**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** | L'acteur ShroudedSnooper cible les entreprises de télécommunications du Moyen-Orient |
| **Numéro de Référence** | 43882009/23 |
| **Date de Publication** | 20 Septembre 2023 |
| **Risque** | Critique |
| **Impact** | Critique |

Un nouvel acteur de la menace appelé « ShroudedSnooper » a ciblé des entreprises de télé-communications au Moyen-Orient avec de nouveaux implants. L'attaque est menée à l'aide d'une porte dérobée appelée « HTTPSnoop », qui exploite le noyau HTTP de Windows. L'attaque est très furtive et peut compromettre la sécurité des organisations ciblées sans être détectée.

Les entreprises de télécommunications contrôlent généralement un grand nombre d'infras-tructures critiques, ce qui en fait des cibles prioritaires pour les adversaires qui cherchent à avoir un impact significatif. Les codes malicieux utilisés sont conçus pour voler des données sensibles, notamment des enregistrements d'appels, des messages texte et l'historique de na-vigation.

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 cette menace.

**Recommandations :**

- Mettre en œuvre des solutions de sécurité réseau capables de détecter et de bloquer le trafic réseau malveillant, y compris le trafic qui semble bénin.

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

- Surveiller le trafic réseau pour détecter tout signe d'activité inhabituelle ou d'accès non autorisé, y compris les requêtes ou réponses HTTP inattendues.
- Effectuer régulièrement des audits de sécurité et des tests de pénétration afin d'identifier et de corriger les vulnérabilités ou les faiblesses des systèmes déployés.
- Former les employés à l'importance d'une bonne hygiène en matière de cybersécurité. (Eviter d'ouvrir les pièces jointes suspects dans les courriels, utiliser des mots de passe forts, ...)
- Mettre en place une segmentation du réseau et des contrôles d'accès pour limiter l'impact de toute violation ou compromission potentielle.
- Mettre à jour régulièrement les systèmes d'exploitation et les applications afin de remédier à toute vulnérabilité connue susceptible d'être exploitée par des logiciels malveillants.

## Indicateurs de compromission (IOCs):

Hash :

- 3ceb959554450c4ed97bc7c7fbe1d84815a8a3d5be07da9e8d9bb2e705caf9eb
- 9113b447722ccfcc7b6d6811c3a4f9434c6537697d0bc1cb16966bf8bfbb47c1
- b133e715a391d653d2c736c95ac8a58cfd37362a77bec4bcce363e61398ffd2b
- b8d323a348aac4e101a3dd0639b2b03d17c2d14f2eba15a70ea0b3e5fb4811a9
- c785a3da9a7acca0bc8bcc1de92dfd6647d0bc2f897a1a747b595f89650378e8
- dfa96bee7ba6bf98a9594b568bc8c02012081c8822a5f52d62dd7fac0b0c6974
- 024b6e2e1d8cabb07215686e005e302c5e16e442902225daffe8f1e3382d02d1
- 29740ff47e77833032744bbbef669755d864da0e1c2a834b903adcb914d6e8a6
- 92463ea41e384f462226e473c40f6011d9f9463a05b441782596a2e6d760fe42
- 2db2fe6e7b7482f14d5d44446353a277f80afb4905493443a93cc48c1ef120ef
- c0fb29c35a026be5839f10f5a1d889b70107cc836fa894091bf721135f3c6e13
- b297496f7723c21162e2598f6d914f148c55409197f26a1fe6936f86d566d50d
- e1a272780aa760870a793bde01697ed5f425bbe7f862e85dc06091317f573394
- 1075c837d0d6b3195c8a2aa2d70419c22ff98e96ebb17ec6e1d1251a5c415db1
- 99ca71460b7cb4aabde41fed37e647042cfc53bc8dff91aa0a2a28b96c5d2089
- e6220dcfa3ebaa19c2ef65ca79ac48a9b2a212e142f37e465adac34c112a8a52

- e559e603702ed249b5c6d057d71be08a1bdba90a19aceaee15d410985c704dde
- 7a826c7755c173d041f48a08deecc5966082ff274f854174c96cee8c4b7d9d08
- 3a1fa39b47697402df3eaa56b0e765addeb83f244aeb80ee0bcd434ae98ba5c3
- 2d4adb8e894b22d6c60c3877995ba5e9845ec6005fc95382c395396eb84b1e73
- c5b4542d61af74cf7454d7f1c8d96218d709de38f94ccfa7c16b15f726dc08c0
- 04cf425e57e7d511f03189749c8c0a95483eeeb4c423e9ee1a6a766d2fe0094c
- 3875ed58c0d42e05c83843b32ed33d6ba5e94e18ffe8fb1bf34fd7dedf3f82a7
- 7495c1ea421063845eb8f4599a1c17c105f700ca0671ca874c5aa5aef3764c1c
- 1146b1f38e420936b7c5f6b22212f3aa93515f3738c861f499ed1047865549cb
- 9117bd328e37be121fb497596a2d0619a0eaca44752a1854523b8af46a5b0ceb
- e1ad173e49eee1194f2a55afa681cef7c3b8f6c26572f474dec7a42e9f0cdc9d

URL:

- Sysnod[.]duckdns[.]org
- educu[.]xyz[:]9999
- 51[.]178[.]39[.]184
- hxxp[://]51[.]178[.]39[.]184[/]?smd_process_download=1&download_id=90
- hxxp[://]51[.]178[.]39[.]184[/]kit[.]bin
- hxxp[://]51[.]178[.]39[.]184
- http://+:80/Temporary_Listen_Addresses/
- https://+:443/Temporary_Listen_Addresses/
- https://+:443/autodiscover/autodiscovers/
- https://+:444/autodiscover/autodiscovers/
- https://+:444/ews/exchange/
- https://+:443/ews/exchange/
- https://+:443/autodiscover/autodiscover /
- https://+:444/autodiscover/autodiscover /
- https://+:444/ews/exchanges/
- https://+:443/ews/exchanges/
- https://+:444/ews/exchange /
- https://+:443/ews/exchange /
- https://+:443/ews/ /
- https://+:444/ews/ /
- https://+:444/ews/ews/

- https://+:443/ews/ews/
- https://+:443/ews/autodiscovers/
- https://+:444/ews/autodiscovers/
- https://+:443/autodiscover/autodiscoverrs/
- https://+:444/autodiscover/autodiscoverrs/
- https://+:443/autodiscover/course/
- https://+:443/autodiscover/because/
- https://+:443/autodiscover/oppose/
- https://+:443/autodiscover/citizen/
- https://+:443/autodiscover/surprise/
- https://+:443/autodiscover/make/
- https://+:443/autodiscover/tiger/
- https://+:443/autodiscover/verb/
- https://+:443/autodiscover/palace/
- https://+:443/autodiscover/congress/
- https://+:443/autodiscover/expire/
- https://+:443/autodiscover/this/
- https://+:443/ews/often/
- https://+:443/ews/evoke/
- https://+:443/ews/pitch/
- https://+:443/ews/sense/
- https://+:443/ews/six/
- https://+:443/ews/tower/
- https://+:443/ews/feature/
- https://+:443/ews/trip/
- https://+:443/ews/jazz/
- https://+:443/ews/second/
- https://+:443/ews/question/
- https://+:443/ews/powder/
- https://+:444/autodiscover/verb/
- https://+:444/autodiscover/palace/
- https://+:444/autodiscover/congress/
- https://+:444/autodiscover/expire/
- https://+:444/autodiscover/this/
- https://+:444/ews/feature/

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

- https://+:444/ews/trip/
- https://+:444/ews/jazz/
- https://+:444/ews/second/
- https://+:444/ews/question/
- https://+:444/ews/powder/
- https://+:444/ews/test/
- http://*:80/eye/
- http://*:80/delay/
- http://*:80/hill/
- http://*:80/uncle/
- http://*:80/ofasdaqgrumm/
- http://*:80/utkvvxwkwgseowps/
- http://*:80/xewnsfqdcxmhwb/
- http://*:80/vzixmvmvbvrzhoo/
- https://*:443/eye/
- https://*:443/delay/
- https://*:443/hill/
- https://*:443/uncle/
- https://*:443/ofasdaqgrumm/
- https://*:443/utkvvxwkwgseowps/
- https://*:443/xewnsfqdcxmhwb/
- https://*:443/vzixmvmvbvrzhoo/
- http://+:80/test_srv/
- https://+:443/test_srv/

**Référence :**

Trend Micro du 19 Septembre 2023**:**

- https://blog.talosintelligence.com/introducing-shrouded-snooper/