CYBER DEFENSE AFRICA : ANNONCE DE SÉCURITÉ **Date** : 08/08/2023

Type de Contenu	**Description**
Titre	*Le groupe hacktiviste Anonymous Sudan à l'origine d'attaques DDOS contre des sites gouvernementaux africains.*
ID	*202308/AS/13*
Code TLP	***Green***
Niveau de risque	*Critique*
Pays victimes	- Suède - Inde - Israël - Etats unis - Danemark - Kenya
Tactiques, Techniques et Procédures (TTPs)	*Le groupe a trois vecteurs d'attaque principaux, observés jusqu'à présent. Ces vecteurs d'attaques sont :* - ***Attaques par défacement*** *: (T1491.001 : défacement interne, T1491.002 : défacement externe)* - ***Attaques DDoS*** *(Déni de service en réseau (T1498.001 : Injection directe du flux dans le réseau, T1498.002 : Réflexion Amplification)* - ***Compromission de comptes*** *(T1586.002 : Comptes de courrier électronique)*
Indicateurs de compromission	- *101.167.152.76,* - *101.167.152.90,* - *109.235.139.13,* - *213.61.253.152,* - *213.61.253.250,* - *213.61.254.11,* - *213.61.254.36,* - *217.110.80.14*
Résumé	Le groupe Anonymous Sudan fait son apparition au début de l'année 2023. Il utilise l'arabe comme langue de communication et se présente comme un groupe d'hacktivistes qui se venge des États-Unis et des pays alliés pour les actes répréhensibles qu'ils ont commis au Soudan et dans d'autres parties du monde musulman. Certains experts en sécurité pensent qu'il s'agirait d'un groupe de pirates informatiques russes agissant sous ce couvert, car il prône souvent les intérêts mutuels et les liens entre la Russie et les nations islamiques.
Impacts	***- L'infrastructure endommagée peut provoquer l'effondrement des services fournis par le site web.***

	- Les sites web deviennent vulnérables à d'autres attaques. ***- Les utilisateurs n'ont plus accès aux sites web et aux ressources impactées.***
Description Détaillée	Anonymous Sudan utilise un réseau d'ordinateurs contrôlés à distance (botnet) pour inonder de trafic un site web ciblé, le rendant inaccessible aux utilisateurs légitimes. Les attaques se caractérisent par des DDoS (Distributed Denial of Service) combinées à des vagues alternées d'inondations UDP et SYN. Les attaques proviennent de dizaines de milliers d'adresses IP unique, avec un trafic UDP atteignant jusqu'à 600 Gbps et de grands volumes de requêtes HTTPS atteignant plusieurs millions de RPS. Le groupe exploite l'infrastructure des serveurs du cloud public pour générer du trafic et des flux d'attaques tout en exploitant des infrastructures de proxy libres et ouvertes pour dissimuler et rendre aléatoire la source des attaques. Le groupe a tendance à utiliser des botnets DDoS de la couche applicative, SkyNet / Godzilla, bien qu'ils aient également des capacités de couche 4. Les attaques DDoS de la couche application sont utilisées pour cibler les applications et les réseaux orientés vers l'utilisateur. Ces attaques ciblent les protocoles de la couche application dans le but de perturber les services et peuvent ne pas être détectées par les systèmes de défense traditionnels.
Solutions	- Configurer les pares-feux et les routeurs pour filtrer et bloquer le trafic. - Utiliser les réseaux de diffusion de contenu (CDN) pour distribuer le trafic. - Mettre en œuvre des technologies et des algorithmes de détection des bots - pour identifier les requêtes web à grande échelle provenant de réseaux de bots utilisés par des acteurs pour mener des attaques DDOS. - Utiliser un WAF (Web Application Firewall) bien configuré et mis à jour. - Utiliser un vérificateur de réputation pour évaluer la réputation avant d'autoriser le trafic à travers le pare-feu. - Supprimer le trafic externe provenant de pays dont vous ne vous attendez pas à recevoir du trafic. - Prévoyez de vous procurer un fournisseur d'accès à Internet de secours au cas où vous n'indisposer pas pour remplacer le fournisseur de services principal s'il est compromis. - Penser à mettre en place une solution anti-DDoS telle que **Cloudflare** ou installer le plugin **hide my wp ghost** de WordPress sur les sites développés en WordPress. - Déployer des répartiteurs de charge pour distribuer le trafic. - Mettre en place des mécanismes de limitation de débit. - Analyser régulièrement votre site web pour détecter d'éventuelles failles de sécurité et de s'assurer que toutes les mises à jour

	nécessaires sont installées pour prévenir d'éventuelles attaques.
Liens pour plus de détails	• *https://www.cpomagazine.com/cyber-security/anonymous-sudan-offering-30-million-microsoft-accounts-for-sale-redmond-denies-data-breach/* • *https://attack.mitre.org/techniques/T1491/001/* • *https://attack.mitre.org/techniques/T1498/001/* • *https://attack.mitre.org/techniques/T1586/002/* • *https://www.radware.com/cyberpedia/ddos-attacks/anonymous-sudan/*