volés et des partages réseau mal sécurisés.

Une fois déployé, "Prometei" adopte un comportement furtif visant à éviter la détection. Il utilise des techniques telles que le « credential dumping » pour récupérer des identifiants, le déplacement latéral pour étendre son emprise sur le réseau, ainsi que des mécanismes d'auto-mise à jour pour intégrer de nouvelles fonctionnalités. Le malware met en place une infrastructure de commande et contrôle (C2) dynamique reposant sur des algorithmes de génération de domaines (DGA), lui permettant de modifier régulièrement ses points de communication.

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

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 :

- 11911eb531be135c23b35caba3879dad5a89c806023b5522978893e9aaaf0cf4
- f32b8a107a9b8a81d6a5bc4edded3efc6a711fda6e8b81b913de61bd3006b0bb
- e826a198a6c9219a2bce89fa327ab1be85515e683f1939ec742c58d91fe23206
- dec965b343475f2ced0fb24e21c83e8a32ea829f85daea2b395a2f3f861ec9d9
- d9c96f1720bce2f189e5eaf2adb1aec4d5c0595ce43beb58ddcc0a1f1f12f73d
- fd5cf27100f3b4b1429e59d34f9db98aff327a89a924cefe36ad6480aad85356
- f2d7e2f333dc827dfaf840950b4a49f9a46bcf9c01bdfd949c3b18362c9468ef
- 75e23acb4cf98eef558849d178caf5fc80a749c37bbf543900736b4db9e87210
- 1f69d5ca357ae74df3b0e237c8b4f3ede1aa32a4bb3e5f7369fea068c4cf48b9
- 1742e0df538512d4c99ab43ad44629a352440d0070fc3581edac29a32b4a5b0b
- daaad6e6ead5f49a21cd7331af6893dd066ecfa77b3d3c8e66febf04a19c4e3d
- fa04f86ea76039527a2d08ef3e02fbc24c0f831bb541d3fbd3869d18fecfe253
- 7704a9288674eda67e5623098e3a574869b890cafecde29c5fee7ae2059b443b
- 207a7e0a93ff730c9618409f15f75280299b3020b92bfc4fb6ee8c73476c3f92
- 27073a3da53569c4b63b122e4af83709eebdbbc153878c85d76f5f0712dcf6cb
- eeaa242a838f9782f3ebccdd23890ccbb0c8c4d7a89446d482acb318c96da1f3
- 30b6ff36e06118347e842d13b1c1c7920e125d5717ed97d6afea0a7cae906740
- 02a9ed5ff679d65cff75cc5369ae4055e69fbc31fcf63999d9571f463f8b9dd9
- 1eff9b28506f50e122271e1aeba096fe878379f082db453db9359a0bd3dd2caf
- 134d78f929bca977cc2759b3f17e910e510eeb19ae3ac7400dc1beec27651a4b
- 315656724634fa7529edc8eb5a08e4dc27e3cb3aced4c730c99f93088896d23d
- 34e9982ee33cd630b7a9dd4070225ced552dff25e6284233c65aa4e6d6c51186
- 81a7def82aa84d91a1feea4f62166a024389629cf8564839eb54bffae34b17ac
- c9d2e45924b41b90f5e5aefa50e4c8cf1ec27a68c209ab13d484d8db1633c4d5
- 4bde2d0bee0e9855d6d91d0e5df86be77eef87a23f9a72e25d70e8c41000da44
- 370e7242d9682c0093d767dee92db19e7379bb2a97efa3411f96fc1b4b2f563d
- 26ba2a7a8e1aaf1c9b451073847cc3ced5634fa5965552007fd3a7608683f34e
- 1779c420231f39443aa48166868d58130ea2e7051648db4b885ba3d1d4e84311
- 39ce0c4d21b8a42cb6ad4b5da8390ff49715fe9d4126cfbea8f7758f85d28984
- 6df162fa35abb65096de167702acd8976e6a85acedd9d0e1850ffab94e3b3a55
- 799d7ef219bbef02e2ebde3235e3749c228072cab9289ed95e4baaeb0b209122
- 317fd0aae3e9fa8a8821990a45d4557b28e1e59b61c453723d87b8199f1fdf98

- 0a2bb131342aad35e59188b8a320f53a7a665c97bb530b85acdf6731dfda2539
- 3bcbd9739bffdfde1faace4e7ca130eefcf29ed12b5c3bd660ccca1432153460
- 653e499f26ff99f6bc103f3a684e01f10e1eeb56f12880af700d394d1d6bf347
- 383ad930162323c55303c5bbff386847c39724aa65ec39caa0154780c04c8b24
- ec29e6294c65c003d6c9264917ad8494e0479acbeca542fd43850cce8675116b
- 1631741f8c7c5963e8b437e74fc8acd96bffd43284b58653005257758ac5068e
- d45d5d9b272caf655a43fe1cd6e8291807e9d42e446497ce64c3604764bdcacb
- 6d09a9d6096851cee883cdc8d67773112e9bb203af4eace37fb7f00be54a2432
- 608b8f6d94e7ed29e95d880a220dbc9847511142139d69e64475c4d18c84c6af
- 32f87418afbfef145c9d16d040545f9ed8de2020c4e78ec556727c84216564a3
- 34eb8483d7bca53ebe029f52f37aebdd23b6f061e024babfc1d063b5b10eecae
- 746d2d149ea5df9cd00437d78d20153778c05ab8eb4f5e6fb2478c36caf54f25
- 6cd9c17117c0e059b4545e6455813f8d0124ef7b2676207c76b80f8c8c3628dc
- ab07223f88f197bc8aa1acdd7af027e170b5931e429f6678f43c518846e2f4bf
- 806a5eabbf1d37a28727021cb594680fdaf0255683ac9b525059708e83d92170
- a8de4246bb401fcc19f2e2a891005788ec59ecac9bc9aedcfb6c72eb68ec1990
- 126c54fad8666300598ef06653754c34709e0f2d40d83b7069f07eaef1d4d18c
- 444532d42b88760225c133604f4dd351dfc68feb1340d73c5a26c14605e0ae1f

Adresses IP:

- 178.62.95.143
- 186.158.209.147
- 176.122.106.103
- 103.190.242.61
- 149.202.115.129
- 46.62.141.104
- 136.144.247.239
- 31.14.136.249
- 181.177.142.103
- 47.242.179.47
- 45.188.76.65
- 45.119.85.237
- 103.184.128.184
- 185.124.87.53
- 103.205.241.245
- 103.143.206.236
- 161.97.164.177

Signatures malware :

- Linux.BackDoor.”Prometei” .12
- Trojan.Linux.”Prometei” .4!c
- Backdoor.”Prometei” .gen.fvzc
- Trojan.Win32.”Prometei” .4!c
- Unix.Trojan.”Prometei” -9992782-0
- Unix.Trojan.”Prometei” -10045459-0
- Trojan.Sdum.dib
- Trojan.Crypt
- Linux.Siggen.4460
- Unix.Trojan.”Prometei” -9941765-0
- linux/malicious
- Trojan.Win32.”Prometei” .m!c
- Win.Trojan.”Prometei” -8977166-0
- Win.Packed.”Prometei” -10058937-0
- Backdoor.”Prometei” .b
- HEUR/QVM19.1.4814.Malware.Gen
- Unix.Trojan.”Prometei” -10045451-0
- Trojan.Linux.”Prometei” .m!c
- Trojan.Linux.”Prometei”
- win/malicious
- Trojan.Sdum.gen.wtxc
- Malicious