MEDIA STATEMENT

20 August 2014

Members of the Media,

Regarding your enquiry with regards to the article that was published in The STAR (Malaysia) newspaper dated on 20 August 2014, we would like to inform you that CyberSecurity Malaysia did not disclosed neither names or the list of agencies involved in the hacking attack incident. The sources were not from CyberSecurity Malaysia.

The MH370 incident has become a global issue and receives significant attention from various organizations locally and also internationally.

However, as the agency responsible in cyber security related matters, CyberSecurity Malaysia did involve in the investigation of MH370. Our involvement was merely on providing technical support through our Digital Forensics team to the local agencies involved in the investigation.

As we also monitor the cyber security incidents in Malaysia, we took the initiative by issuing two advisories related to MH370 incidents to the general public as follows:

(i) 24 March 2014 - Malware Related to Missing Malaysia Airlines MH370 Plane

http://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/962/index.html

(ii) 18 March 2014: Missing Malaysia Airlines MH370 Plane Found Hoax

http://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/960/index.html

(iii) 18 April 2014 - Spear Phishing Attacked Related to MH370 Plane

http://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/967/index.html

Due to the fact that the MH370 incident is still under investigation, we do not intend to complicate the issue by responding to further enquiry. We feel that it is appropriate for those authorized organizations to make further statement and give comments on issue pertinent to MH370.

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999
www.cybersecurity.my

Information on "Spearphishing attack"

Advance Persistent Threat attack or in short APT usually happen and link to a major news cycle or major incident, in this case the MH370 tragedy. The APT attack is carefully crafted and it usually targets the nation, organisation or an individual with the main purpose of gathering sensitive information, confidential data, and/or trade secret.

"Spearphishing attack" is one of the most popular attack vector used for APT which contain malicious email attachment that can bypass unprotected network environment.

Internet users and organisations are advised to be precautions of any suspicious activities and threats that could take advantage on the current news and incidents. They must deploy good standard security practises and always review their security policy by stressing and focusing on the current IT technology with in mind on how to be prepared in addressing current cyber threats.

Among steps to prevent being a victim are:-

i. Use best practises and guidelines;
ii. Frequent up-to-date patching of Operating System (OS), common vulnerabilities Internet browser, Java, Adobe Reader, Flash etc.;
iii. Constant update on the signatures of Firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS) and Anti-malware;
iv. Deploy centralise logging system or/and Security Information and Event Management (SIEM) to monitor organization infrastructure and network activities;
v. Recruit a dedicated IT Security team to monitor and response cyber threat incident.

~ end.

For further enquiries about this document, please feel free to call 603-8992 6888, Mohd Shamil Mohd Yusoff (ext: 6978), email shamil@cybersecurity.my / Sandra Isnaji (ext: 6977), email sandra@cybersecurity.my / Zul Akmal Abdul Manan (ext: 6945), email zul.akmal@cybersecurity.my