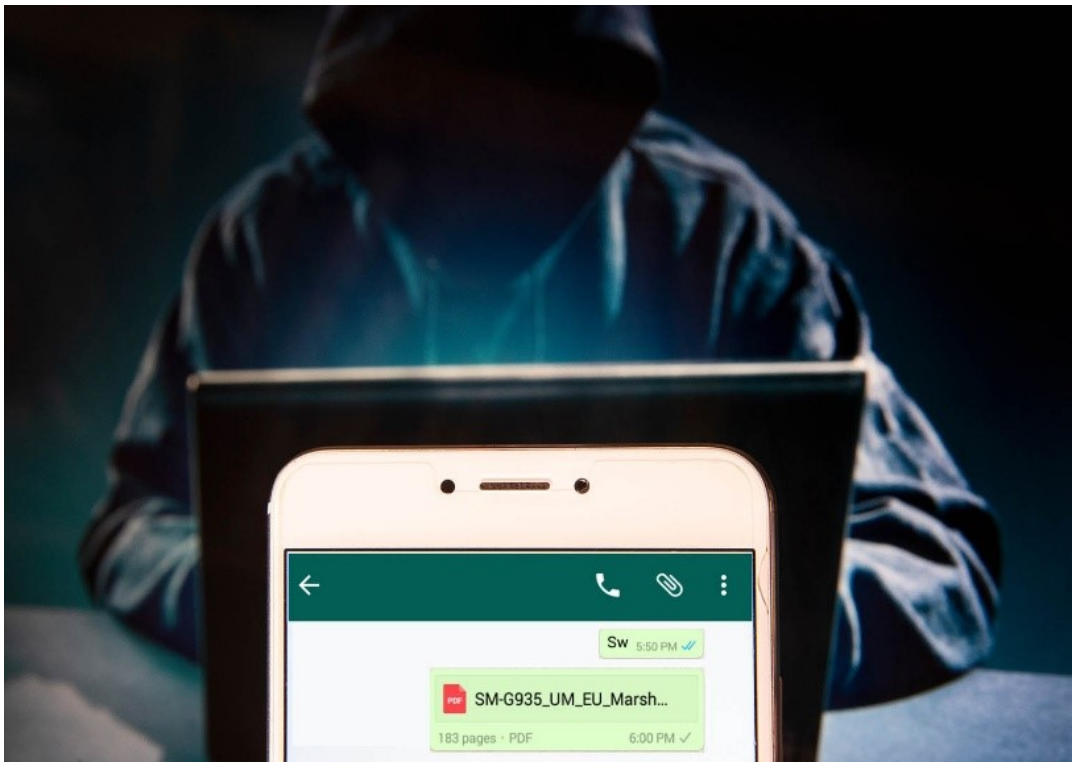
海运业成为网络犯罪分子的作案目标

挪威当局的一项评估显示，该国的海运及石油与天然气行业近期已成为多起专门针对美国、欧洲和中东公司的网络攻击行动的受害者，并告诫相关公司在短期至中期内准备好防御持续性的攻击活动。



在近期发布的一封致海运业的情况通报函中，挪威国家安全局（简称“挪威国安局”）通报称，自 2019 年 6 月以来，针对若干不同行业的网络行动数量有所上升，并指出海运和油气行业都是这些有针对性攻击的受害者。

到目前为止，这些行动已经通过社交媒体（主要是 LinkedIn，也有 WhatsApp 和 Facebook Messenger），利用电子邮件和个人消息的社交工程手法，造成了以下后果：

- 在用户的电脑上安装恶意软件；
- 收集有关用户、其雇主或与他们相关联的其他用户的信息；及
- 使行动进一步扩散。

尽管据报道，这些行动及后续事件的范围都是全球性的，但挪威国安局表示，“*美国、欧洲和中东的公司一直都是主要攻击目标*”，而且经查实，威胁实施者还展现出了很强的行动能力和执行能力。

根据目前的情况及查明的风险，挪威国安局建议各公司和组织，在短期至中期内做好防御恶意网络行动企图的准备，并且指出，引人注目和不太引人注目的公司都可能受到影响，这意味着各种类型的船舶以及船东的陆上基础设施都容易受到网络行动的攻击。挪威海事局在2019 年 8 月 19 日发布的声明中进一步强调称：“*特别是有船在 ISPS / MARSEC 保安等级第二级或更高级的区域内营运的船东，更应该了解相关情况。*”

建议

虽然挪威国安局的通报函是针对挪威公司的，但我们建议所有船舶经营人以及负责船上基础设施的公司持续监控和审查数字化安全情况，并遵循所提出的建议，包括：

- 确保已设置网络分段。网络的管理部分和操作部分之间不应存在任何物理连接。
- 将所有端点处及网络内的活动记录下来。挪威国安局建议，记录至少保留六个月。
- 在可能的情况下使用加密通信，在船舶和陆上基础设施之间也是如此。未经加密的通信内容很容易遭到篡改。
- 根据相关人员所担任的职务和岗位，设置其对信息和系统的访问权限。在大多数情况下，设置访问权限能够限制网络行动产生的后果。

在建议的对策中，强调了开展网络安全意识培训的重要性。所有“用户”，包括海员、岸上工作人员和其他相关人员，都应该：

- 注意带有链接或附件的电子邮件，谨慎做出判断。
    - 如果对于能否安全打开附件或链接有任何疑问——请评估确定是否有必要打开它。向您的雇主报告与公司有关的可疑电子邮件或消息。
    - 对于 Word、Excel 或 PowerPoint 中提示启用宏的文档，请多加小心。
- 在社交媒体中：
    - 报告通过社交媒体收到的可疑消息，特别是当该等消息与您的受雇情况或公司整体相关时。
    - 只跟身份可以验证的人建立并保持联系。
    - 极为谨慎地判断社交媒体中带有链接和附件的消息，这是犯罪分子瞄准的新战场。
    - 预想到每个人都能看到您分享在社交媒体上的、有关工作和私人生活的所有信息。
    - 未经雇主同意，不发布与工作有关的信息。
    - 未经其他人同意，不发布与他们有关的信息。
    - 在产品和应用程序中，启用可用的安全设置。
    - 不要在各类服务系统中重复使用同一密码。
    - 成为安全 **STAR**：每当您怀疑可能遭到攻击或不确定该怎么做时，请 **S**top（停下）–**T**hink（思考）– **A**sk（询问）– **R**eport（报告）。

船舶经营人还应密切关注其国家安全主管部门提供的任何网络安全建议。举例而言，建议挪威公司遵循挪威国安局“关于信息技术和通信技术（ICT）安全的基本原则”以及“有关社交媒体的措施和建议”（两者都只有挪威语版本）。我们还建议船舶经营人和海员，向其船旗国政府和/或国家安全主管部门报告所有可疑行动和安全漏洞，因为这样做能协助其对不断出现的网络威胁和风险实施监控。

其他指引

希望了解网络风险管理方面的其他建议，请参阅本协会于 2019 年 7 月 10 日发布的“船舶经营人无法忽视网络安全”和 2018 年 12 月 12 日发布的“船上网络安全程序亟待加强”。在开展安全意识培训时，我们与挪威船级社联合制作的防损意识视频也能有所帮助。

我们也提醒船舶经营人，最晚在 2021 年 1 月 1 日之后根据《ISM 规则》进行首次年度审核时，船舶现有的安全管理体系（定义见《ISM 规则》）中的网络风险必须得到适当处理。有关实施网络风险管理的指南和最佳实践，请参见国际海事组织通函 MSC-FAL.1/Circ.3 及行业指南《船上网络安全指南》。