MEDIA RELEASE

14 NOVEMBER 2018

FOR IMMEDIATE RELEASE

USERS ARE ADVISED TO BE ALERT ON RANSOMWARE ATTACK

Seri Kembangan (14 November 2018) – CyberSecurity Malaysia, the national cyber security specialist and technical centre under the purview of the Ministry of Communications and Multimedia Malaysia recommends users and network administrators to take the following preventive measures to protect their computers and networks from ransomware infection:-

- Employ data backup and recovery plan for all critical information - perform regular backups to limit the impact of data or system loss and to expedite the recovery process. Ideally, keep data on a separate device, and backups should be stored offline;
- Use application whitelisting to help prevent malicious software and unapproved programs from running;
- Keep your Operating System, Software, Java, Shockwave and Flash up-to-date as exploit kits rely on vulnerabilities on the client machine to get malware to execute. Ensure these are patched with the latest updates to reduce the number of exploitable entry points available to an attacker;
- Maintain up-to-date anti-virus software and scan all software downloaded from the Internet prior to executing;
- Restrict users' ability (permissions) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services;
- Avoid enabling macros from email attachments. If user opens the attachment and enables macros, embedded code will execute the malware on the machine. For enterprises or organizations, it may be best to block email messages with attachments from suspicious sources;
- Do not follow unsolicited Web links in emails.

CyberSecurity Malaysia
(726630-U)

Best Brand Internet Security 2008 & 2009
ISMS CERTIFIED TO ISO/IEC 27001:2013 CERT. NO.: AR 4656
MS ISO/IEC 17025 TESTING SAMM NO. 456 (MySEF LABORATORY)
MSC MALAYSIA Status Company
Best Child Online Protection Website

T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

Securing Our Cyberspace

If you are a victim of ransomware, you are advised to remove the malware from the infected computer and observe the following advises:-

- Isolate the infected server from the network;
- Run an updated version of anti-virus software to scan, detect and remove the malware from the infected server;
- It is recommended to change all online account passwords and network passwords after removing the system from the network. Change all system passwords once the malware is removed from the system;
- Re-scan the computer using an updated version of anti-virus software to confirm the computer is clean;
- Once the computer is confirmed clean and running an updated version of anti-virus software, re-connect the computer to the network;
- Restore the encrypted files from backup.

Meanwhile, users are advised to be aware with the latest security announcements and follow best practice security policies to determine the safety of the data and networked systems.

Users can contact us for further enquiries through the following channels:

- E-mail: cyber999@cybersecurity.my or mycert@mycert.org.my
- Phone: 1-300-88-2999 (*monitored during business hours*)
- Fax: +603 8945 3442
- Mobile: +6019 266 5850 (*24x7 call incident reporting*)
- SMS: CYBER999 report email complaint to 15888
- Cyber999 Mobile Apps: IOS Users or Android Users

~ End ~

Issued by CyberSecurity Malaysia. For further enquiries about this document, please email: media@cybersecurity.my or call +603-89926888, Mohd Shamil Mohd Yusoff (ext: 6978) or Zul Akmal Abdul Manan (ext: 6945)