勒索软件 Wannacry

Image Source: Kaspersky.com

By Bernard Kan
@HKCERT
HKCERT Wannacry 最新數字

As at 17/5 14:00

• About 400 enquiry
• Over 30 infected reports
• Most are Windows 7 household broadband users
• Most are unpatched machines, about half of them has no AV and no broadband router
Broadband host without Internet router

Attack traffic

Wannacry
Infected hosts

Internet

Direct Internet Connection
Public IP address

HKPC®
HKCERT
Broadband host with Internet router

Wannacry
Infected hosts

Attack traffic

Internet router with
Public IP address

Internet Connection
Private IP address
Security Blog
Beware of WannaCry Ransomware Spreading

Release Date: 14 / 05 / 2017

Contents
- High Risk Areas
- Preventive measures for individual users
- Preventive measure for enterprise users
- Other preventive measures
- What if my computer is infected with WannaCry ransomware?
- Reference

Download PDF version of the following guideline here.

An new ransomware variant called WannaCry (also known as WannaCrypt, Wanna Decryptor) was spreading and impacted many important public services overseas by encrypting the important files for ransom.

Ransomware is a type of malware which will encrypt victim's files and request a ransom in order to recover the files. The latest new "WannaCry" variant is the first ransomware which can spread throughout home or office network and infect much more devices. Individual and enterprise users are advised to take extra precautions to prevent its infection and the data loss.
多謝