MEDIA RELEASE

26 August 2013

FOR IMMEDIATE RELEASE

CYBER SECURITY SCENARIO IN MALAYSIA FIRST HALF 2013 REVIEW

Review on the latest trends and activities related to cyber security based on the incidents reported to Cyber999 Help Centre

(**KUALA LUMPUR**) – As Malaysia moves towards becoming a developed Nation, information and communication technology (ICT) become significantly important across all sectors. The rapid development of ICT supported by various innovation-based activities enhances the socio-economic quality of the country. However, there are side effects caused by high usage of ICT, namely cyber security incidents and threats. If these threats are not controlled and the community is not given a proper education and awareness, the threats could undermine and destroy the country's well-being.

Today, CyberSecurity Malaysia, a technical agency in the field of cyber security and also an agency under the purview of the Ministry of Science, Technology and Innovation (MOSTI) that is responsible to monitor Malaysia's e-security aspects holds a special media briefing session to share with the general public about the cyber security scenario in Malaysia based on cyber security incidents reported to Cyber999 Help Centre.

From January to June 2013, a total of 5,592 cyber security incidents were reported to Cyber999 compared to 5,581 incidents reported in First Half of 2012. The number of incidents in First Half of 2013 recorded a very small increase compared to First Half 2012 with an increase of only 0.2 %. Fraud is the most-reported incidents followed by Intrusion, Spam, Malicious Codes, Cyber Harassment, Content Related, Intrusion Attempts, Denial of Service and Vulnerability Report.

Analysing the data of reported cyber security incidents in the First Half of 2013 and comparing them with the data for the same period in 2011 and 2012, we found a similar pattern where Fraud, Intrusion and Malicious Codes are always in the top three of most-reported cyber security incidents in the country.

Within the first six months period of 2013, the following categories of cyber security incidents have increased: Content Related (320%), Spam (111%), Cyber Harassment (35%), Malicious Codes (25%) and Fraud (2%); whereas the following categories have decreased: Intrusion (-22%), Intrusion Attempts (-56%), Denial of Service (-17%), and Vulnerability Reports (-76%).

The details are as follows:

Incidents	*January - Jun 2012*	January - Jun 2013	% increase (decrease)
Fraud	*2439*	2490	2
Intrusion	*2203*	1726	(22)
Spam	*291*	614	111
Malicious Codes	*353*	442	25
Cyber harassment	*173*	233	35
Content Related	*10*	42	320
Intrusion Attempts	*55*	24	(56)
Denial of Service	*12*	10	(17)
Vulnerability Report	*45*	11	(76)
TOTAL	***5,581***	**5,592**	

Table 1: Comparison of Cyber Security Incidents Reported to Cyber999 from January – June

Dr. Amirudin Abdul Wahab, Chief Executive Officer of CyberSecurity Malaysia, said "These are the reported incidents and not yet considered as cyber crime cases. The incidents came from the public who wish to seek our technical assistance in resolving cyber security issues that they encountered while using the Internet."

"We found that incidents involving technical aspects like Intrusion (mostly involving web defacement), intrusion attempts (such as attempts to hack networks) and vulnerability reports have decreased slightly. On the contrary, incidents that relies on 'human weakness' such as Fraud, Spams, Cyber harassment and Content-related incidents have increased significantly. This shows that cyber criminals are targeting 'people' instead of 'machines', because people are the weakest link in cyber security. Furthermore, advanced technical measures such as three-tier security verifications are making it more difficult to penetrate machines and networks. Therefore, we advise the public to be wary of 'social engineering', a tactic used by criminals to befriend their victims before deceiving them." Added Dr. Amirudin.

Cyber security incidents are reported to Cyber999 Help Centre on a voluntary basis by the public as well as organizations within Malaysia. There are also incidents reported from outside the country such as foreign CERTs and security teams.

Detail analysis is as follows:

(i) Fraud incident
Even though the increased is only 2% compared to First Half 2012, Fraud activity is still prevalent on the internet and continue to grow. With more people connected to the Internet, it gives more opportunities for scammers to carry out their scam activities. Majority of Fraud incident reported to Cyber999 are Phishing, Nigerian Scam, Fraud Purchase, Online Scam. Scam cases that have criminal elements will be escalated to the Law Enforcement Agency for their further investigation.

(iii) Intrusion incident
Intrusion incidents reported had slightly dropped in the First Half of 2013 compared to same period last year. However, System Administrators must always be vigilant and take serious precautions towards their systems by having proper patches and security fixes to the

T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999
a@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
www.cybersecurity.my

network. Majority of Intrusion incidents reported to Cyber999 are web defacements, a type of unauthorised modifications to a website. Web defacement incidents are usually issues-based, which means web defacement incidents would increase when some disputes or issues between Malaysia and another country are taken online, where the citizens of one country would attack and deface websites in the other country, causing citizens from the other country to retaliate.

(iii) Malicious Codes

Malicious Codes recorded more than 25% increase in First Half of 2013 compared to the First Half of 2012. The significant increase in malicious codes is contributed by a distributed denial of service (DDoS) botnet, known as Nitol botnet that mostly operated in China. The incident was reported by CNCERT (The National Computer Network Emergency Response Technical Team Coordination Center of China), which collected information about machines infected with the Nitol botnet and notified relevant constituencies for their action to rectify the infected machines.

More information on Nitol Botnet is available at:

- *http://blogs.mcafee.com/mcafee-labs/digging-into-the-nitol-ddos-botnet*
- *http://www.csoonline.com/article/716188/microsoft-downs-botnet-that-infiltrated-chinese-pc-supply-chain*

(iv). Cyber harassments

Cyber harassment also increased by 35% compared to First Half of 2012. The increase could be due to the increase in social networking sites usage, because the majority of cyber harassments incidents happened via social networking sites. Social networking sites have also become a popular avenue for people with malicious intention to harass other people on the net.

"We urge Internet users to pay extra attention and be careful when selecting who they want to be friends with on the net as there are irresponsible users on the net with malicious purpose to threaten other Internet users into giving them money. Internet users who are harrassed, bullied or threatened by someone over the Internet are advised to save the evidence such as email headers and chat history and email them to cyber999@cybersecurity.my. They are also advised to lodge a police report immediately at a nearby police station and bring the evidence." said Dr. Amirudin.

(**v). Content Related**

Content related incidents are contents that can cause disruption to peace and harmony of the country such as contents that is defamatory towards race, religion, and the Malay Rulers. Content-related incidents have increased tremendously in the first half of 2013 compared to the first half of 2012 with more than 100% increase. The significant increase is due to the increase is Internet usage which leads to increase in social networking sites. Majority of content related incidents are done through social networking sites besides emails. Contents related incidents that are considered disruptive to the Nation's peace and harmony are referred to the Law Enforcement Agency for further investigation.

Dr. Amirudin also urges Internet users to be ethical, learn to respect other religions, race and never create sentiments while posting messages on the net.

CyberSecurity Malaysia always play its roles in mitigating cyber threats by conducting more awareness programmes, producing innovative cyber security related services, collaborating with various external organisations and enhancing the employee's skills in order to make the safety of Malaysian cyberspace.

~ End ~

CyberSecurity Malaysia is the national specialist centre for cyber security, under the Ministry of Science, Technology and Innovation (MOSTI). For additional information, please visit our website at http://www.cybersecurity.my. Stay connected with us on www.facebook.com/CyberSecurityMalaysia and www.twitter.com/cybersecuritymy

For further enquiries about this document, please call +603-8992 6888,
Mohd Shamil Mohd Yusoff (ext: 6978), or Sandra Isnaji (ext: 6977) or email media@cybersecurity.my