MEMORANDUM
FOR ATTENTION

Association Of Stockbroking Companies Malaysia

Ref No : 0035 of 2017/PO
Date : 22 August 2017

To : Executive Director/ Head of Dealing
Executive Director/ Head of Operations

From : The Secretariat, ASCM
No. of pages : As per attachment

By Email

RE : Latest Advisory From NC4 On Cyber Threat

Dear Members,

We understand that Bursa has notified members yesterday on an alert issued by the National Cyber Coordination & Command Centre (NC4).

Bursa has been advised by the NC4 of possible massive intrusion, distributed denial of service (DDoS) and web defacement threats targeting Malaysian websites by Indonesian Hackers.

For ease of reference, attached is the email notification, dated 21st August 2017 by Ms. Tay Yu Hui of Bursa Malaysia for your attention.

In view of the critical need to manage such cyber-attack timely and effectively, we urge members who have any form of cybersecurity threats to immediately escalate the matter to Bursa.

Thank you

Yours sincerely

Lim Boon Hang
Executive Director, ASCM Secretariat

D-3-53, Block Dahlia,10 Boulevard, Lebuhraya SPRINT, PJU 6A
47400 Petaling Jaya, Selangor, Malaysia
Reg No: PPM-001-14-31071996
Tel: +603-7732 7768
+603-7732 7769
Fax: +603-7733 7760
www.ascm.org.my

Subject: Latest Advisory From NC4 On Cyber Threat - Important Note

From: Tay Yu Hui [mailto:tayyuhui@bursamalaysia.com]
Sent: Monday, August 21, 2017 3:13 PM
Subject: Latest Advisory From NC4 On Cyber Threat - Important Note

Dear All,
Bursa Malaysia has received advisory from National Cyber Coordination & Command Centre (NC4) of possible massive intrusion, distributed denial of service (DDoS) and web defacement threats targeting Malaysian websites by Indonesian Hackers.

Impact

Information leakage, information loss, service disruption and integrity of information compromised.

Brief Description

In view of the current incident involving the Indonesian flag error during the recent opening of KL SEA Games 2017, a few Indonesian hacker's groups had launched a few campaigns to launch threats to Malaysian websites.
Therefore, organisations are urged to take the necessary actions to prevent your organisation from becoming a victim of these threats.

Affected Products

All operating systems and web servers.

Recommendation

As advised by NC4, please take the following actions:

1. Update your critical assets with the latest security patches and updates;
2. Warn your users not to open or click on unsolicited mails and links with/without attachments;
3. Ensure that anti-virus/anti-malware signatures are up to date and functioning;
4. Block or restrict access to every port and services except for those that should be publicly available;
5. Review your user credentials list for any new additional unknown user;
6. Monitor your environment closely for any anomalies;
7. Check whether your organisation's credentials have been exposed in pastebin;
8. If you suspect that your servers have been compromised, reset all usernames and passwords; and
9. Report any anomalies and suspicious events happening within your network and enterprise environment to Bursa Malaysia Customer Service immediately.

Please stay vigilant and report to us immediately if you experience any cyber threats or notice any suspicious events.

Thanks & Best Regards

Yuhui

Tay Yu Hui | Executive Vice President | Exchanges Operations | Market Operations,
Bursa Malaysia Berhad, 10th Floor, Exchange Square, Bukit Kewangan, 50200 Kuala Lumpur, Malaysia
t: +603-20347697 | f: +603-20266163 | email: tayyuhui@bursamalaysia.com | website: www.bursamalaysia.com