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	Campagne de spear-phishing attribuée au groupe « APT29 »
Numéro de Référence	50510411/24
Date de Publication	04 Novembre 2024
Risque	Critique
Impact	Critique

Une campagne de spear-phishing attribuée au groupe « APT29 » a récemment été signalée, ciblant des entités sensibles à savoir (des organismes gouvernementaux, armées et des agences de sécurité) dans le monde entier.

Le groupe exploite des fichiers de configuration du protocole (RDP) signés numériquement pour paraître légitimes dans des e-mails de phishing qui se font passer pour des communications provenant d'entités de confiance telles qu'Amazon et Microsoft.

Les techniques couramment utilisées incluent le phishing (T1566), l'exécution par l'utilisateur (T1204) et l'accès à distance via RDP (T1219), visant principalement le vol d'identifiants pour obtenir un accès privilégié aux systèmes des victimes. Parmi les incidents notables, une campagne massive de spear-phishing détectée par Microsoft a utilisé des fichiers RDP malveillants pour se connecter à des serveurs contrôlés par les attaquants pour exfiltrer des données.

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 ce malware.

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

Mesures préventives :

- **Restreindre les connexions RDP sortantes :** Il est fortement conseillé aux organisations d'interdire ou de limiter considérablement les connexions RDP sortantes vers des réseaux externes ou publics. Cette mesure est cruciale pour minimiser l'exposition aux menaces cybernétiques potentielles.

- **Bloquer les fichiers RDP sur les plateformes de communication :** Les organisations doivent interdire la transmission de fichiers RDP via les clients de messagerie et les services de messagerie web. Cette étape aide à éviter l'exécution accidentelle de configurations RDP malveillantes.

- E**mpêcher l'exécution des fichiers RDP :** Mettre en œuvre des contrôles pour bloquer l'exécution de fichiers RDP par les utilisateurs. Cette précaution est essentielle pour réduire le risque d'exploitation.

- **Activer l'authentification multi-facteurs (MFA) :** L'authentification multi-facteurs doit être activée partout où cela est possible pour ajouter une couche de sécurité pour les accès à distance.

- **Adopter des méthodes d'authentification résistantes au phishing :** Les organisations sont encouragées à déployer des solutions d'authentification résistantes au phishing, telles que les jetons FIDO. Il est important d'éviter la MFA par SMS, car elle peut être vulnérable aux attaques de type SIM-jacking.

- **Sensibilisation des utilisateurs** sur les menaces liées à l'ingénierie sociale et les attaques de phishing.

Indicateurs de compromission (IOCs):

IP addresses:

- 185.99.2.195
- 91.201.65.164
- 185.246.189.12
- 79.124.60.173
- 5.206.227.176
- 91.149.243.82
- 212.224.86.97
- 169.239.129.123

- 194.68.26.114
- 51.195.49.197
- 154.216.20.126
- 82.221.139.96
- 3.26.26.250

Référence:

- https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/
- https://aws.amazon.com/fr/blogs/security/amazon-identified-internet-domains-abused-by-apt29/
- https://atwork.safeonweb.be/recent-news-tips-and-warning/warning-government-themed-phishing-rdp-attachments