KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

CyberSecurity MALAYSIA
An agency under MOSTI

MEDIA RELEASE

13 May 2017
FOR IMMEDIATE RELEASE

CYBERSECURITY MALAYSIA ISSUES ALERT ON 'WANNACRY RANSOMWARE'

SERI KEMBANGAN (13 MAY 2017) – CyberSecurity Malaysia, the national cyber security specialist agency under the Ministry of Science, Technology, and Innovation (MOSTI), today issued an alert on ransomware attack known as 'WanaCrypt0r 2.0'.

The ransomware uses a vulnerability first revealed to the public as part of a leaked stash of NSA-related documents to infect Windows PCs and encrypt their contents before demanding a ransom for the key to decrypt the encrypted files. The co-ordinated attack had managed to infect large numbers of computers across the health service around the world after it was first noticed by security researchers on 12 May 2017, in part due to its ability to spread within networks from PC to PC.

According to Dato' Dr. Haji Amirudin Abdul Wahab, Chief Executive Officer, CyberSecurity Malaysia, the ransomware attack used Server Message Block (SMB) exploit leaked by the Shadow Brokers. The malware may spread to vulnerable systems through a security hole in Windows that has been recently patched by Microsoft. In view of this attack, we have recently released an advisory alert to highlight steps and suggestion to address Shadow Brokers exploits.

"In the meantime, we would like to urge system administrators to patch their systems as soon as possible and keep their users aware of the new ransomware in order to prevent them to open suspicious emails/files. Currently, CyberSecurity Malaysia is monitoring the situation of the ransomware attack in Malaysia and will take necessary action by providing technical assistance to the affected organizations and individual users on remediation and preventions through our Cyber999 service" added Dato' Dr. Amirudin.

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

System administrators and internet users may take the following preventive measures to protect their computer from ransomware infection:

i. Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline;
ii. Maintain up-to-date anti-virus software;
iii. Keep operating system and software up-to-date regularly with the latest patches;
iv. Do not follow unsolicited web links in email;
v. Be extra careful when opening email attachments;
vi. Follow best and safe practices when browsing the web.

Ransomware is a malicious malware that blocks access to a computer or its data and demands money to release it. When a computer is infected, the ransomware typically contacts a central server for the information it needs to activate and then begins encrypting files on the infected computer with that information. Once all the files are encrypted, it posts a message asking for payment to decrypt the files and threatens to destroy the information if it doesn't get paid, often with a timer attached to ramp up the pressure. Most ransomware is spread hidden within Word documents, PDFs and other files normally sent via email, or through a secondary infection on computers already affected by viruses that offer a back door for further attacks.

Ransomware does not only target home users, businesses can also become infected with ransomware which can have negative consequences, including:

- Temporary or permanent loss of sensitive or proprietary information;
- Disruption to regular operations;
- Financial losses incurred to restore systems and files; and
- Potential harm to an organization's reputation.

Advisories and alerts recently issued by CyberSecurity Malaysia that needs immediate patches as a measure to prevent ransomware infection are:
https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1262/index.html
https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1255/index.html".

For further enquiries, please contact CyberSecurity Malaysia (MyCERT) through the following channels:

- E-mail : cyber999@cybersecurity.my or mycert@mycert.org.my
- Phone : 1-300-88-2999
- Fax : +603 89453442
- Mobile : +6019 2665850 (24x7 call incident reporting)
- SMS : Cyber999 report email complaint to 15888

For additional information, visit our website at http://www.cybersecurity.my and for general inquiry, email to info@cybersecurity.my.

Stay connected with us on social networks: facebook/ CyberSecurityMalaysia, twitter/cybersecuritymy, youtube/cybersecuritymy, instagram/CyberSecurity_Malaysia.

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