MyCERT 4th Quarter 2011 Summary Report

Introduction

The MyCERT Quarterly Summary Report provides an overview of activities carried out by the Malaysian 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 MyCERT. The summary highlights statistics of incidents according to categories handled by MyCERT in Q4 2011, security advisories and other activities carried out by MyCERT personnel.

The statisticsprovided in this report reflect only the total number of incidents handled by MyCERT and not elements such as monetary value or repercussions of the incidents. Computer security incidents handled by MyCERT are those that occur or originate within the Malaysian constituency. MyCERT works closely with other local and global entities to resolve computer security incidents.

Incidents Trends Q4 2011

Incidents were reported to MyCERT by various parties within the constituency as well as from foreign sources, which include home users both local and foreign, private sector entities, government sector, security teams from abroad, foreign CERTs, Special Interest Groups including MyCERT's proactive monitoring on specific incidents such as Intrusions.

From October to December 2011, MyCERT, via its Cyber999 service, handled a total of 3,288 incidents representing a 27.35 percent decrease compared to the previous quarter. In Q4 2011, incidents such as Intrusions, Intrusion Attempts and Cyber Harassment showed an increase compared to the previous quarter while other types of incidents had considerably decreased.

Figure 1 illustrates incidents received in Q4 2011 classified according to the type of incidents handled by MyCERT.

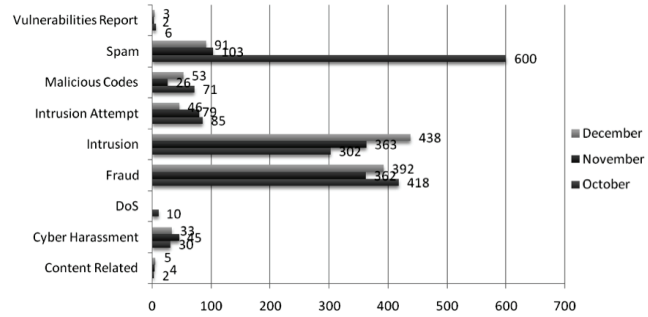

Figure 1: *Breakdown of Incidents by Classification in Q4 2011*

Figure 2 illustrates the incidents received in Q4 2011 classified according to the type of incidents handled by MyCERT and its comparison with the number of incidents received in the previous quarter.

Categories of Incidents	Quarter		Percentage
	Q3 2011	Q4 2011	
Intrusion Attempt	189	209	10.58
Denial of Service	14	1	-92.86
Spam	1646	299	-81.83
Fraud	1355	1153	-14.91
Vulnerability Report	17	11	-35.29
Cyber Harassment	80	105	31.25
Content Related	14	11	-21.43
Malicious Codes	233	142	-39.06
Intrusion	978	1357	38.75

Figure 2: *Comparison of Incidents between Q3 2011 and Q4 2011*

Figure 3: Shows the percentage of incidents handled according to categories in Q4 2011.

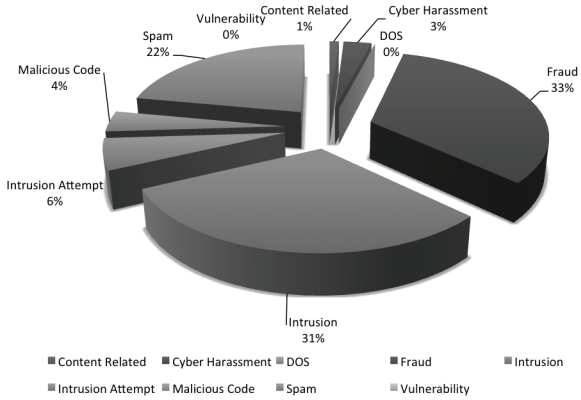

Figure 3: *Percentage of Incidents in Q4 2011*

In Q4 2011, a total of 1,357 incidents on Intrusion representing a 38.75 percent increase compared to previous quarter. Most of these Intrusion incidents are web defacements, also known as web vandalism followed by account compromise. Web defacements are referred to as unauthorised modifications to a website with inappropriate messages or images with various motives by the defacer. This was made possible due to vulnerable web applications or unpatched servers involving mostly web servers running on IIS and Apache with a few others involving other platforms.

In this quarter, we received a total of 565 .MY domains defaced with the majority involving .COM.MY and .COM domains belonging to the private sector. The defaced domains were hosted on single servers that host single domains as well as on virtual hosting servers that host multiple domains, belonging to local web hosting companies. These web defacements were successfully controlled. MyCERT advised System Administrators on steps to rectify and recover from these defacements.

As was in the previous quarter, MyCERT observed that the majority of web defacements were done using the SQL injection attack technique.

More information about SQL Injection technique and fixes is available at: http://www.mycert.org.my/en/resources/web_security/main/main/detail/573/index.html

Figure 4 shows the breakdown of domains defaced in Q4 2011.

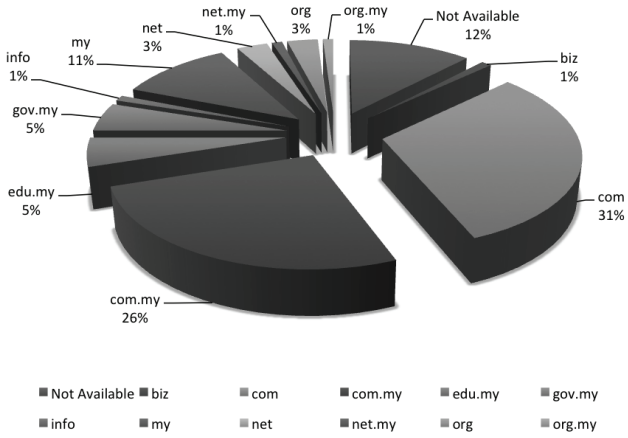

Figure 4: *Percentage of Web Defacement by Domain in Q4 2011*

Account compromise refers to unauthorised access or ownership to another account via stolen passwords or the act of sharing passwords for various malicious motives. The account compromise reported to us mainly involved free-based email and social networking accounts. The compromised accounts will then be used in malicious activities on the net such as in Nigerian scams, impersonation and cyber harassment. Based on our observation, account compromise incidents are mainly due to poor password management practices such as using weak passwords and the act of sharing passwords. As such we advise users to practice good password

management to prevent their accounts from being compromised.

Users may refer to the below URL on good password management practises:
http://www.auscert.org.au/render.html?it=2260
http://www.us-cert.gov/cas/tips/ST04-002.html

Fraud incidents had decreased to about 14.91 percent in this quarter compared to the previous quarter. The majority of fraud incidents handled were phishing attacks involving foreign and local brands with the rest of fraud incidents consisting of Nigerian scams, lottery scams, illegal investments, job scams and fraud purchases. The reason for the decrease could possibly be due to more awareness among Internet users of scam activities.

A total of 1,153 incidents were received on fraud activities in this quarter, from organisations and home users. A total of 241 phishing websites involving domestic and foreign brands were reported to us in this quarter with the majority of them belong to local brands. In this quarter, we observed an increase in local Islamic Banking entities becoming target of phishing activities compared to previous quarters. MyCERT handled both the source of the phishing emails as well as the removal of the phishing sites by communicating with the respective Internet Service Providers (ISPs).

Based on our analysis, the majority of the phishing sites were hosted on compromised machines besides phishers hosting them on purchased or rented domains. The machines may had been compromised and used to host phishing websites and other malicious programmes on it.

As was in the previous quarter, incidents on job scams and fraud purchases continue to increase with fraudsters using the same modus operandi.

We continue to receive incidents on cyber harassment in this quarter with a total of 105 incidents representing a 31.25 percent increase compared to the previous quarter. Harassment reports mainly involved cyberstalking, cyberbullying and threatening. Many of cyberharassment victims are people known to the perpetrators such as their friends, relatives, colleagues. etc. Threats via emails, blogs and social networking sites are prevalent in this quarter in which victims are threatened to pay money to individuals they just got to know on the net. If they refuse,their pictures will be exposed or uploaded on porn websites. MyCERT advised users to be very careful with whom they befriend with and never provide their personal details or photos to a third party on the net as details of such materials can be used for malicious activities.

In Q4 2011, MyCERT handled 142 incidents on malicious codes, which represents a 39.06 percent decrease compared to the previous quarter. Some of the malicious code incidents we handled are active botnet controllers, hosting of malware or malware configuration files on compromised machines and malware infections to computers.

Advisories and Alerts

In Q4 2011, MyCERT had issued a total of two advisories and alerts for its constituency which involved popular end -ser applications such as Adobe PDF Reader and Multiple Microsoft Vulnerabilities.

Attackers often compromise end-users' computers by exploiting vulnerabilities in the users' applications. Generally, the attacker tricks the user in opening a specially crafted file (i.e. a PDF document) or web page.

Readers can visit the following URL on advisories and alerts released by MyCERT http://www.mycert.org.my/en/services/advisories/mycert/2011/main/index.html

Other Activities

In Q4 2011, MyCERT wasinvited to conduct an Incident Handling training session for OIC-CERT Conference participants in Brunei. The training was held from 21 – 25 November 2011 focusing on Incident Handling, network and web security. The participants were mostly from the CERT of their respective countries. MyCERT staff had also presented findings at the Homeland Security Conference in Malaysia on topics concerning CyberSecurity Incidents in October 2011 and also at the Indonesian Information Security Forum on CERT/CC in December 2011. Other presentations were on MyCERT Experience in Handling Child Online Related Issues at Seminar Child Online Protection in October 2011 and a keynote address at the Cloud Computing Conference in November 2011 on Are We Ready to Go Into Cloud Computing? Another keynote address was also given at the ARADO CyberSecurity Seminar in December 2012 on CyberSecurity Trends and Technology.

Another important activity that was held in Q4 2011 was the country's fourth annual Cyber Drill, codenamed **X-MAYA4**, a simulated and coordinated exercise to assess the cyber security emergency readiness of Malaysia's Critical National Information Infrastructure (CNII) to cope against cyber attacks. This year's Cyber Drill scenarios involved two cyber security emergency incidences: web defacement and malware infection in which the players were required to identify the origin of the attacks, take minimising and mitigating steps, and rectify the defacement and/or outbreak.

Conclusion

Basically, in Q4 2011, the number of computer security incidents reported to us had decreased compared to the previous quarter. In addition, most categories of incidents reported to us had also decreased. The decrease is also a reflection that more Internet users are aware of current threats and are taking proper measures against these threats. It could also probably be due to the absence of significant attacks on the net specifically to Malaysian constituency. No severe incidents were reported to us this quarter and we did not observe any crisis or outbreak in our constituencies. Nevertheless, users and organisations must be constantly vigilant of the latest computer security threats and are advised to always take measures to protect their systems and networks from these threats.

Internet users and organisations may contact MyCERT for assistance at the below contact:

E-mail: mycert@mycert.org.my
Cyber999 Hotline: 1 300 88 2999
Phone: (603) 8992 6969
Fax: (603) 8945 3442
Phone: 019-266 5850
SMS: Type CYBER999 report <email> <report> & SMS to 15888
http://www.mycert.org.my/

Please refer to MyCERT's website for latest updates of this Quarterly Summary. ■