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	ViperSoftX Malware
Numéro de Référence	56941709/25
Date de Publication	18 Septembre 2025
Risque	Critique
Impact	Critique

ViperSoftX est un malware de type « Info Stealer » diffusé principalement via des logiciels crackés, des réseaux de partage (torrents), et via des eBooks malicieux pour tromper les utilisateurs et faciliter l'installation. Il utilise des techniques avancées d'évasion et des mécanismes de persistance, rendant la détection difficiles sur les systèmes compromis.

ViperSoftX fonctionne selon une chaîne d'exécution multi-étapes : il exploite l'environnement « AutoIt » pour charger du code dans le Common Language Runtime (CLR), puis exécute dynamiquement des commandes PowerShell. Ce mécanisme permet d'exécuter des opérations malveillantes sans laisser de trace évidente et d'échapper aux contrôles traditionnels. Les variantes 2025 ajoutent des délais d'exécution destinés à contourner les solutions de sandboxing.

Les fonctionnalités malveillantes comprennent l'exfiltration d'informations sensibles (identifiants, données personnelles), la recherche et le vol de portefeuilles de cryptomonnaies, la capture du contenu du presse-papier et le téléchargement d'autres malwares (Quasar RAT, TesseractStealer…).

Pour se prémunir contre cette menace, il est recommandé:

- D'intensifier la sensibilisation des utilisateurs aux risques liés aux logiciels piratés et aux sources non officielles,

- De surveiller de près l'exécution d'AutoIt et des scripts PowerShell dans les logs et solutions EDR, et de restreindre l'exécution de scripts non signés.
- Le maintien à jour des solutions de sécurité et l'intégration des IoC pertinents (hashes, domaines C2, …) dans les outils de détection.

Le maCERT recommande d'intégrer les indicateurs de compromission (IOCs) ci-dessous au niveau des moyens de détection et d'alerter le maCERT/DGSSI en cas de détection d'une activité relative à ce malware.

Indicateurs de compromission (IOCs):

Hashs :

- 1b26d62c80689746de39869dfab8d8f05257bd16e46fe923344988802569be10
- 0cb5c69e8e85f44725105432de551090b28530be8948cc730e4b0d901748ff6f
- 3529336d0733bd2ee92acc8ed332f6c4eed36a8b0b272371ffdeb80117689b26
- 0ca08b8044c466e286fb5ec2162a23fe35dda700019a1bc9f4528c777abb2a69
- 5c5202ed975d6647bd157ea494d0a09aac41d686bcf39b16a870422fa77a9add
- 42018acd1660989d939814b2bdfaac086540f7a793b0d1b5b82ef72cd7dc2d6a
- 09620efdc1324f063aec6aa3d822c194f253d9393c5a7b4f7c8880b8fa260d2c
- 23b9075dac7dbf712732bb81ecd2c21259f384eb79ae8fdebe29b7c5a12d0519
- 30a7ff659d267e9e201273087d4ced99f6eefe3078b40f38a1f6c5ff4e6d4fd3
- 0a0b5f64870c166c1fe246a7ac815f738e15dbc8481b985da862026f61c48282
- 380697610810cdecaa497ad75b031106b486bc6c7da78add23885a963aab6dc0
- 1d6845c7b92d6eb70464a35b6075365872c0ae40890133f4d7dd17ea066f8481
- 3fe448df20c8474730415f07d05bef3011486ec1e070c67683c5034ec76a2fcb
- e1dc058fc8282acb95648c1ee6b0bc36b0d6b5e6853d4f602df5549e67d6d11a
- 705deecbbb6fd4855df3de254057c90150255c947b0fb985ea1e0f923f75a95f
- 7107ab14a1760c6dccd25bf5e22221134a23401595d10c707f023f8ca5f1b854
- d7dfc84af13f49e2a242f60804b70f82efff7680cddf07f412667f998143fe9c
- 083837c37de9fce9e49257bc2b38dec11530b990b023fadc6f82a7cb00685fc0
- 2769ff525276045565a15fb959ae54a1ba294eb7903fa80a8656577d7dd5e76c
- 204a056399bbb7e1b4fcf2bdd8f463cf2d3ff21d9f7c5b745d74d62eb6184e88

- 0bad2617ddb7586637ad81aaa32912b78497daf1f69eb9eb7385917b2c8701c2
- 7b75c1150ef10294c5b9005dbcd2ee6795423ec20c512eb16c8379b6360b6c98
- 0a4888750a50461effd10757fc9bebfacbc661a9ad57fd4c23eefbc735f7ca94
- 0de9a23f88b9b7bda3da989dce7ad014112d88100dceaabca072d6672522be26
- ddee23e2bfd6b9d57569076029371e6e686b801131b6b503e7444359d9d8d813
- 7c028a7a4eccd48049f0b66ab0211cccf136e56d2af8cd27cfb1c720a43993d0
- 947215a1c401522d654e1d1d241e4c8ee44217dacd093b814e7f38d4c9db0289
- 4da1352e3415faa393e4d088b5d54d501c8d2a9be9af1362ca5cc0a799204b37
- 88c46a74d0b7ba05e4641628f546cf29b322f1e0147b5bcb8439f3716f6da847
- 0d8e99281629352c68e5d1e462db3b003571fdc21149d6834bd2aa2d86ea03b9
- 22981d8cd10e0aeede5a2c5c209cf2d1a46b9eb54f85eca9f97d816b202d186b

Ip :

- 86.105.252.246
- 212.56.35.232

Domains :

- chatgigi2.com
- apps-analyser.com
- api.private-chatting.com
- arrowlchat.com
- wmail-service.com
- static-cdn-349.net
- ahoravideo-schnellvpn.xyz
- wmail-blog.com
- myststemsgame.com