Ministry of Science, Technology and Innovation

An agency under MOSTI

MEDIA RELEASE

10 September 2014
FOR IMMEDIATE RELEASE

E-BUSINESSES, ONLINE SHOPPERS, JOB-SEEKERS URGED TO BE SUSPICIOUS

2014 HALF-YEAR INCIDENTS STATISTIC RELEASED BY CYBERSECURITY MALAYSIA REVEALED MORE THAN HALF (51 PERCENT) ARE DUE TO FINANCIALLY MOTIVATED FRAUDS AND SCAMS.

KUALA LUMPUR, 10TH SEPTEMBER 2014. CyberSecurity Malaysia, the national cyber security specialist agency under the Ministry of Science, Technology and Innovation (MOSTI) today released the 2014 half-year incident statistics. The cyber security incidents were voluntarily reported to the Cyber999 Help Centre between January and June this year. The reports come from home users, private sectors, government sectors, security teams from abroad, foreign CERTs, Special Interest Groups, Security Feeds and CyberSecurity Malaysia's own initiative in proactively monitoring several events for cyber incidents.

According to Dr. Amirudin Abdul Wahab, the Chief Executive Officer of CyberSecurity Malaysia:

> "The highest number of incidents reported to **Cyber999** is the **financially motivated frauds and scams** at 51.3 percent or 2113 incidents, more than half the total of 4117 incidents.
>
> **Technically motivated attacks** such as intrusion or attempts or vulnerability of network involves a total of 880 (21.4 percent), or almost a quarter of total incidents.
>
> **Malware and Virus Infection** make up 14.1 percent of all incidents,
>
> **Spams** 247 or 6 percent,
>
> **Cyber Harassment** 6.8%, and
>
> **Inappropriate Contents** 0.4 percent. Inappropriate Contents include Vulgar, Defamatory, Seditious and Bogus posting in blogs and social networking sites."
>
> "The incidents were reported via email, fax, online form, SMS and phone call. But today we are also launching the Cyber999 App for smart phones running on Android and iOS. This will make it much easier to submit online complaints, and we hope it

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

will encourage more people to voluntarily report cyber security matters to the Cyber999 Help Centre of CyberSecurity Malaysia" Dr. Amirudin added.

Dr. Amiruddin said: "We believe that financially motivated incidents will continue to dominate. We advise e-business owners (sellers), online shoppers (buyers) and job seekers to be extremely careful and be suspicious whenever an advance payment is required. Once you part with your money, it is very difficult to get them back, especially when you're dealing over the Internet because you do not know each other well enough and it is very difficult to produce evidence and to prove the acts of cheating or frauds or scams"

PLEASE REFER BELOW FOR DETAILED ANALYSIS OF THE STATISTC

~ END ~

For media enquiries email us at media@cybersecurity.my or call 603-8992 6888, Mohd Shamil Mohd Yusoff (ext: 6978) / Sandra Isnaji (ext: 6977) / Zul Akmal Abdul Manan (ext: 6945)

CYBERSECURITY MALAYSIA FIRST HALF 2014 REVIEW REPORT

Introduction

The CyberSecurity Malaysia Half Year Report provides an overview of activities carried out by the Malaysia Computer Emergency Response Team (hereinafter referred to as MyCERT), a department within CyberSecurity Malaysia. These activities are related to computer security incidents and trends based on security incidents handled by CyberSecurity Malaysia. The statistics provided in this report reflect only the total number of incidents handled by CyberSecurity Malaysia and not elements such as monetary value or repercussions of the incidents. Computer security incidents handled by CyberSecurity Malaysia are those reported to us, that occur or originate within the Malaysian constituency.

Incidents were reported to CyberSecurity Malaysia by various parties within the constituency as well as from foreign. This include home users, private sectors, government sectors, security teams from abroad, foreign CERTs, Special Interest Groups, Security Feeds and including CyberSecurity Malaysia's proactive monitoring on several cyber incidents.

Incident Trends

The increase of cyber security incidents in Malaysia, from year to year, is closely related to various factors, which includes the increase of the Internet usage in the country. At present, Malaysia has more than 17 million Internet users and the number is growing with the support from the robust development of broadband infrastructure. This is combined with the wide

availability and fast technology advancements in smart phones and mobile devices which makes Internet access much easier and more convenient.

Year	No. of Incidents
2011	15218
2012	9986
2013	10, 636
2014 (Jan – July)	4117

Figure 1: Number of Incidents on Yearly

From January to June 2014, CyberSecurity Malaysia, via its Cyber999 service, handled a total of 4117 incidents. Figure 2 illustrates the number of incident classified according to categories of incident and by month.

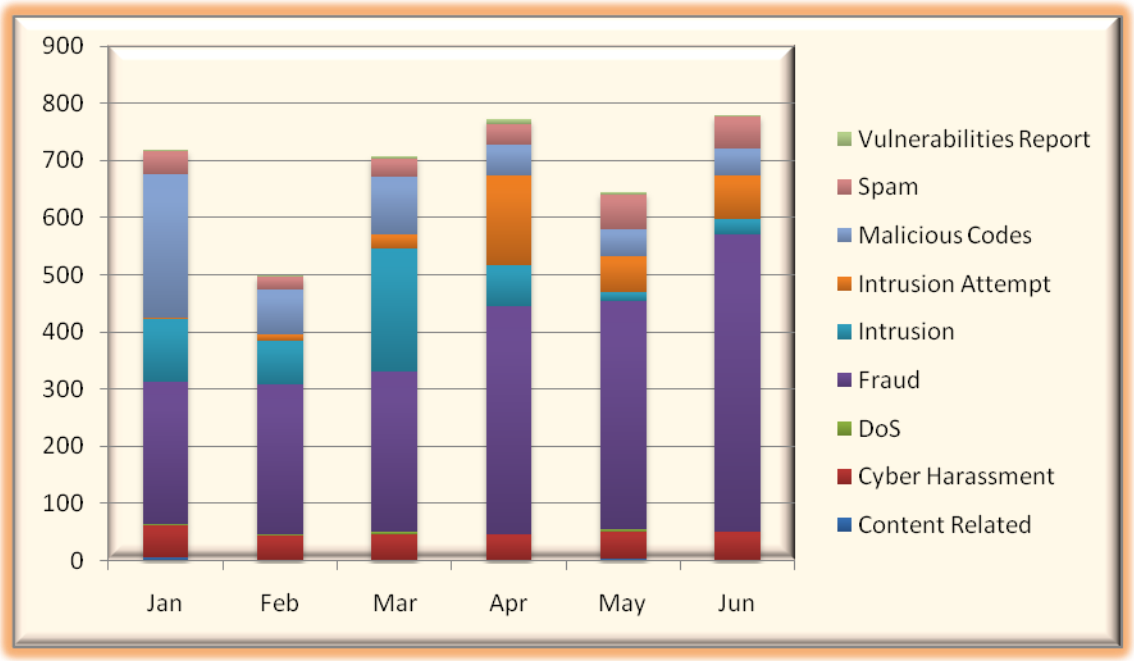

Figure 2: Number of incident by month

The average incident that Cyber999 received each month is around 686 incidents. Apart from the month of February 2014, Cyber999 received more than 600 incidents per month. Comparatively, the number of incident that we received for the first half of this year is lesser than the first half of 2013. The total number of incident that CyberSecurity Malaysia received

between January until June 2013 is 5592 incidents, which is 1475 incidents more than first half of 2014.

Cyber Security Incidents	Number of	Percentage
Total Incidents	***4117***	***100***
Frauds & Scams (Phishing, Job scams, Online shopping frauds, etc)	2113	51.3%
Technical attacks or attempts (Intrusion, DDoS, Defacement, Vulnerability report etc)	880	21.4%
Malware or Virus	580	14.1%
Cyber Harrassment	281	6.8%
Spams	247	6.0%
Inappropriate content	16	0.4%

Figure 3 illustrates percentage of incident by category in the first half of 2014. Based on figure below, the highest incident that has been reported is fraud incident representing 51% of the total incident. This is a continuation from the previous year as fraud is the most incident that has been reported for the year 2013. The incident that falls under fraud is phishing, online scam, fraud purchase and job scam.

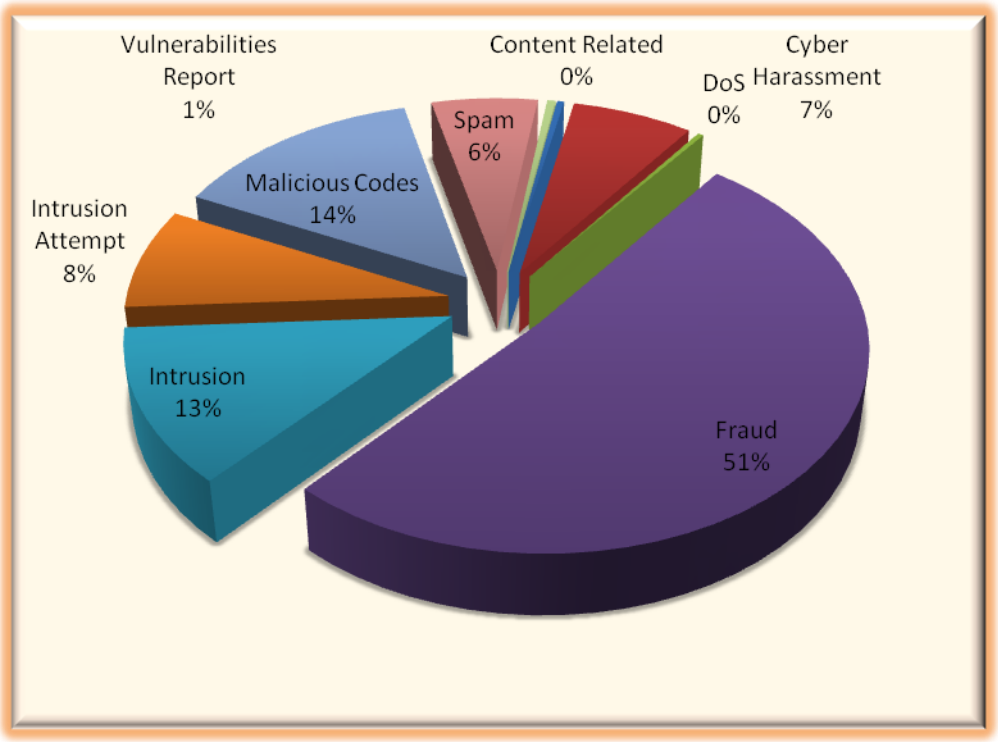

Figure 3: Percentage of incident in 1st half of 2014

Fraud incidents recorded highest number compared to other incidents with majority of them are phishing incidents followed by fraud purchases, job scams and upfront-money scams.

CyberSecurity Malaysia predicts that fraud incident will continue to grow and always be among the most reported incident. Because of that, CyberSecurity Malaysia advised Internet users to be precautious and always adhere to best practices when they purchase goods online. Users must ensure that the dealing is made with trusted parties and never simply transfer money to seller without prior checking on the status of the seller.

The second and third most reported incident to Cyber999 is separated with only 1% or 66 incidents. The second most reported incident is malicious code with 580 incidents or 14% of the total incident. This follows with intrusion with 514 incidents. The majority of malicious code incidents are mostly reported by Foreign Security Company and Security Feeds regarding Malaysia IPs involved in botnet and Command& Control Server activities. Other Malicious Code incidents reported to us are Malware Hosting, where vulnerable hosts belonging to Malaysia constituency are compromised and used to serve malware.

During the beginning of New Year 2014, CyberSecurity Malaysia observe significant increase of defacement incident. The domains belong to various sectors within the .MY constituency. CyberSecurity Malaysia responded to web defacement incidents by notifying respective Web Administrators to rectify the defaced websites by following our recommendations, leading to the defaced websites being rectified by the respective Administrators. As was in the years, web defacements or web vandalism was still occurring continuously. Based on the findings, majority of these web defacements were due to vulnerable web applications or unpatched servers involving web servers running on IIS and Apache. Majority of the defacements attacks were using SQL Injection and cross-site scripting (XSS) methods.

Account compromise involve perpetrators are taking advantage of various techniques to compromise accounts belonging to other Internet users. Majority of account compromise incidents involved free web based email accounts and social networking accounts such as Facebook. Account compromise incidents could be prevented if users practice good password management such as using strong passwords, never share passwords and avoid using a single password for multiple services.

Users may refer to the below URL on good password management practise:

- http://www.auscert.org.au/render.html?it=2260
- http://www.us-cert.gov/cas/tips/ST04-002.html

In the 2014 First Half, Microsoft has released an official announcement that Microsoft is ending support for the Windows XP Operating System and Office 2003 on April 8, 2014. After this date, both Microsoft products will no longer receive any software or content updates, security patches and assisted technical support from Microsoft. CyberSecurity Malaysia has released an alert regarding this matter and monitored the situation if there is an increase in incident. There is however no increase in incident related to this matter.

In the 2014 First Half, the situation related to MH370 had contributed to the increase, though not significantly, in incidents reported in first half of 2014. The related incidents are defacement and malicious code. The total defacement incident related to MH370 is 61. The most TLD that related to this incident is .com.my with 29 incident. Malicious code incident

that connected with MH370 is about fake Facebook Apps, that contains malware. When user clicked on the Apps, the computer will be infected with malicious code.

We had released three (3) Alerts and an Advisory on the above matter:

http://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/960/index.html
http://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/962/index.html
http://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/967/index.html

In the First Half of 2014, CyberSecurity Malaysia received information from valid source regarding a vulnerability that exist on OpenSSL Versions 1.0.1 through 1.0.1f that could disclose sensitive information belonging to users to an attacker.

The vulnerability allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. There is a possibility that this may compromise the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop communications, steal data directly from the services and users and to impersonate services and users.

CyberSecurity Malaysia had issued 2(two) Alert and Advisory related to the above vulnerability at:

http://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/963/index.html
http://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/964/index.html

Alerts and Advisories

From January to June 2014, CyberSecurity Malaysia had issued a total of 37 Advisories and Alerts for its constituency. This included related to Microsoft Security Bulletin Summary, Security updates for Adobe Flash Player, Adobe Reader and Acrobat, OpenSSL Heartbleed Information Disclosure Vulnerability, Malware related to the Missing MH370, New Zero Day Exploit, Security Updates for Firefox, Thunderbird, Seamonkey, Critical Vulnerability in Internet Explorer 9and Increase in web defacement activities. The Alert and Advisory comes with descriptions, recommendations and references that can be used as as Guide for

Internet Users and System Administrators. The Alerts and Advisory are available at our website at:

Readers can visit the following URL on advisories and alerts released by CyberSecurity Malaysia.

http://www.mycert.org.my/en/services/advisories/mycert/2013/main/index.html

~ End ~