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	MidgeDropper Malware
Numéro de Référence	43932109/23
Date de Publication	21 Septembre 2023
Risque	Critique
Impact	Critique

MidgeDropper est un logiciel malveillant sophistiqué qui utilise une chaîne d'infection complexe, y compris l'obfuscation du code et le téléchargement latéral, pour échapper à la détection et déployer d'autres logiciels malveillants.

L'attaque commence généralement par un fichier d'archive malveillant, qui peut être déguisé en document légitime ou en un autre type de fichier. Lorsque l'utilisateur ouvre l'archive, le logiciel malveillant est exécuté et commence son processus d'infection. La variante Midge-Dropper utilise diverses techniques pour échapper à la détection, notamment :

- Obfuscation du code : Le code du logiciel malveillant est obscurci afin de le rendre difficile à analyser et à comprendre pour les chercheurs en sécurité.
- Sideloading : Le logiciel malveillant transfère d'autres logiciels malveillants sur l'appareil de la victime sans passer par le processus d'installation habituel. Il est donc difficile pour les logiciels de sécurité de les détecter et de les bloquer.

Une fois MidgeDropper infecte un appareil, il peut être utilisé pour déployer toute une série d'autres logiciels malveillants, tels que des ransomwares, des chevaux de Troie et des logi-ciels espions. Ces logiciels malveillants peuvent être utilisés pour voler des données, crypter des fichiers ou même prendre le contrôle de l'appareil.

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

Recommandations :

- Bloquer les IOC attachés au réseau et utiliser les dernières données de renseignement sur les menaces pour rester au courant des TTP et des IOC utilisés par les acteurs de la menace.
- Installer les mises à jour des systèmes d'exploitation, des logiciels, des pilotes, des plugins et des microprogrammes.
- Déployer des solutions de protection des machines des utilisateurs finaux de l'organisation.
- Former les employés à l'importance d'une bonne hygiène en matière de cybersécurité. (Eviter d'ouvrir les pièces jointes suspects dans les courriels, utiliser des mots de passe forts, ...)

Indicateurs de compromission (IOCs):

Hash :

- 2dcf00b0f6c41c2c60561ca92893a0a9bf060e1d46af426de022d0c5d23d8704
- 30417ca261eefe40f7c44ff956f9940b766ae9a0c574cd1c06a4b545e46f692e
- 527afa0c415af005594acaac1093a1ea79e3639fa5563602497eabbae7438130
- 59334a6e2c5faabe3a1baf5347ba01f2419d731fcbb7ab1b021185c059c8fa6f
- b3e0388f215ac127b647cd7d3f186f2f666dc0535d66797b6e1adb74f828254e
- c22cc7111191e5a1a2010f4bc3127058bff41ecba8d753378feabee37d5b43bb
- f26f5a52bddda5eb3245161b784b58635ffa2381818816e50b8bae9680ff88eb
- f43cca8d2e996ee78edf8d9e64e05f35e94a730fbe51e9feecc5e364280d8534
- fc40e782731b8d3b9ec5e5cf8a9d8b8126dc05028ca58ec52db155b3dadc5fc6

URL:

- http://185.225.68.37/jay/nl/
- http://185.225.68.37/jay/nl/35g3498734gkb.dat
- http://185.225.68.37/jay/nl/35g3498734gkb.xn--dat-9o0a

- http://185.225.68.37/jay/nl/VCRUNTIME140_1.dll
- http://185.225.68.37/jay/nl/seAgnt.exe

Référence :

Fortinet «MidgeDropper Variant » **:**

- https://www.fortinet.com/blog/threat-research/new-midgedropper-variant