**Singapore Cyber-Attack on Shipping Company**

**A Singapore based shipping company** **is the latest major corporation to suffer a malware cyber-attack which has caused a major disruption to its operational and commercial services.**

The BW Group, a Norwegian owned corporation operating much of its fleet out of Singapore has been struggling to restore full-operating capability. Many of the group-wide systems have been shut down for over a month, since the attack first struck, preventing employees accessing web services and using business services.

It is understood that the denial of service attack affects only shore based systems and that ship operations are not affected. However, all back-office systems such as payroll are only just being recovered.

The source of the attack is unknown and a tight hold on has been kept on information and no official announcements have been made. This is a departure from the practise of other companies which have been open about such attacks in an effort to support a coordinated response against malicious hackers. The level of secrecy is such that it is understood that even company executives have not been informed as to the causes or reason for the attack.

BW Group have declined to comment on the matter. But one employee who wished to remain anonymous confirmed the extent of the disruption and the major impact it has been having on business operations. “It has brought the Company to a halt and no one really knows the full story. Fortunately, the fleets are not affected”.

To solve the situation IT forensics specialists from the professional services company KPMG have been quietly drafted in to determine the cause of the attack. However, despite some weeks on BW’s operating sites the source of the attack has not been discovered and in order to restore services the entire BW networking infrastructure is having to be rebuilt to bring its services back online. This indicates the extent and seriousness of the attack.

The cost to commercial operations and the rebuilding of IT infrastructure is not yet known but is likely to be considerable. A previous attack on ship operator Maersk is likely to run into the hundreds of millions of dollars’ worth of lost business.

The Maersk attack is understood to have used the Petya virus which originated in the Ukraine in June and has been used widely in attacks against a number of international corporations including Mondelez International - which owns chocolate-maker Cadbury - and consumer health manufacturer Reckitt Benckiser.

The usual motive for a denial of service attack is to demand a ransom to restore the systems to operating capability. It is not known whether a ransom has been demanded from BW, however, the scale of effort undertaken by the Company and the length of time is systems have been inoperable is consistent with the criminally motivated denial of service attacks seen elsewhere.

In recent times, significant efforts to protect critical infrastructure have been made. Malicious hackers have moved their attention to less well-defended corporate systems which generally have lower levels of protection and undeveloped disaster and recovery plans. Such targets are regarded as ‘easy meat’ and potentially lucrative targets for hackers. Most businesses now have woken to the realisation that they cannot stop cyber-attacks but must manage them.

ENDS

**James Maclaren Associates**

**a**   Penhurst House ¦  352 Battersea Park Road ¦ London ¦ SW11 3BY ¦ United Kingdom

**e**   [james.maclaren@maclarenassociates.co.uk](mailto:james.maclaren@maclarenassociates.co.uk)

**w**  [www.maclarenassociates.co.uk](file:///C:\Users\chedham\Desktop\www.maclarenassociates.co.uk)

**m**  +44 (0) 7597 774 794

t    +44 (0) 121 286 3137

Copyright © 2017 by James Maclaren

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the author.