**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** | BeaverTail Malware |
| **Numéro de Référence** | 55972207/25 |
| **Date de Publication** | 22 Juillet 2025 |
| **Risque** | Critique |
| **Impact** | Critique |

BeaverTail est un malware utilisé dans le cadre de campagnes d'ingénierie sociale ciblant principalement les professionnels du secteur IT. Ces attaques se déploient notamment à travers de faux entretiens d'embauche organisés via des plateformes frauduleuses, telles que le site « BlockNovas ». Les victimes, convaincues de participer à un processus de recrutement, sont incitées à résoudre un prétendu problème technique (par exemple, un dysfonctionnement de la caméra) en téléchargeant un script piégé contenant le malware. Des paquets malveillants diffusés via le gestionnaire de paquets npm ont également été utilisés dans le cadre de tests techniques envoyés aux candidats.

Une fois exécuté, BeaverTail permet l'exfiltration d'informations sensibles, notamment des identifiants de connexion et des données de portefeuilles de cryptomonnaies. Il agit aussi comme loader, téléchargeant des malwares additionnels tels que le backdoor « InvisibleFerret », qui permet une prise de contrôle à distance et une persistance sur les systèmes compromis. Cette menace présente un risque élevé pour les organisations, en particulier dans les secteurs technologique et financier, ainsi que pour les profils disposant de privilèges d'accès étendus aux infrastructures internes.

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 :

- 48e75d6e2bdb2b00ecbf4801a98f96732e397858
- 0f5f0a3ac843df675168f82021c24180ea22f764f87f82f9f77fe8f0ba0b7132
- 40645f9052e03fed3a33a7e0f58bc2c263eeae02cbc855b9308511f5dc134797
- 2d8a5b637a95de3b709780898b7c3957f93d72806e87302f50c40fe850471a44
- 6a104f07ab6c5711b6bc8bf6ff956ab8cd597a388002a966e980c5ec9678b5b0
- 75f9f99295f86de85a8a2e4d73ed569bdb14a56a33d8240c72084f11752b207e
- da6d9c837c7c2531f0dbb7ce92bfceba4a9979953b6d49ed0862551d4b465adc
- c5a73896dc628c23a0b6210f50019445e2b8bfc9770f4c81e1fed097f02dfade
- 1f9169492d18bffacebe951a22495d5dec81f35b0929da7783b5f094efef7b48
- 6b3fce8f2dad7e803418edd8dfc807b0252705c11ec77114498b01766102e849
- 94ef379e332f3a120ab16154a7ee7a00
- d801ad1beeab3500c65434da51326d7648a3c54923d794b2411b7b6a2960f31e
- 92aeea4c32013b935cd8550a082aff1014d0cd2c2b7d861b43a344de83b68129
- de6f9e9e2ce58a604fe22a9d42144191cfc90b4e0048dffcc69d696826ff7170
- 10f86be3e564f2e463e45420eb5f9fbdb14f7427eac665cd9cc7901efbc4cc59
- fd9e8fcc5bda88870b12b47cbb1cc8775ccff285f980c4a2b683463b26e36bf0
- 24b89c77eaeebd4b02c8e8ab6ad3bd7abaa18893ecd469a6a04eda5e374dd305
- d5c0b89e1dfbe9f5e5b2c3f745af895a36adf772f0b72a22052ae6dfa045cea6
- 0621d37818c35e2557fdd8a729e50ea662ba518df8ca61a44cc3add5c6deb3cd
- 9e3a9dbf10793a27361b3cef4d2c87dbd3662646f4470e5242074df4cb96c6b4
- 07183a60ebcb02546c53e82d92da3ddcf447d7a1438496c4437ec06b4d9eb287
- 8de446957ce96826628c88da9fd4e7ff9d6327d8004afc4e9e86d59e7d6948dc
- d0a5b9dc988834cc930624661e6e7dd1943d480d75594fff0f4bc39d229c5999
- cde5afd20b7bb5c9457b68e02c13094125025fb974df425020361303dc6fcdfc

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

- c0110cb21ae0e7fb5dec83ca90db9e250b47a394662810f230eb621b0728aa97
- 30043996a56d0f6ad4ddb4186bd09ffc1050dcc352f641ce3907d35174086e15
- 36cac29ff3c503c2123514ea903836d5ad81067508a8e16f7947e3e675a08670
- db6e75987cabdbfc21d0fdcb1cdae9887c492cab2b2ff1e529601a34a2abfd99
- 104926c2c937b4597ea3493bccb7683ae812ef3c62c93a8fb008cfd64e05df59
- e58864cc22cd8ec17ae35dd810455d604aadab7c3f145b6c53b3c261855a4bb1
- 2618a067e976f35f65aee95fecc9a8f52abea2fffd01e001f9865850435694cf
- 6e09249262d9a605180dfbd0939379bbf9f37db076980d6ffda98d650f70a16d
- d502f822e6c52345227b64e3c326e2dbefdd8fc3f844df0821598f8d3732f763
- c8c11f9b308ea5983eebd8a414684021cc4cc1f67e7398ff967a18ae202fb457
- 09a508e99b905330a3ebb7682c0dd5712e8eaa01a154b45a861ca12b6af29f86
- 592769457001374fac7a44379282ddf28c2219020c88150e32853f7517896c34

Ip :

- 37.221.125.200
- 23.106.253.194
- 167.88.36.13
- 171.22.127.221
- 45.61.160.14
- 147.124.212.125
- 144.172.79.23
- 147.124.213.11
- 45.61.131.218
- 173.211.106.101
- 165.140.85.105
- 147.124.213.232
- 144.172.105.235
- 147.124.213.19
- 66.235.168.17
- 165.140.86.154
- 144.172.105.189
- 144.172.109.98

- 45.59.163.23
- 66.235.175.117

Domains :

- blocknovas.com
- softglide.co
- lianxinxiao.com
- easydriver.cloud
- blocktestingto.com
- gitlab.blocknovas.com
- wuxiantechltd.com
- worldenterprise-beta.com
- apply-blocknovas.site
- bookings.blocknovas.com
- lumanagi.online