# Conficker Worm

本中心提供 Conficker worm 網頁自我檢測回報系統，讓使用者可以自行檢測個人電腦是否感染，並回報檢測狀況。

- 清華大學 Conficker 自我檢測回報系統 NEW

## Conficker 簡介

2008年10月23日微軟緊急發佈了重大安全性更新: MS08-067之後，透過該漏洞的木馬程式Trojans出現在網路上，同時首隻利用該漏洞的蠕蟲 Conficker 現身，並且對未完成更新的使用者進行感染。目前 Conficker 已有多個變種產生並且影響相當數量的使用者。

Conficker 利用下述多種方式進行攻擊：

- 攻擊未安裝 MS08-067 重大安全性更新的電腦
- 攻擊使用弱密碼的網路分享，然後將惡意程式複製到網路分享資料夾再感染其他使用者
- 透過可攜式儲存設備（如USB擴大感染範圍

當電腦一旦感染 Conficker 後，會有下列行為進行自我保護：

- 修補其利用的漏洞，阻擋其他惡意軟體進入
- 關閉 Windows 自動更新
- 關閉安全模式
- 禁止使用者連線至資訊安全相關的網站，導致受感染的電腦無法下載或更新軟體
- 移除電腦中與防毒或安全分析工具相關字串的處理程序

現在大多數防毒軟體都能檢測及阻擋此蠕蟲。如果有定時更新作業系統、防毒軟體及病毒碼，被感染的風險便會減低。

## 線上檢測

- 清華大學 Conficker 自我檢測回報系統 NEW
- University of Bonn: Conficker Online Infection Indicator NEW
- Conficker Eye Chart（Conficker肉眼檢測法）英文版

## 遠端檢測工具

- Simple Conficker Scanner v2 NEW
- Nmap NEW
- McAfee Conficker Detection Tool

## 移除工具

如果您已經檢測出感染 Conficker 蠕蟲，那麼您點擊下列的連結應該會出現錯誤。請使用另一台正常未感

染的電腦來下載。

- Symantec W32.Downadup Removal Tool 下載使用說明
- Kaspersky KK_v3.4.7.zip使用說明
- Trend Micro Fixtool 下載使用說明

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
**https://net.nthu.edu.tw/netsys/security:malware_conficker**

Last update: **2009/05/08 15:18**