香港電腦保安事故協調中心緊急呼籲
防範加密勒索軟件「WannaCry 」

本文 URL: https://www.hkcert.org/my_url/zh/blog/17051401

一款名為 WannaCry (亦稱 WannaCrypt 或 Wanna Decryptor) 的新型勒索軟件正在散佈，透過加密檔案進行勒索，以致影響海外多個重要公眾服務。

勒索軟件是一種透過加密受害人檔案及要求贖款以取回檔案的惡意軟件。WannaCry 是第一款能在家用或辦公室網絡散佈，並感染更多裝置的新型勒索軟件。個人及企業用戶需更小心採取防範措施以防止受感染及損失數據。

高風險範圍

HKCERT 接到兩宗事故報告，並有共同特徵：

1. 該兩名用戶直接連接電腦至互聯網而沒有使用寬頻路由器或設置防火牆。
2. 他們的電腦沒有安裝最新的保安更新程式。

高風險範圍 1：電腦直接連線到互聯網

HKCERT 提醒用戶直接連線到互聯網會將電腦曝露於互聯網而受攻擊。用戶應使用寬頻路由器或防火牆。低階寬頻路由器能提供簡單的 NAT 防火牆功能以阻擋外來攻擊。

高風險範圍 2：辦公室網絡內有未作保安更新的電腦

即使在辦公室網絡設置了防火牆，只能保護網絡不受外界的網絡掃描或入侵。若受感染的電腦連接到網絡，該電腦會掃描及攻擊其他未作保安更新的內部電腦。因此必須確保連接到辦公室網絡的電腦已安裝了最新的保安更新程式。

個人用戶的防範措施

1. 設置寬頻路由器供裝置連線到互聯網。不要把裝置直接連接到互聯網。
2. 在沒有互聯網連線的情況下，使用其他儲存裝置 USB 「手指」或外置硬碟進行備份。
3. 備份後立即移除儲存裝置。
4. 安裝最新的保安更新程式。

   各版本視窗修補程式下載連結(亦提供視窗 XP、視窗伺服器 2003 及視窗 8 特別修補程式):
   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
   (捲動至頁底)
5. 安裝防毒軟件或互聯網保安應用程式並更新病毒資料庫。

辦公室網絡用戶的防範措施

1. 確保已設置防火牆或寬頻路由器，且沒有開放 SMB 服務（技術上要關閉 TCP 139 和 445 端口）。
2. 在不連上互聯網連線的情況下，為需要數據備份的電腦，使用 USB 「手指」或外置硬碟進行備份，備份後立即移除儲存裝置。
3. 為辦公室網絡的電腦執行 Windows Update，安裝 Microsoft 安全公告 MS17-010 保安修補程式。
   - 先為桌面電腦執行，然後逐部連接手提電腦執行。外攜手提電腦除非能確定未受惡意軟件感染，否則禁止其連接辦公室網絡。

   視窗修補程式下載連結 (亦提供視窗 XP、視窗伺服器 2003 及視窗 8 特別修補程式):
   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
   (捲動至頁底)

先為桌面電腦執行，然後逐部連接手提電腦執行。外攜手提電腦除非能確定未受惡意軟件感染，否則禁止其連接辦公室網絡。

4. IT 管理員參照以下步驟停用 SMBv1:
   https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
5. 以後定期為備份數據，並保留離線備份。

其他防護措施

- 進行離線備份 (即是使用其他儲存裝置，備份後立即移除)。
- 不要打開任何可疑電郵內的連結或附件。
- 確保電腦已有基本保護，包括啟用及執行視窗更新、安裝已有最新病毒資料庫的防毒軟件及啟用視窗防火牆。

若電腦受 WannaCry 勒索軟件感染，應怎麼辦？

- 若電腦已受感染，應立即停止網絡連線進行隔離，並移除連接到該電腦的儲存裝置。
- 立即隔離其他電腦及檔案伺服器。最迅速的做法是關閉網絡交換器（network switch）以停止大規模擴散。
- 未清理惡意軟件前不要開啟任何檔案。
- 我們不建議繳交贖款。

有關微軟保安更新的技術問題，可參閱 https://wp.me/p5FsOe-4lu，或致電 (852) 2388 9600 與微軟香港客戶服務熱線查詢。

香港電腦保安事故協調中心
網址: https://www.hkcert.org
電郵: hkcert@hkcert.org
熱線: (852) 8105 6060

Beware of WannaCry Ransomware Spreading

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.

High Risk Areas

HKCERT received two incident reports. They share two commonalities:

1. Both users connected their computers directly to the Internet, without using a broadband router nor a firewall
2. Their computers were not applied the latest security update.

High Risk Area 1: Computers connecting directly to the Internet

HKCERT warned the users that direct connection to the Internet can expose the computer to attacks. They should have a broadband router or a firewall. A low-end broadband router can provide a simple NAT firewall function to block incoming attack.

High Risk Area 2: Unpatched Computers in the Office Network

Even if you have a firewall at the office network, you can only protect your network from scanning and exploit from the external. If an infected computer connected to your network, it will scan and attack other internal computers which have not been patched. So you must ensure computers connecting to the office network have applied the latest security update.

Preventive measures for individual users

1. Set up a broadband router for connecting your devices to the Internet. Prevent your devices from connecting to the Internet directly.
2. Perform backup on another storage device such as USB thumb drive, external hard disk, when not connected to the Internet.
   Remove your storage device right after backup.
3. Apply latest Windows security update.

> Direct links for downloading patch for individual Windows versions are provided (exceptional Windows XP, Windows Server 2003 and Windows 8 patch also released):
> https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
> (scroll down to the bottom)

4. Ensure that anti-virus or Internet security application is installed, and have its signature updated.

Preventive measure for office network users

1. Ensure that there is a firewall or broadband router in place, and SMB service is not open (close TCP ports 139 and 445 technically).
2. Perform backup on another storage device such as USB thumb drive, external hard disk, when not connected to the Internet.
   Remove your storage device right after backup.
3. Run Windows Update for computers in the office network, and install Microsoft Security Bulletin MS17-010 security patch.

   > Direct links for downloading patch for individual Windows versions are provided (exceptional Windows XP, Windows Server 2003 and Windows 8 patch also released):
   > https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
   > (scroll down to the bottom)

   Apply the above for desktop computers first, then corporate laptop computers one by one.
   If you cannot verify whether an outsider laptop computer is free from malware, do not allow it to connect to the office network.
4. When all done, connect corporate laptop computers one by one and apply Windows security update.
5. IT administrator proceed to disable SMBv1 for computers using the following steps:
   https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
6. If you cannot verify whether an outsider laptop computer is free from malware, do not allow it to connect to the office network.

Other preventive measures

- Perform offline backup (i.e. backup in another storage device, disconnect it after backup).
- Do not open links and attachment in any suspicious emails.
- Ensure that your computer have baseline protection, i.e. enable and run Windows Update, install anti-virus application with signature updated, enable Windows Firewall.

What if my computer is infected with WannaCry ransomware?

- Once infected, isolate the infected computer immediately from the network, and disconnect from external storage.
- Also isolate other computers and file servers from the network immediately. The quickest way is to turn off the network switch.
- Do not open any file before removing the malware.
- We do not recommend paying the ransom.

If you have technical questions on Microsoft patch, you can refer to this URL: https://wp.me/p5FsOe-4lu , or call their customer hotline (852) 2388 9600.

HKCERT
Website: https://www.hkcert.org
Email: hkcert@hkcert.org
Hotline: (852) 8105 6060