**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** | Cheana Stealer Malware |
| **Numéro de Référence** | 49032908/24 |
| **Date de Publication** | 29 Août 2024 |
| **Risque** | Critique |
| **Impact** | Critique |

Cheana Stealer est un logiciel malveillant diffusé par un site de phishing, ciblant les utilisateurs qui téléchargent des applications gratuites de réseau privé virtuel (VPN) sur Windows, Linux et macOS.

Les acteurs malveillants ont créé un site de phishing qui se fait passer pour un service VPN légitime et propose des instructions d'installation détaillées pour Windows, Linux et macOS. L'infection initiale se produit lorsque les utilisateurs suivent les instructions du site de phishing, qui impliquent de copier et de coller dans leur système des commandes spécifiques à chaque plateforme. Chaque ensemble de commandes adaptées à Windows, macOS et Linux garantit que le code malveillant est exécuté correctement sur le système d'exploitation concerné.

Le Cheana Stealer est programmé pour extraire une large gamme de données, y compris les mots de passe stockés dans les navigateurs, les cookies, les clés SSH, ainsi que les données de connexion. De plus, ce malware s'intéresse particulièrement aux extensions de navigateur liées à la crypto-monnaie et aux portefeuilles cryptographiques autonomes.

Les victimes peuvent subir des pertes financières significatives, une exfiltration de données sensibles, et une compromission complète de leurs appareils. Les données volées sont ensuite revendues sur le dark web.

## Indicateurs de compromission (IOCs):

URLs :

- 70f08497d7a9e6a8e5f2dd3683a20563d20668e1c78df636ff1e36a014c9d493
- acf807def82c4b56752a9fa9b081dbb37ba9cc9f6e1c522568ff502b6b49b6db
- 48964c11fcbefd6508164239866c94b55ca2798e9745671c37447ad0a6f3e1c4
- d3ece8616d0dd8244666af574cc2475d947180ed240f49b1a6e61443a896f65d
- 3ef838502663c167f5c502585e810ffae3e03152b3f82544b813389c19a33dce
- ac4aeab3952f6ca960cbd48c3123f09a68f50818f9bdf35c9d811570893fa102
- 6a68e95ae67aa8c61bd74ecf5f57f98fbdc0bbe0489ae71b7c8732edf49ac3a9
- c044b1a36249f6fe7219e6c48270d9927bf359110ff3583129dcbdff809f2d2d
- ba8058b704a55e50c24383a765fd74b38d7dbbf8546c4f179266c265403174b8

Domains :

- warpvpn[.]net
- hxxps://ganache[.]live

## Annexe

- https://cyble.com/blog/new-cheana-stealer-targets-vpn-user/?__hstc=202258190.a25d22137b745cd14ecf20f735f0e4b9.1724825568337.1724825568337.1724825568337.1&__hssc=202258190.2.1724825568338&__hsfp=797865114