MEDIA RELEASE

25 September 2014
FOR IMMEDIATE RELEASE

COMPUTER FINANCIAL MALWARE IS NOW ON SMARTPHONES TOO

CyberSecurity Malaysia issued advisory and guidelines to ensure continued safe use of Maybank2u and CIMB Clicks

Kuala Lumpur, 25 September 2014 – The national cyber security specialist agency under the Ministry of Science, Technology and Innovation (MOSTI) issued an alert to inform Maybank2U and CIMB Clicks users who use Internet Banking.

"The cyber attackers are using the Zeus Malware Family to infect computers and subsequently trick the users to collect their mobile phone numbers. The attacker will then send SMS that has link to download the malware and install in the mobile phone. However, Zeus Trojan is a known banker malware that infect computers with purpose to steal banking credentials from victims." said Dr. Amirudin Abdul Wahab, Chief Executive Officer of CyberSecurity Malaysia.

"We are not asking users to stop using Maybank2U and CIMB Clicks. Maybank2U and CIMB Clicks are still safe. People should continue to do Internet Banking on their computers as well as their Android smartphones. But they need to be aware of this threat, and take certain precautions. We have published an advisory on our technical website (http://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/1002/index.html) and social media." he added.

"Please disregard the viral SMS or social media messages that are currently spreading, which are requesting users not to used Maybank2U and CIMBclicks. The message is misleading and not true. Please do not believe and forward viral SMS/social media messages that contain misleading information of bank services. Contact CyberSecurity Malaysia via emel to cyber999@cybersecurity.my to verify such information or to seek our assistance." Dr. Amirudin advises Internet Users.

The guidelines and best practices below are included in the advisory released by CyberSecurity Malaysia earlier.

For users of personal computers or laptop:

i. Install robust anti-virus, anti-spyware and firewall software on your computer and other devices and configure it to update regularly.

ii. Perform regular scans of your systems for malware and other risks.

iii. Operating system providers such as Microsoft, periodically releases updates and patches that improve the security of your operating system. You should periodically check for these updates and keep your system current or configure it to do so

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

automatically.

iv. When accessing to online banking, make sure there is no pop-up/window that requires personal info such as credit card number, smartphone platform (Android/iOS) etc. Do not enter those information if requested by the popup.

v. Use only a dedicated computer or laptop to do online banking

vi. If you suspect your bank account has been compromised or spot any activity you have not authorized, please notify your banking provider immediately.

vii. Please ensure you logout properly at the end of each session by clicking log-out button. Do not exit by simply closing the browser window.

viii. If you come across anything suspicious when you do banking online such as unusual web pages asking for banking information, notify your bank provider immediately.

ix. Never respond to any email/advertisements requesting you to provide your login details or login via a link sent in an email/applications. The bank will never send you a mail or provide links in any applications like that, and such a request is likely to be a phishing attempt.

In preventing Phishing incidents, Banks / Financial Institutions we would like to advise internet users to install Anti-phishing browser add-ons such as "DontPhishMe" that can help to alert and prevent users from visiting phishing websites and prevent them from disclosing their credential on the phishing websites;

Note: Users can download "DontPhishMe" from MyCERT website at: http://www.mycert.org.my/en/

For Smartphone Users:

i. Verify an app's permission and the app's author or publisher before installing it.

ii. Do not click on adware or suspicious URL sent through SMS/messaging services. Malicious program could be attached to collect user's information.

iii. Since URL on mobile site appears differently from desktop browser, make sure to verify it first.

iv. Always run a reputable anti-virus on your smartphone/mobile devices, and keep it up to date regularly.

v. Do not use public Wi-Fi networks for bank transactions and turn off Bluetooth connection when not in use. These can be open windows for eavesdroppers intercepting the transaction or installing spyware and other malware on user's smartphone/tablet.

vi. Update the operating system and applications on smartphone/tablet, including the browser, in order to avoid any malicious exploits of security holes in out-dates versions.

vii. Do not root or otherwise 'Jailbreak' your phone; avoid side loading (installing from non-official sources) when you can. If you do install Android software from a source other than the Market, be sure that it is coming from a reputable source.

We would like to advise Internet users to reporting any cyber security incidents to CyberSecurity Malaysia's Cyber999 Help Centre through various channels as follows:

- Email: cyber999@cybersecurity.my
- Call 1-300-88-2999 (during office hour) or +6019-2665850 (24 hours)
- SMS: Type <CYBER999 REPORT> <YOUR EMAIL> <REPORT>, and send to 15888
- Fax: +603 - 8945 3442
- Online reporting:
  Go to www.mycert.org.my
  or www.cybersecurity.my
  or www.cybersafe.my
  or http://www.mycert.org.my/report_incidents/online_form.html

~ 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

Untuk pertanyaan lanjut mengenai dokumen ini, sila hubungi +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