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

BULLETIN DE SECURITE

Titre	Utilisation des documents "PowerPoint" pour la distribution des Malwares via des campagnes de phishing
Numéro de Référence	34472601/22
Date de Publication	26 Janvier 2022
Risque	Important
Impact	Important

Plusieurs campagnes de phishing utilisent des documents "PowerPoint" malveillants pour distribuer différents types de malwares, notamment des trojans d'accès à distance et de vol d'informations. Les cybers-attaquants utilisent des fichiers "PowerPoint" combinés à des services cloud légitimes qui hébergent les payloads des malwares.

Les malwares les plus répondus utilisant cette technique sont "Warzone" (alias AveMaria) et "AgentTesla", deux puissants RAT qui peuvent voler les mots de passe des navigateurs, enregistrer les frappes du clavier, voler le contenu du presse-papiers, etc.

Les utilisateurs doivent être sensibilisés pour avoir plus de vigilance vis-à-vis des documents "PowerPoint" et n'ouvrir que ceux provenant des sources légitimes.

Ci-dessous certains indices de compromissions (IOC) relatifs aux malwares susmentionnés:

Hashes :

- be453dcadd408fae5227f8b58f539f3f68aad081c9bf4f2c3dc0ff35c601ef5e
- eff2feb50bebb797db7d881a44c549234315a84c861d2bb675899f7165db3ce7
- 4674f942f3b1841744d81c6bb740879540a6514f57c54ecc443a2ea250a0c459
- 7a0da7d7bc7e60548bbac036b675c2a8df0869d37bdaf337d16dc93d5bd39da3
- 37bbddb8e25859349f18c619f863f151660d1ed688c05e0f4a06da942fa154ec
- 271028308b8a45535b865b0818f39c098e78506a36de57ffee0087c810a65cdb
- 38207b0af1ad9d0ce047ae8d3b3535921106609c1b4d640a83d1592bb06cf1e2
- 8915469cb570b038f78d1fcf97d4f132df89e08086a07231cd43da3c443a8016

Registry Keys:

- HKCU\Microsoft\Windows\CurrentVersion\cjjhutyyaggw
- HKCU\Microsoft\Windows\CurrentVersion\pilodkis

URLs:

- hxxps://hahahahhasd@j[.]mp/kdwocqwqwqerheurfje

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

- hxxps://download1507.mediafire[.]com/af0tbthsvewg/od8k8i5brx9cpof/19.doc
- hxxps://8db3b91a-ea93-419b-b51b-0a69902759c5.usrfiles[.]com/ugd/8db3b9_e926d447972f4d23b3c2af4abee9467e.txt?dn=rendomtext
- hxxps://8db3b91a-ea93-419b-b51b-0a69902759c5.usrfiles[.]com/ugd/8db3b9_92ec48660f134f3bb502662383ca4ffb.txt?dn=rendomtext
- hxxps://kukadunikkk@kdaoskdokaodkwldld.blogspot[.]com/p/19.html
- hxxp://www.starinxxxgkular.duckdns[.]org/s1/19.txt
- hxxps://raw.githubusercontent[.]com/swagkarna/Bypass-Tamper-Protection/main/NSudo.exe
- hxxps://www.mediafire[.]com/file/qh5j3uy8qo8cpu7/FINAL+MAIN+vbs+-+Copy.vbs/file
- hxxp://103.147.185[.]68/j/p19xw/mawa/48608c2b91739edc3959.php

En cas de détection de l'un des IoCs, veuillez le signaler au maCERT via : **incident@macert.gov.ma**