PRESS RELEASE

16Jun 2011
CBMR-5-RFI-6-ALERT-V1
FOR IMMEDIATE RELEASE

MYCERT ALERT - INCREASE IN CYBER SECURITY INCIDENTS

DATE OF PUBLICATION: 2011-06-15 WWW.MYCERT.ORG.MY

In relation to the recent cyber attacks against Malaysian websites, we received a large number of inquiries from the media, mostly requesting information about the technical aspects of the attack. Our computer emergency response team detected the anomalies and released the alert, below, on the 15th of June 2011. I would like to share this alert with the media. Thank you.

- ***Lt. Col. Dato' Husin bin Jazri, Chief Executive Officer***
  CyberSecurity Malaysia
  16 June 2011

1.0 Introduction

CyberSecurity Malaysia, through its technical arm THE MALAYSIA COMPUTER EMERGENCY RESPONSE TEAM (MyCERT), released an alert yesterday 15 June 2011, as it has observed significant increase in cyber security related activities (i.e. vulnerability scanning, intrusion attempts) in the last 24 hours. The attacks are targeting websites belonging to organizations and government in Malaysia, and are expected to last for several days.

2.0 Impact

Successful attack will affect the confidentiality, integrity of information and availability of the websites. This may further impact business activities of organizations.

3.0 Targeted Websites

Based on our observation, the attackers are targeting web applications that are vulnerable to publically known attack techniques, weak passwords and misconfiguration.

4.0 Recommendation

MyCERT advises all system owners to be alert and do the necessary to secure their websites. Please refer to the link in the references section for tips and best practices that can be applied to secure the websites.

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 8, Block A
Mines Waterfront Business Park
No 3 Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
T +603 8946 0999
F +603 8946 0888
www.cybersecurity.my

If your website is defaced or you observe attack attempts, do not hesitate to contact Cyber999 via the following channels:

E-mail : cyber999@cybersecurity.my or mycert@mycert.org.my
Phone : 1-300-88-2999 (monitored during business hours)
Fax : +603 89453442
Handphone : +60 19 2665850 (24x7 call incident reporting)
SMS : CYBER999 REPORT <EMAIL> <COMPLAINT> to 15888
Business Hours : Mon - Fri 08:30 -17:30 MYT
Web: http://www.mycert.org.my

5.0 References

- What you should know about web defacement - http://www.mycert.org.my/en/resources/incident_handling/main/main/detail/756/index.html
- Steps for recovering from a UNIX or NT system compromise http://www.auscert.org.au/render.html?it=1974&cid=1920
- Intrusion Detection Checklist http://zeltser.com/log-management/security-incident-log-review-checklist.pdf
- Guides On Fixing Sql Injections Vulnerabilities http://www.mycert.org.my/en/resources/web_security/main/main/detail/573/index.html
- How To: Protect From SQL Injection in ASP.NET http://msdn.microsoft.com/en-us/library/ms998271.aspx
- ModSecurity http://www.modsecurity.org/

~ End ~

CyberSecurity Malaysia is the national specialist centre for cyber security, under the purview of the Ministry of Science, Technology and Innovation (MOSTI). For additional information, please visit our website at http://www.cybersecurity.my. For general inquiry, please email to: info@cybersecurity.my. To report cyber incidents such as harassment, fraud or intrusion to our Cyber999™ Help Centre, you may email to cyber999@cybersecurity.my. Follow us on social networks: www.facebook.com ("CyberSecurity Malaysia" fan page) and www.twitter.com/cybersecuritymy

For further enquiries about this document, please feel free to call +603-89460999, Mohd Shamil Mohd Yusoff (ext: 0895) or shamil@cybersecurity.my / Sandra Isnaji (ext: 0867) or sandra@cybersecurity.my

CyberSecurity Malaysia
T +603 8946 0999
F +603 8946 0888