SARNIA MARINE
INSURANCE BROKERAGE CO. LTD

"SARNIA NEWS" CIRCULAR

(Ref: 301/16/GP)

TO ALL SHIPOWNER CLIENTS 29TH June 2016

Re: IMPORTANT ALERT- EMAIL "MACRO MALWARE" CYBER THREAT

The below "ALERT" has been received from Gray Page warning of the recurrent malware attacks via attachments of Microsoft Word and Excel documents to emails. Caution should be applied when receiving emails from both KNOWN and UNKNOWN sources and ship owners should NOT OPEN such attachments, unless they are satisfied that their IT systems in place protect them.

Best regards,

The Loss Prevention Team

A NEW ALERT FROM GRAY PAGE

Email “Macro Malware” Cyber Threat

Background

Many companies are reporting receiving “invoice”, “receipt” and “bunker delivery receipt” emails with Microsoft Word documents attached which are in fact malware attacks.
The emails - originating most recently from well-known companies in the Asia Pacific bunker market, as well as commodity trading groups whose systems have been infected by malware-imbedded viruses – are designed to trick people into enabling ‘malicious’ macros to run and install malware on IT networks and computers.

Assessment and Analysis

There are millions of cyber-attacks on the IT infrastructure and networks of companies globally each day. Email-delivered malware is not a new phenomenon, but it persists because it is a relatively simple attack to execute and it continues to succeed.

Email users are reminded to be alert to unexpected emails with attachments, whether they are received from known or unknown sources. Caution should be paid particularly to Microsoft Office attachments - including Word and Excel - which claim users must enable macros to view a document, invoice or receipt, for example.
Users unfamiliar with macros should report emails containing them to their IT departments and NOT open them first.