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	"Acreed " infostealer
Numéro de Référence	57872910/25
Date de Publication	29 Octobre 2025
Risque	Critique
Impact	Critique

"Acreed " est un logiciel espion (infostealer), apparu en février 2025, connaît une croissance rapide sur les forums cybercriminels. Suite au démantèlement de Lumma en mai 2025, "Acreed " s'est imposé comme le troisième infostealer le plus actif sur le marché clandestin, représentant environ 17 % de la part de marché, derrière « Rhadamanthys et Lumma ».

Les campagnes de diffusion d'"Acreed " reposent principalement sur des courriels de phishing contenant des pièces jointes ou des liens malveillants conçus pour inciter l'utilisateur à exécuter du code malicieux. Elles s'appuient également sur des publicités compromises (malvertising) redirigeant vers des sites piégés, ainsi que sur la distribution de logiciels légitimes modifiés ou de versions piratées diffusées via des plateformes de téléchargement non officielles. Ces vecteurs combinés permettent aux attaquants d'élargir rapidement leur surface d'infection et de cibler aussi bien des particuliers que des environnements professionnels.

Une fois exécuté sur un système compromis, "Acreed " procède à :

- La collecte d'informations système (noms d'utilisateur, adresses IP, configuration de la machine),
- Le vol de données de navigateurs web (cookies, mots de passe enregistrés, historiques),
- L'exfiltration d'informations de portefeuilles de cryptomonnaies,

- Le vol de jetons de session liés à des services cloud tels que « Microsoft 365 et AWS ».

Les données volées sont transmises vers un serveur de commande et de contrôle (C2) contrôlé par les attaquants.

Le maCERT/DGSSI recommande d'appliquer les mesures préventives ci-dessous et de l'alerter en cas de détection d'une activité relative à ce groupe via « incident@macert.gov.ma ».

Mesures préventives :

- Intégrer les indicateurs de compromission (IOCs) ci-dessous au niveau des moyens de détection.
- Surveiller les connexions HTTP/HTTPS afin de détecter les communications suspectes et les comportements anormaux.
- Mettre à jour les solutions EDR/AV avec les dernières signatures.
- Analyser les logs d'authentification pour repérer toute activité anormale depuis des comptes compromis.

Indicateurs de compromission (IOCs):

IP adresses:

- 186.2.166.198
- 89.169.54.153

Domain Name:

- my-sharepoint-inc.com
- googl-165a0.web.app
- cloud-233f9.web.app
- cloud-ed980.web.app
- cloud-233f9.firebaseapp.com
- googl-6c11f.web.app
- my2cloudlive.com
- cloud-ed980.firebaseapp.com
- googl-6c11f.firebaseapp.com
- my1cloudlive.com
- web-16fe.app

Hash:

- 92495afb2cfdb814bc59c9ab2fbcb848423fe8479e97d657e1208da965918f40
- 24f0ca5a05fbe67a6c11e7e5e63308392abd36a0b747daf0a8a506e5f4fbc184
- c20f0e9bfdf1c25a68d1646f2b1228cec9460c71a043c3719789afc019038ce2
- b8d179cca6fe61ae175cc8c2f4377d1c249c24a73dc616358267f02d23d61776
- 2cb1735ac9dab2b519b209b56cdad5e434a97590a1754fd07bdf52425ae58bc6
- 13c599e1c083786286c06c9e9ff4301bb844d1e911cd138d4b098ce40198ee1d
- c84f48d7f383a98220b8d3aa851b0c6b6516c4fe6c90ba4dbee8be2d7164ce73
- 9dc45228abaeb224c2981675c8c9a2018d6fecdc06a819382b90674711a71fd7
- 64948576fa1031f19ff58b8dc1abcf65bba29e5ba97c99c7b7fba88f93405996
- 31856f84c73b66428547afcfb812051f45b32fdd4ca41fa005587356773a10d0
- 3d94cf5e0b4d7ea8cc616ea0993f2d87774b037381687078284eac19e8738935
- 39cff529c3b085d93c3ca08853663146d571496dcb29f406f8fbbc90e6976c7c
- 0aaee7554c09eb7695b5c835f4016166221ba3330791777fe0db9d7dcae5ec29
- 5adf74aec76fd9aafd0e4a53e7c701ac757437556074c9412d42bf9a4b807beb
- 90137cca23dea5ef2aaaf21b4479710ebc77525e52896287d6a6f1ef86570339
- 54958f7caf43c3d8edb3ca4653421a7ea3b3bd327ae96e14c372df2649feb34b
- cbe48ec5996c53e96f5b126669bcfb92440587892798580f3341f29403bcf58a
- d6e38bbcad701ec0cc8f0727fd437e563d069a610dd147bbb8086efd20a63bd9
- 3703037a2794aeafb56379b6c50f7e73ba3190b7e7150ddb79aca4084c259668
- 17cb7a9755659a69497e8434174d503e8e978dc4238dd9dec4044d8ee015d2cf
- e44d66a0e46e09b1946682c0e83ed62e9c679ef70a6f05e769c5d12a4f7941a4
- 3de47aee739a91085e62a6a0bb4d1640f7a55cc08db6906bd8724c43a6ba9209
- 606b2261d15df8ae587ac7cb929d37de6b4520f4d6a7a7d3b98134de915925e3
- 2aae207859670ff81542cf41c661e1ffa1ccfd304c7dd3dceb59206bb14d6f0e
- 6d9d9ed4ddbf63aa133bd1616942ae2d984baaca1550933ee84e70d3b33d302c

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