CYBER DEFENSE AFRICA : ANNONCE DE SÉCURITÉ **Date** : 26/07/2024

Type de Contenu	Description
Titre	***Le groupe de cyberespionnage Muddywater déploie un nouveau Backdoor dans ses récentes campagnes de phishing.***
ID	*202407/AS/10*
Code TLP	*Green*
Niveau de Risque	***Critique***
Application et service affectés	*N/A*
Version / Edition	*N/A*
Plateforme	*N/A*
Mise à jour	*N/A*
Résumé	*Le Backdoor **BugSleep** vient d'être ajouté à la liste des malwares utilisés par le groupe de cyberespionnage MuddyWater dans ses attaques.*
Impacts	- ***Exécution des attaques par phishing ou hameçonnage*** - ***Exécution des attaques d'injection SQL programmées*** - ***Exfiltration des informations sensibles de la base de données*** - ***Violation de données importantes, entraînant la fuite d'informations sensibles*** - ***Chiffrement de données et blocage des systèmes***
Description Détaillée	*Le groupe cyberespionage iranien MuddyWater utilise des emails de phishing envoyés depuis des comptes compromis pour déployer des outils de gestion à distance spécialement son nouveau malware (backdoor) appelé **BugSleep**. Ce groupe utilise des méthodes pour éviter la détection, telles que des techniques d'évasion contre les solutions EDR.* *BugSleep quant à lui est en étant en cours de développement est déployée par le groupe **MuddyWater** dans des campagnes de phishing ciblant plusieurs pays dans le monde. Il permet aux attaquants d'exécuter des commandes à distance et de transférer d'une manière furtive des fichiers entre la machine compromise et le serveur de commande et de contrôle (C&C).* *Le programme de chargement injecte un shellcode qui charge **BugSleep** en mémoire via l'un des processus suivants, selon qu'ils sont déjà en cours d'exécution ou non :* • *msedge.exe* • *opera.exe* • *chrome.exe* • *anydesk.exe* • *Ondedrive.exe* • *powershell.exe*

Recommandations	***Il faut :*** • ***Surveiller et empêcher toutes communication en entrée comme en sortie avec les domaines y compris les URL et les adresses IP cités dans les IOCs.*** • ***Sensibiliser les utilisateurs sur les dangers des campagnes de phishing ou d'hameçonnage*** • ***Effectuer toujours des mises des systèmes uniquement depuis les sources officielles des fournisseurs.***
Indicateurs de Compromission	***Domaines :*** *kinneretacil.egnyte[.]com* *salary.egnyte[.]com* *gcare.egnyte[.]com* *rimonnet.egnyte[.]com* *alltrans.egnyte[.]com* *megolan.egnyte[.]com* *bgu.egnyte[.]com* *fbcsoft.egnyte[.]com* *cnsmportal.egnyte[.]com* *alkan.egnyte[.]com* *getter.egnyte[.]com* *ksa1.egnyte[.]com* *filecloud.egnyte[.]com* *nour.egnyte[.]com* *airpazfly.egnyte[.]com* *cairoairport.egnyte[.]com* *silbermintz1.egnyte[.]com* *smartcloudcompany[.]com* *onlinemailerservices[.]com* *smtpcloudapp[.]com* *softwarehosts[.]com* *airpaz.egnyte[.]com* *airpazflys.egnyte[.]com* *fileuploadcloud.egnyte[.]com* *downloadfile.egnyte[.]com* ***URLs :*** *https://shorturl[.]at/NCxJk* *https://shorturl[.]at/bYqUx*

	https://ws.onehub[.]com/files/bbmiio1c *https://ws.onehub[.]com/files/zgov9aqy* ***Adresses IP Malveillantes*** ***Serveurs C&C :*** *146.19.143[.]14* *91.235.234[.]202* *85.239.61[.]97* ***Autres adresses IP :*** *95.164.32[.]69* *5.252.23[.]52* *194.4.50[.]133* *193.109.120[.]59* ***Adresses IP utilisées pour l'envoi d'emails :*** *89.221.225[.]81* *45.150.108[.]198* *200.200.200[.]248* *169.150.227[.]230* *169.150.227[.]205* *185.248.85[.]20* *141.98.252[.]143* *31.171.154[.]54* *146.70.172[.]227* *198.54.131[.]36*
Liens pour plus de détails	*https://blog.checkpoint.com/research/muddywater-threat-group-deploys-new-bugsleep-backdoor/*