勒索軟件Wannacry

Image Source: Kaspersky.com

HKCERT

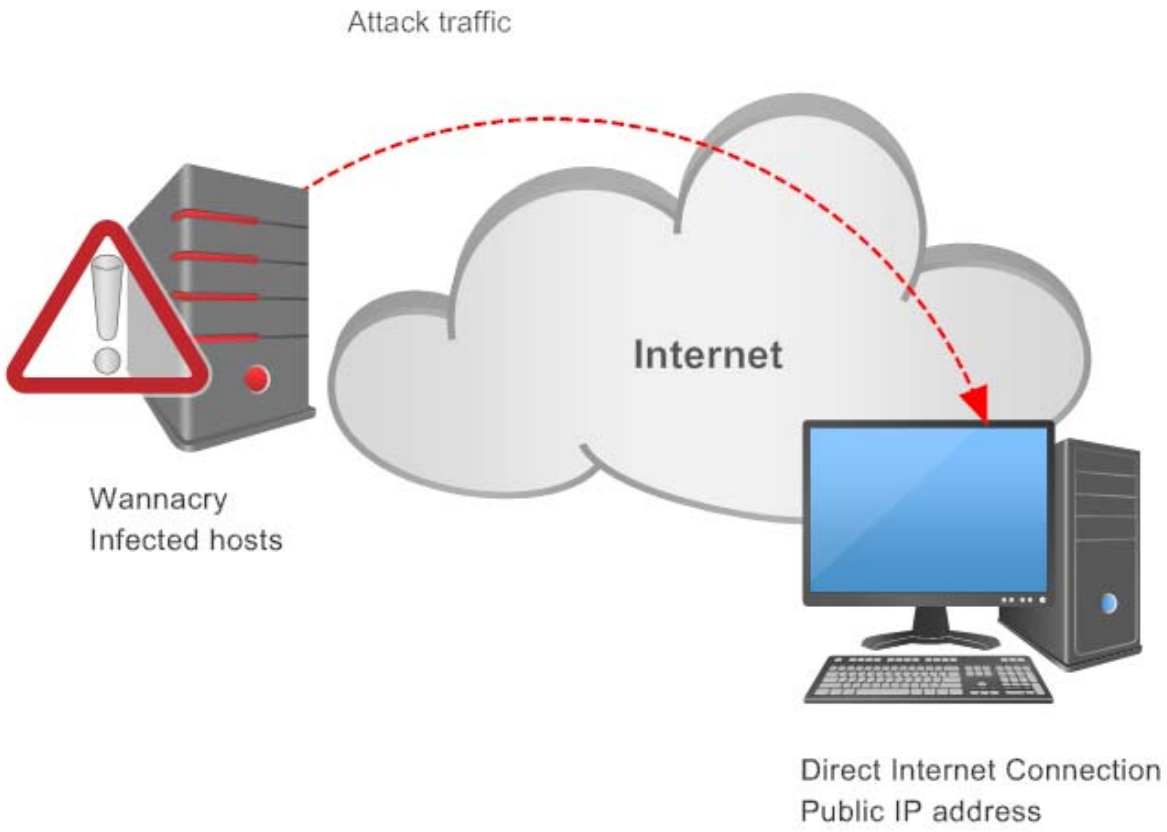
By Bernard Kan
@HKCERT

HKCERT Wannacry 最新數字

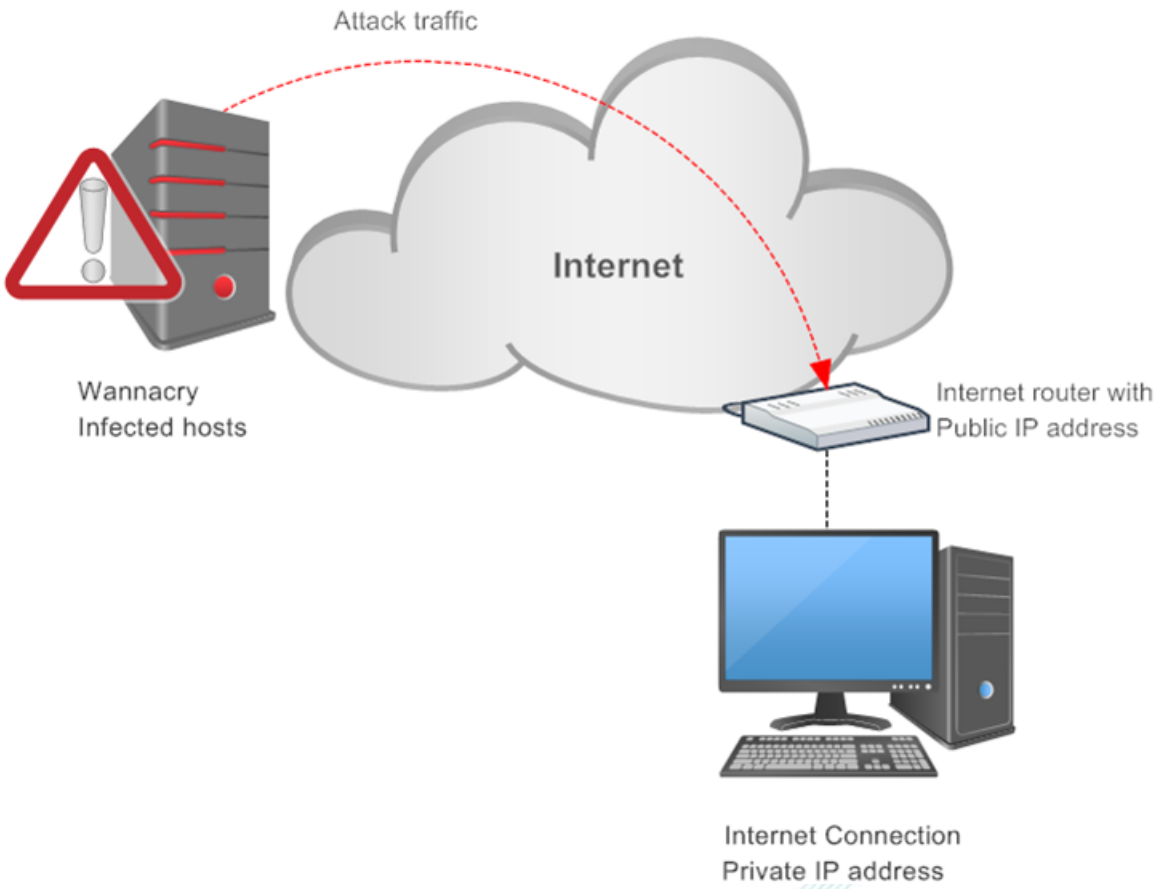
As at 17/5 14:00

- 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



Broadband host with Internet router




Secure | https://www.hkcert.org
Sitemap | Verify the identity of this website
中文 | English
AAA
Search...
HKCERT
Hong Kong Computer Emergency Response Team Coordination Centre
About Us
Alerts & News
Services
Publications
Resources
Mobile
RSS
Getting Help
Incident Reporting
Useful Resources
Subscription
Receiving timely security alert information. Securing your system better
Subscribe Now
Highlight
Favourite Security Reads of the Week (28 Apr 2017)
Security Bulletin
Apple Products Multiple Vulnerabilities 2017/05/16
PostgreSQL Multiple Vulnerabilities 2017/05/15
WannaCry (WannaCrypt) Ransomware Encrypts Victim Data 2017/05/13
IBM WebSphere Application Server Multiple Vulnerabilities 2017/05/11
Cisco Webex Meetings Server Information Disclosure Vulnerability 2017/05/11
WannaCry Ransomware
Beware of Crypto Ransomware 提防加密勒索軟件
Defense Against Malware for Small Businesses
Event Highlight
"Smart Home, Safe Living" 1- 2017/07/07

HKPC

HKCERT

Security Blog

Beware of WannaCry Ransomware Spreading

Release Date: 14 / 05 / 2017

Last Update: 15 / 05 / 2017

Contents

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

HKCERT
Website: www.hkcert.org
Email: hkcert@hkcert.org
Tel: 81056060