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	Backdoor "ChillyHell" ciblant les environnements MacOS
Numéro de Référence	56791109/25
Date de Publication	11 Septembre 2025
Risque	Critique
Impact	Critique

ChillyHell est un backdoor modulaire ciblant macOS, diffusé via des applications malicieuses. Il exploite des mécanismes avancés de persistance tels que « LaunchAgents et LaunchDaemons » intégrés au système d'exploitation qui permettent d'exécuter automatiquement des programmes ou des scripts, souvent utilisés pour la gestion des services en arrière-plan, mais aussi abusés par les malwares pour assurer leur persistance. Les attaquants créent des fichiers de configuration « .plist » pointant vers leur binaire malveillant. Ainsi, à chaque démarrage de l'ordinateur ou connexion d'utilisateur, le malware est relancé automatiquement, pour communique avec des serveurs de commande et contrôle (C2) et garantir une persistance discrète. Une fois installé, il permet l'exécution de commandes arbitraires, le vol d'identifiants, des attaques de type force brute et l'installation de modules additionnels, ouvrant ainsi la voie à une compromission complète de l'environnement macOS.

Pour se protéger, il est recommandé de vérifier la présence des fichiers et chemins suspects listés dans les IoC, de surveiller toute communication réseau sortante vers les adresses IP C2 connues, de supprimer immédiatement les binaires infectés et de réinstaller uniquement depuis des sources fiables. Il est également conseillé d'appliquer des politiques EDR/antivirus renforcées et de mettre en place une supervision continue des environnements macOS pour détecter rapidement toute activité anormale.

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

La DGSSI 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 :

- eDrawMaxBeta2023.zip : e2037eac2a8ec617a76c15067856580c8b926b37
- eDrawMaxBeta2023.app/Contents/MacOS/eDrawMaxBeta: c52e03b9a9625023a255f051f179143c4c5e5636
- chrome_render.zip : 785eb7488b4b077d31b05a9405c8025e38c1626f
- chrome_render binaire : 87dcb891aa324dcb0f4f406deebb1098b8838b96
- applet.zip (Mandiant) : d83216abbcb331aa1bfa12a69996ca12cc5c6289
- applet (Mach-O binaire) : 6a144aa70128ddb6be28b39f0c1c3c57d3bf2438

Ip :

- 93.88.75.252
- 148.72.172.53

Path :

- ~/Library/LaunchAgents/com.apple.qtop.plist
- ~/Library/com.apple.qtop/qtop
- /Library/LaunchDaemons/com.apple.qtop.plist
- /usr/local/bin/qtop
- /tmp/kworker

Annexe

- https://www.jamf.com/blog/chillyhell-a-modular-macos-backdoor/?nav=1