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	"AZOrult " malware
Numéro de Référence	62740204/26
Date de Publication	02 Avril 2026
Risque	Critique
Impact	Critique

"AZOrult " est un cheval de Troie de type infostealer, conçu pour exfiltrer des données sensibles depuis les systèmes compromis. Il cible principalement les navigateurs web, les clients FTP et certaines applications afin de collecter des identifiants, mots de passe, cookies, historiques de navigation ainsi que des portefeuilles de cryptomonnaies.

Le malware communique avec des serveurs de commande et contrôle (C2) pour transmettre les données volées, recevoir des instructions et éventuellement télécharger d'autres charges malveillantes. "AZOrult " est distribué via des campagnes de phishing, des exploit kits ou encore par l'intermédiaire d'autres malwares.

"AZOrult " peut également agir comme un loader, c'est-à-dire qu'il est capable de télécharger et d'exécuter d'autres charges malveillantes sur le système compromis. Cette fonctionnalité est avérée et largement observée dans des campagnes réelles, où il est utilisé en combinaison avec d'autres malwares, notamment des ransomwares.

Enfin, les données collectées par "AZOrult " sont généralement revendues sur des marchés clandestins ou exploitées pour des activités frauduleuses, telles que la compromission des comptes, le vol financier ou la préparation à des attaques ciblées.

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/DGSSI recommande d'intégrer les indicateurs de compromission (IOCs) ci-dessous au niveau des moyens de détection et de l'alerter en cas de détection d'une activité relative à ce malware via « incident@macert.gov.ma ».

Indicateurs de compromission (IOCs):

Hashs :

- 0160a6c3437adea4ea0ed1da9ab2f30e07f261526ce68fe9b7234cb3ff70db4a
- 0fbbf22253089cf5c00d07b7711784f0c736a2cf276dfe8e906d607ce2eafb6a
- 11856382d73029171f8963d0bbbe0bf5b120dfc850d65f6aa1ae7bc69065116d
- 1654b67cce0768ca3fe0b183aa616d4a0b13be9b98e40328e7f854b8e7565ecc
- 1bbe873ce003f250e416fc57b8bcd5077b754f0a5c0f05ebe29475a32a6ab848
- 1bc2043c6c927eef2f471491438eecd958605f0970179b0c0ccad2d449a55ec6
- 1c0a02b537e0655089b25cd440e96955f6f0134db8ca54d22f5070c8b6b37e67
- 1c214d289902b74aa877c4e0c077c6078595122385836e32fb258ef7526461c2
- 24712785cb8503e7e9ecdaba9c951b534bc0992f3837df3a2ff6eeedc4edacfc
- 24bdca810b99f38111aca5868686e3f03e1ce140b3f757172ebe0afcf68161a4
- 254e0adc83d19c0b163ced66e59b72df66c6c5bc1955246473313ae7bd5c402f
- 26a369e2d92960bf95d52507ff4119e2f3e6183a36cf0a3b9e9a3e993c932ce7
- 289e4b6d21073fac8e501ec588e849ea91021ab287e9a1d7e5003a0df9a61927
- 2d756d57dd04e6f7d76c5a42a92c5b8bd5d3402106d838ee75cf2e944fb14554
- 2f18cb1000b73d9857f5098cdd31d4d0fa892ce9e4905f2b7b91edb0db7d6bfc
- 3191aa6584ff77d59bb6e6f85bbbc95cfd5eb9535df58dca63fedca26fc9d41c
- 3518a14556756fea9aed12471bc681199a828cc03f83058837af3041ac4d3d8e
- 353b74e4fca84879a4f7406e1ab7972761bfec524b15294b9feab567b8d0744b
- 3bbc5b572d33534e82a19f69f4178889557c73b779207e4593bb995c778123c4
- 3d7d1b5249487b019906bf171e620c637d600bc34e25f7a74f29e2022ccb0500
- 3e385633fc19035dadecf79176a763fe675429b611dac5af2775dd3edca23ab9
- 3eb31fc91a1b2f31d1114937e6f71e03656d764862e5419ff815ade6dec9776a
- 40f404d5f2e4903b8f75c4cf8088b376a861b2640c1832df376cf7bbfe771f9f
- 43b313f88945f1cb8773509ea58d421f69283cbd2b88176158d21f6e1b4e104c
- 4603c35a5b812feae2befb09ed5f56cc7fd1361e66c4b82704fb2bcbd352d426
- 487d5b08142c47fc2297e0ed60a1e83a42037a4134b5b5add01fe93c70354919
- 4a1198c7f8bb55be3c6a373a6b8d87744c594b79a35ba236fe2f39831b26995d
- 503d831ae30f65c0d07e3b1ebb57c7c254123cbeb908ee7694da999fe77ea6dc
- 52a01f52c23a884b3f4e1c52183eb3a2922cdc6832d43bbfce309ac7b96025eb
- 560ad29504c055e85722fd2a149da7f1a3a5c38ffd4a0d8103f65588c0c77a68
- 571de4698edff95c328d3521b11e800a3b9659ad55281dd7729b2ce2210ac931

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

- 5928b0f62b5559f96b7ba18c3ce8f75336483f869a90ef34ea94c8c917c489da
- 596adfe20faf22048b1587ecbea5ee950f3b4a0a0c88d76682ddccbd8e7f3825
- 5b7ac07ec896bf4c742f55c5e54fc485ce65708a052e5d4c020a000802777db4
- 5b9c1dd1394b82458dcee9dbfa26951228bc448d4781aae33ae035edf6ad47bb
- 5fa1d35389760d5933130a0ed092e38d065d77833f54da3af856f6afb85f1472
- 60b290310f67adb0ae186b4b938ca466a6b55653b2519261fa425127f5500a1f
- 612c1e3ee2a0c7eed672d42eb83a27a0eab6bf184994ec983d225dc956f1df96
- 6195491f151636735ef4be19bc22374b9700ef9ac8eb78eaba6382785249f52b
- 6581248fd3b5416f0b2cb4e71321f98b2d25ef557e81456eeb0be97e5a108e18

IP:

- 168.119.250.13
- 216.170.114.4
- 185.189.151.50
- 31.41.44.179
- 185.79.156.23
- 45.88.186.251
- 192.121.112.218
- 51.15.215.173
- 195.245.112.115
- 62.173.140.150