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	" Nightspire " Threat Actor
Numéro de Référence	62593003/26
Date de Publication	30 Mars 2026
Risque	Critique
Impact	Critique

"Nightspire" est un groupe cybercriminel actif spécialisé dans les ransomwares, connu pour recourir à des tactiques de double extorsion, combinant le chiffrement des systèmes compromis et la menace de divulgation publique des données volées afin de contraindre les victimes à payer une rançon. Les observations récentes indiquent une intensification de ses activités, avec une augmentation du nombre de victimes publiées sur ses plateformes d'extorsion, ce qui témoigne d'une montée en puissance de ses campagnes.

"Nightspire" cible des secteurs variés tels que la santé, l'industrie, l'éducation, la logistique et l'administration publique. Pour obtenir un accès initial, le groupe exploite plusieurs vecteurs, notamment des équipements exécutant des versions FortiOS vulnérables, l'utilisation des identifiants compromis pour accéder à des services exposés comme le Remote Desktop Protocol ou les VPN, ainsi que des campagnes de phishing sophistiquées.

Après l'exfiltration et le chiffrement des données, les victimes sont invitées à entrer en contact avec les acteurs malveillants via des adresses « ProtonMail, OnionMail ou des identifiants Telegram ». Les sites de fuite du groupe, accessibles sur le réseau Tor, publient des exemples de données volées et affichent des comptes à rebours de 2 à 3 jours pour faire pression sur les victimes afin qu'elles paient rapidement.

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 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 groupe.

Indicateurs de compromission (IOCs):

Hashs :

- 143c19fd746d41e828e0d94cfdbe506c6c1dfaf05ecfe1d0d347fd30375b2b91
- 9e085cd36c9997b3e44111f63757d0c7592c5b849aaf30d7c9ad0459b09f99e7
- c06f5959cde05e2af57d46214d49e6025582b73498379c162804eba86a2fc368
- 75911dc6fa5d482feb87fb96a1e2733395312459aa9096e2e78f54bb1090a7f4
- dbf0121a87fc39e05f6b4358cd8493c28e57f9e26fc76b97e12a78a457a2f5d7
- c723cd06c2c13ebf781e433fe839bff51b228004622a699e1b9078ce139fa2e7
- c5f526cc62688cf34c49d098dab81e24e4294f832ada57433ef505d5ac6da8f3
- 2c3f8889c9f5d765632ad91b4cc2a852c54845e143dbd2b68359b6f9cdfd8f99
- 22534381980d27fd15bb70f908cc31ac84b08a2e8bb60da3627e11b2b6ebc48d
- 35cefe4bc4a98ad73dda4444c700aac9f749efde8f9de6a643a57a5b605bd4e7
- 32e10dc9fe935d7c835530be214142041b6aa25ee32c62648dea124401137ea5
- d5f9595abb54947a6b0f8a55428ca95e6402d2aeb72cbc109beca457555a99a6
- e275b8a02bf23b565bdaabadb220b39409eddc6b8253eb04e0f092d697e3b53d

Malware Signature:

- rojan-Ransom.”Nightspire”
- Trojan-Ransom.FileCrypter
- Win64/Ransom.Generic.H8oArz0A
- win/malicious
- Ransom/EDR.Decoy.M2470
- Ransom/MDP.Event.M1946
- Ransomware/Win.”Nightspire”.C5769860
- Ransomware/Win.”Nightspire”.C5775165
- Ransom/MDP.Decoy.M1171
- MEGAcmd
- Everything.exe
- WinSCP-6.3.7-Setup.exe
- 7z2408-x64.exe
- 7zG.exe
- 7z.exe

Hostnames :

- WINDOWS-DTX-8GB
- XDRAGON-SERVER1

E-mails :

- night.spire.team@onionmail.org
- night.spire.team@gmail.com
- night.spire.team@proton.me
- “Nightspire”team.receiver@gmail.com
- “Nightspire”team.receiver@onionmail.org
- contact@”Nightspire”-ransomware.com
- support@”Nightspire”-team.onionmail.org

Liens .onion:

- http://a2lyiiaq4n74tlgz4fk3ft4akolapfrzk772dk24iq32cznjsmzpanqd.onion
- http://nspiremkiq44zcxjbgvab4mdedyh2pzj5kzbmvftcugq3mczx3dqogid.onion
- http://nspireyzmvapgiwgtuoznlafqvlyz7ey6himtgn5bdvdcowfyto3yryd.onion

Most used CVE :

- CVE-2024-55591

Persistance registres:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

- IP: 14.139.185.60
- Path d'exécution payload : C:\Windows\Temp
- Extension des fichiers cryptés : .nspire