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	APT73 (Bashe)
Numéro de Référence	62272403/26
Date de Publication	24 Mars 2026
Risque	Critique
Impact	Critique

Le groupe « Bashe », également connu sous les noms « APT73 », est un acteur cybercriminel apparu publiquement en 2024 et associé à des opérations de ransomware à l'échelle mondiale. APT73 a ciblé un large éventail d'organisations, notamment des institutions financières, des entités gouvernementales, des établissements de santé et des entreprises industrielles, ce qui démontre la capacité du groupe à s'attaquer aussi bien à des infrastructures critiques qu'à des organisations publiques.

Leur mode opératoire repose sur des attaques de ransomware associées à une stratégie de double extorsion. Les attaquants infiltrent d'abord les réseaux en exploitant des vulnérabilités exposées, en utilisant le phishing ou en compromettant des identifiants. Une fois l'accès obtenu, ils procèdent à l'exfiltration de données sensibles avant de chiffrer les systèmes des victimes, mettant ainsi en œuvre la technique « MITRE ATT&CK T1486 (Data Encrypted for Impact) ». Les victimes sont alors menacées de publication de leurs données sur des sites de fuite dédiés si elles refusent de payer la rançon.

Le groupe utilise une infrastructure variée, souvent composée de domaines créés spécifiquement pour des campagnes malveillantes, ce qui complique la détection et la corrélation des incidents.

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

Le maCERT recommande d'intégrer les recommandations suivantes et d'alerter le maCERT en cas de détection d'une activité relative à ce groupe.

Recommandations:

1. **Réduire les risques d'accès initial :**

APT73 exploite principalement le phishing et les vulnérabilités des services exposés.

Mesures recommandées :

- Mettre en place une gestion rigoureuse des correctifs pour toutes les applications exposées (web, VPN, messagerie).
- Restreindre l'exposition des services critiques (RDP, SMB) à Internet.

2. **Renforcer la sécurité des identités et des accès**

Les attaques de Bashe reposent fréquemment sur des identifiants compromis.

À mettre en œuvre :

- Activer la MFA sur tous les accès sensibles (VPN, comptes administrateurs, messagerie).
- Appliquer des politiques de mots de passe robustes et uniques.
- Surveiller les fuites d'identifiants sur le dark web afin de détecter une compromission en amont.

3. **Limiter la propagation dans le réseau (lateral movement)**

Une fois à l'intérieur, le groupe utilise SMB et des outils natifs pour se déplacer latéralement.

Mesures clés :

- Mettre en place une segmentation réseau entre les environnements utilisateurs, serveurs et systèmes critiques.
- Appliquer le principe du moindre privilège sur tous les comptes.
- Désactiver ou restreindre les partages administratifs inutiles.

4. **Détecter et bloquer l'exécution de ransomware**

APT73 utilise des scripts PowerShell et des outils légitimes pour éviter la détection.

Contremesures :

- Déployer des solutions EDR/XDR capables de détecter les comportements suspects (exécution de scripts, création de tâches planifiées).
- Mettre en place une liste blanche applicative pour empêcher l'exécution de binaires non autorisés.
- Surveiller les modifications de registre et la désactivation des outils de sécurité.

5. **Protéger les données contre la double extorsion**

Le groupe exfiltre les données avant de chiffrer les systèmes.

Mesures recommandées :

- Surveiller les transferts de données anormaux vers Internet ou vers des services cloud.

6. Assurer la résilience face au chiffrement des systèmes

APT73 applique la technique « T1486 – Data Encrypted for Impact », rendant les systèmes indisponibles.

Bonnes pratiques :

- Maintenir des sauvegardes hors ligne (offline) et isolées du réseau.
- Tester régulièrement les procédures de restauration.
- Documenter et maintenir un plan de réponse aux incidents ransomware.

7. Améliorer la détection et la réponse aux incidents

Une détection précoce permet de bloquer l'attaque avant le chiffrement.

Actions recommandées :

- Centraliser les journaux dans un SIEM pour corréler les événements (authentification, PowerShell, SMB).
- Mettre en place des alertes sur :
    - créations de tâches planifiées
    - exécutions PowerShell encodées
    - accès SMB anormaux
- Conserver des logs suffisants pour les analyses forensiques post-incident.