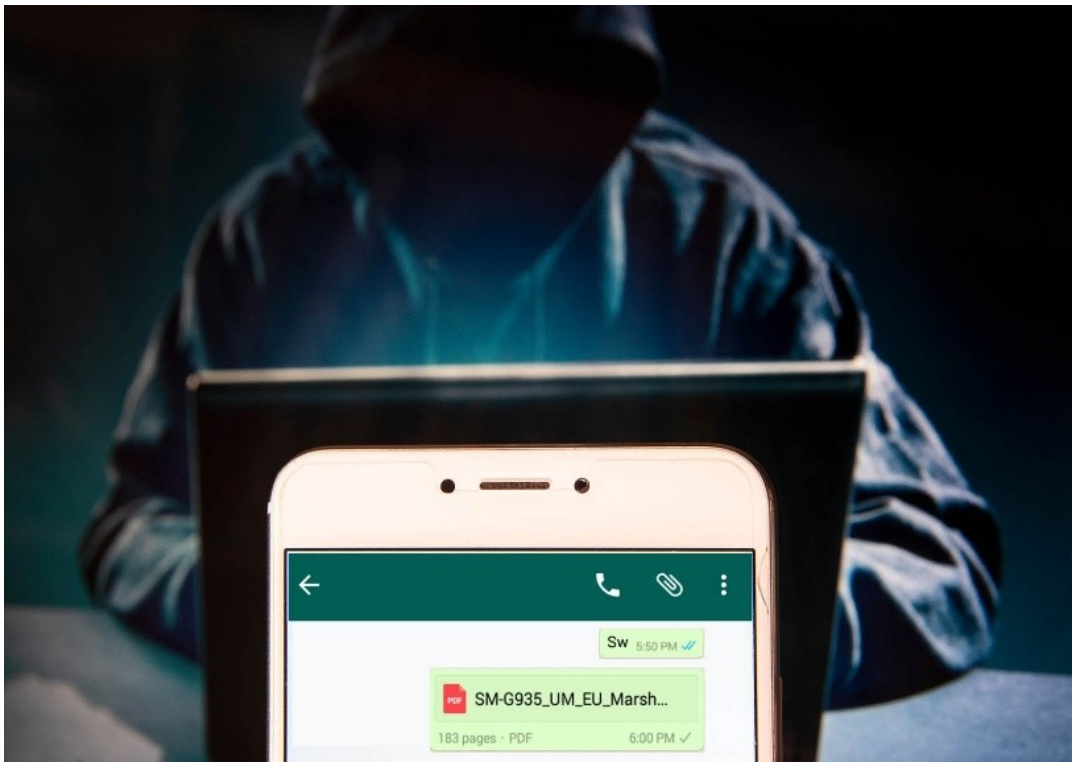
海運業成為網路犯罪分子的作案目標

挪威當局的一項評估顯示，該國的海運及石油與天然氣行業近期已成為多起專門針對美國、歐洲和中東公司的網路攻擊行動的受害者，並告誡相關公司在短期至中期內準備好防禦持續性的攻擊活動。



在近期發佈的一封致海運業的情況通報函中，挪威國家安全局（簡稱“挪威國安局”）通報稱，自 2019 年 6 月以來，針對若干不同行業的網路行動數量有所上升，並指出海運和油氣行業都是這些有針對性攻擊的受害者。

到目前為止，這些行動已經通過社交媒體（主要是 LinkedIn，也有 WhatsApp 和 Facebook Messenger），利用電子郵件和個人消息的社交工程手法，造成了以下後果:

- 在使用者的電腦上安裝惡意軟體;
- 收集有關用戶、其雇主或與他們相關聯的其他使用者的資訊；及
- 使行動進一步擴散。

儘管據報導，這些行動及後續事件的範圍都是全球性的，但挪威國安局表示，“*美國、歐洲和中東的公司一直都是主要攻擊目標*”，而且經查實，威脅實施者還展現出了很強的行動能力和執行能力。

根據目前的情況及查明的風險，挪威國安局建議各公司和組織，在短期至中期內做好防禦惡意網路行動企圖的準備，並且指出，引人注目和不太引人注目的公司都可能受到影響，這意味著各種類型的船舶以及船東的陸上基礎設施都容易受到網路行動的攻擊。挪威海事局在2019 年 8 月 19 日發佈的聲明中進一步強調稱：“*特別是有船在 ISPS / MARSEC 保安等級第二級或更高級的區域內營運的船東，更應該瞭解相關情況。*”

建議

雖然挪威國安局的通報函是針對挪威公司的，但我們建議所有船舶經營人以及負責船上基礎設施的公司持續監控和審查數位化安全情況，並遵循所提出的建議，包括：

- 確保已設置網路分段。網路的管理部分和操作部分之間不應存在任何物理連接。
- 將所有端點處及網路內的活動記錄下來。挪威國安局建議，記錄至少保留六個月。
- 在可能的情況下使用加密通信，在船舶和陸上基礎設施之間也是如此。未經加密的通信內容很容易遭到篡改。
- 根據相關人員所擔任的職務和崗位，設置其對資訊和系統的存取權限。在大多數情況下，設置存取權限能夠限制網路行動產生的後果。

在建議的對策中，強調了開展網路安全意識培訓的重要性。所有“用戶”，包括海員、岸上工作人員和其他相關人員，都應該：

- 注意帶有連結或附件的電子郵件，謹慎做出判斷。
    - 如果對於能否安全打開附件或連結有任何疑問——請評估確定是否有必要打開它。向您的雇主報告與公司有關的可疑電子郵件或消息。
    - 對於 Word、Excel 或 PowerPoint 中提示啟用宏的文檔，請多加小心。
- 在社交媒體中：
    - 報告通過社交媒體收到的可疑消息，特別是當該等消息與您的受雇情況或公司整體相關時。
    - 只跟身份可以驗證的人建立並保持聯繫。
    - 極為謹慎地判斷社交媒體中帶有連結和附件的消息，這是犯罪分子瞄準的新戰場。
    - 預想到每個人都能看到您分享在社交媒體上的、有關工作和私人生活的所有資訊。
    - 未經雇主同意，不發佈與工作有關的資訊。
    - 未經其他人同意，不發佈與他們有關的資訊。
    - 在產品和應用程式中，啟用可用的安全設置。
    - 不要在各類服務系統中重複使用同一密碼。
    - 成為安全 **STAR**：每當您懷疑可能遭到攻擊或不確定該怎麼做時，請 **S**top（停下）–**T**hink（思考）– **A**sk（詢問）– **R**eport（報告）。

船舶經營人還應密切關注其國家安全主管部門提供的任何網路安全建議。舉例而言，建議挪威公司遵循挪威國安局“關於資訊技術和通信技術（ICT）安全的基本原則”以及“有關社交媒體的措施和建議”（兩者都只有挪威語版本）。我們還建議船舶經營人和海員，向其船旗國政府和/或國家安全主管部門報告所有可疑行動和安全性漏洞，因為這樣做能協助其對不斷出現的網路威脅和風險實施監控。

其他指引

希望瞭解網路風險管理方面的其他建議，請參閱本協會於 2019 年 7 月 10 日發佈的“船舶經營人無法忽視網路安全”和 2018 年 12 月 12 日發佈的“船上網路安全程式亟待加強”。在開展安全意識培訓時，我們與挪威船級社聯合制作的防損意識視頻也能有所幫助。

我們也提醒船舶經營人，最晚在 2021 年 1 月 1 日之後根據《ISM 規則》進行首次年度審核時，船舶現有的安全管理體系（定義見《ISM 規則》）中的網路風險必須得到適當處理。有關實施網路風險管理的指南和最佳實踐，請參見國際海事組織通函 MSC-FAL.1/Circ.3 及行業指南《船上網路安全指南》。