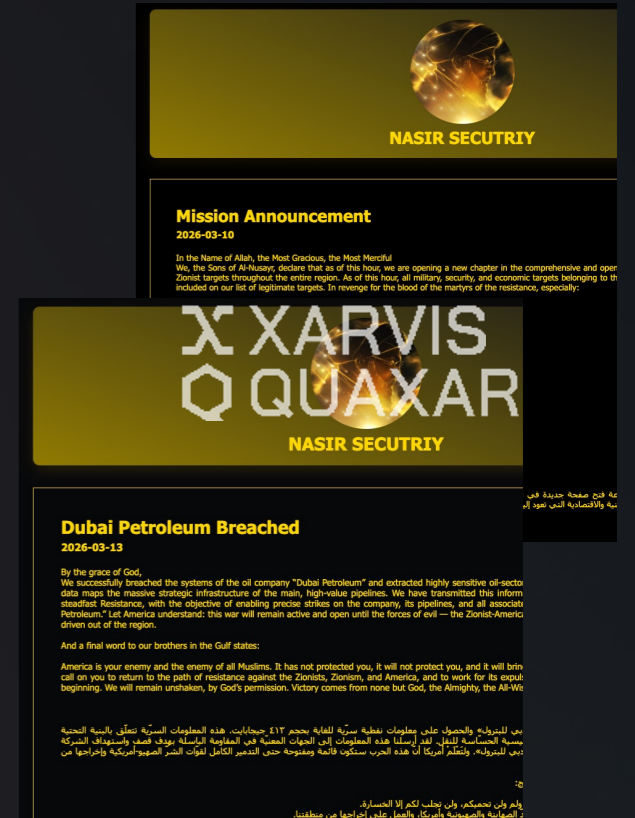


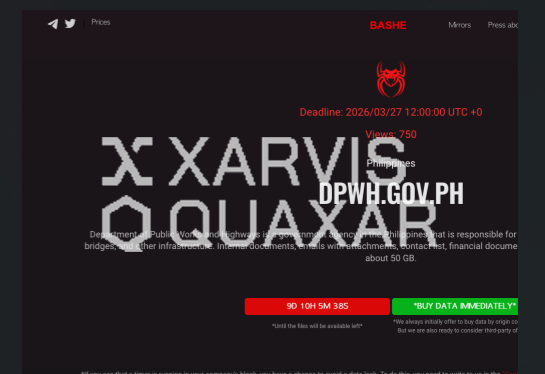
### アラブ首長国連邦の国営石油企業D社でデータ流出、親イラン系ランサムウェアグループ「Nasir」の犯行

- 3月13日、アラブ首長国連邦（UAE）の国営石油企業D社が、ランサムウェアグループ「Nasir」のリークサイトに投稿されていることが確認されました。
  - D社はドバイ政府が運営する国営企業で、ドバイ領海内の全ての海上油田を独占的に管理・運営しています。
- 同ランサムウェアグループは、D社から主要な高価格パイプラインのインフラ地図を含む極秘データ413GBを窃取し、当該データを抵抗組織に渡したと主張しています。
- 同ランサムウェアグループは、攻撃の証拠としてパイプラインや圧縮機的设计図、定格荷重表、インフラの位置を示した地図、パイプラインのダッシュボードなどを含むスクリーンショットとファイルを投稿しました。
  - ランサムウェアグループ「Nasir」は2025年10月に登場したヒズボラ系組織で、3月10日、米国とイスラエル勢力を標的としたサイバー攻撃を予告する声明文を投稿しました。



### フィリピン公共事業道路省、ランサムウェアの「BASHE」の感染を確認

- 3月17日、フィリピン公共事業道路省（Department of Public Works and Highways）の内部データ50GBが、ランサムウェアグループ「BASHE」によって流出の危機に曝されていることが確認されました。
- 同ランサムウェアグループは、窃取したデータに内部文書、添付ファイルを含むメール、連絡先リスト、財務関連の書類、役職員の個人情報などが含まれていると主張し、4月27日を交渉期限として提示しています。
- 同ランサムウェアグループは攻撃の証拠として、役職員の身分証や成績証明書の画像を添付しました。



### イスラエルの情報機関の現職・元高官のメールをハッキングしたと主張する投稿、ダークウェブのフォーラム内で確認

- 3月16日と17日の両日、イスラエルの情報機関モサドの現職や元高官のメールをハッキングしたと主張する投稿が、イランから支援を受けているとされるハクティビストグループ「Handala」のダークウェブフォーラム内で確認されました。
  - [モサド前副長官]16日、同グループのフォーラム内に、モサド前副長官の個人メールをハッキングして約10万件の機密情報を確保したと主張する投稿がアップロードされました。同ハクティビストグループは、窃取の証拠として前副長官のパスポート画像や、2018年から2024年の間に送信されたメールのスクリーンショット画像など8枚を公開しました。
  - [モサド傘下イスラエル国家安全保障研究所（INSS）CFO]17日、同グループのフォーラム内に、モサド傘下の国家安全保障研究所（Institute for National Security Studies）CFOのメールをハッキングし、約5万件の機密情報を窃取したと主張する投稿が確認されました。同グループは、ハッキングの証拠として、CFOのパスポート画像や内部メールのスクリーンショットなど10枚を公開しています。

