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	Exploitation massive de la vulnérabilité CVE-2023-7102 affectant Barracuda Email Security Gateway
Numéro de Référence	45352812/23
Date de Publication	28 Décembre 2023
Risque	Critique
Impact	Critique

Barracuda confirme l'observation des deux logiciels malveillants, SEASPY et SALTWATER, exploitant la faille critique « CVE-2023-7102 » au cours des attaques récentes, pour se faire passer pour des modules et des services Barracuda ESG légitimes.

Il est à noter que « SEASPY » est un backdoor persistant x64 qui se fait passer pour un service légitime de Barracuda Networks et se fait passer pour un filtre PCAP, surveillant spécifiquement le trafic sur le port 25. SEASPY prend également en charge une fonctionnalité de backdoor activé par un "magic packet". En outre, « SALTWATER » est un module contenant des logiciels malveillants pour le démon SMTP (Simple Mail Transfer Protocol) de Barracuda (bsmtpd) qui prend en charge de nombreuses fonctionnalités telles que le téléchargement de fichiers arbitraires, l'exécution de commandes, ainsi que le proxy et le tunnelage du trafic malveillant afin d'éviter la détection.

Indicateurs de compromission (IOCs):

Hash :

- 2b172fe3329260611a9022e71acdebca (MD5),
- 803cb5a7de1fe0067a9eeb220dfc24ca

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

- 56f3f571a986180e146b6cf387855bdd (SHA256)
- e7842edc7868c8c5cf0480dd98bcfe76 (MD5),
- 952c5f45d203d8f1a7532e5b59af8e330
- 6b5c1c53a30624b6733e0176d8d1acd (SHA256)
- e7842edc7868c8c5cf0480dd98bcfe76 (MD5),
- 952c5f45d203d8f1a7532e5b59af8e330
- 6b5c1c53a30624b6733e0176d8d1acd (SHA256)
- 7b83e4bd880bb9d7904e8f553c2736e3 (MD5),
- 118fad9e1f03b8b1abe00529c61dc3edf
- da043b787c9084180d83535b4d177b7 (SHA256)
- d493aab1319f10c633f6d223da232a27 (MD5),
- 34494ecb02a1cccadda1c7693c45666e1
- fe3928cc83576f8f07380801b07d8ba (SHA256)

IP Addresses:

- 23.224.99[.]242
- 23.224.99[.]243
- 23.224.99[.]244
- 23.224.99[.]245
- 23.224.99[.]246
- 23.225.35[.]234
- 23.225.35[.]235
- 23.225.35[.]236
- 23.225.35[.]237
- 23.225.35[.]238
- 107.148.41[.]146

Référence :

Barracuda Email Security Gateway Appliance (ESG) Vulnerability**:**

- https://www.barracuda.com/company/legal/esg-vulnerability

Bulletin de sécurité maCERT « Vulnérabilité critique dans Barracuda Email Security Gateway » du 28 Décembre 2023**:**

- https://www.dgssi.gov.ma/fr/bulletins/vulnerabilite-critique-dans-barracuda-email-security-gateway-0