

# Rustock 電腦病毒 清除流程

適用對象：Microsoft Windows 作業系統

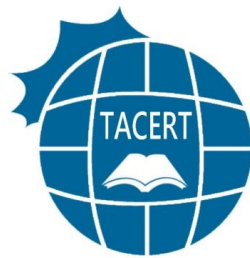
版本：1.0

日期：中華民國 100 年 4 月 20 日



## 目錄

前言 .....	3
一、 Rustock 殭屍網路簡介 .....	3
二、Rustock 電腦病毒清除流程.....	4
(一)移除被 Rustock 電腦病毒感染的程式.....	4
(二)掃描是否還有潛藏其他惡意程式.....	6
三、電腦主機的安全性建議設定 .....	8
(一)開啟微軟的自動更新功能.....	8
(二)確認是否已安裝最新系統更新檔.....	9
(三)開啟本機防火牆 .....	11
(四)更新防毒軟體的病毒碼.....	12
(五)提高密碼強度 .....	12
四、參考資料 .....	12



## 前言

本份文件的主旨在於提供受到 Rustock 電腦病毒感染的 Microsoft Windows 作業系統用戶作為移除 Rustock 電腦病毒的參考。文中所提供的工具程式以及下載位置，皆為 Microsoft 所製作及提供，詳細的操作說明以及使用方式請參考 Microsoft 的官方網站。

## 一、Rustock 殭屍網路簡介

Rustock botnet 是全世界最大的殭屍網路集團之一，由被 Rustock 電腦病毒感染的主機所組成，主要的犯罪活動為利用受到惡意程式感染的主機發送垃圾郵件。根據報導，一台受到 Rustock 電腦病毒感染的主機，可以在一天之內發送 24 萬封的垃圾郵件，嚴重影響他人的電子郵件信箱並耗損大量網路頻寬；此外，這些受到 Rustock 電腦病毒感染的主機上的個人資料也非常有可能會遭到犯罪集團的竊取以及冒用，侵害使用者的權益；再者，這些遭到 Rustock 電腦病毒感染的主機也很有可能會被網路犯罪集團控制，進而發動大規模的網路攻擊，例如：分散式阻斷式服務攻擊(Distributed Denial of Service)。

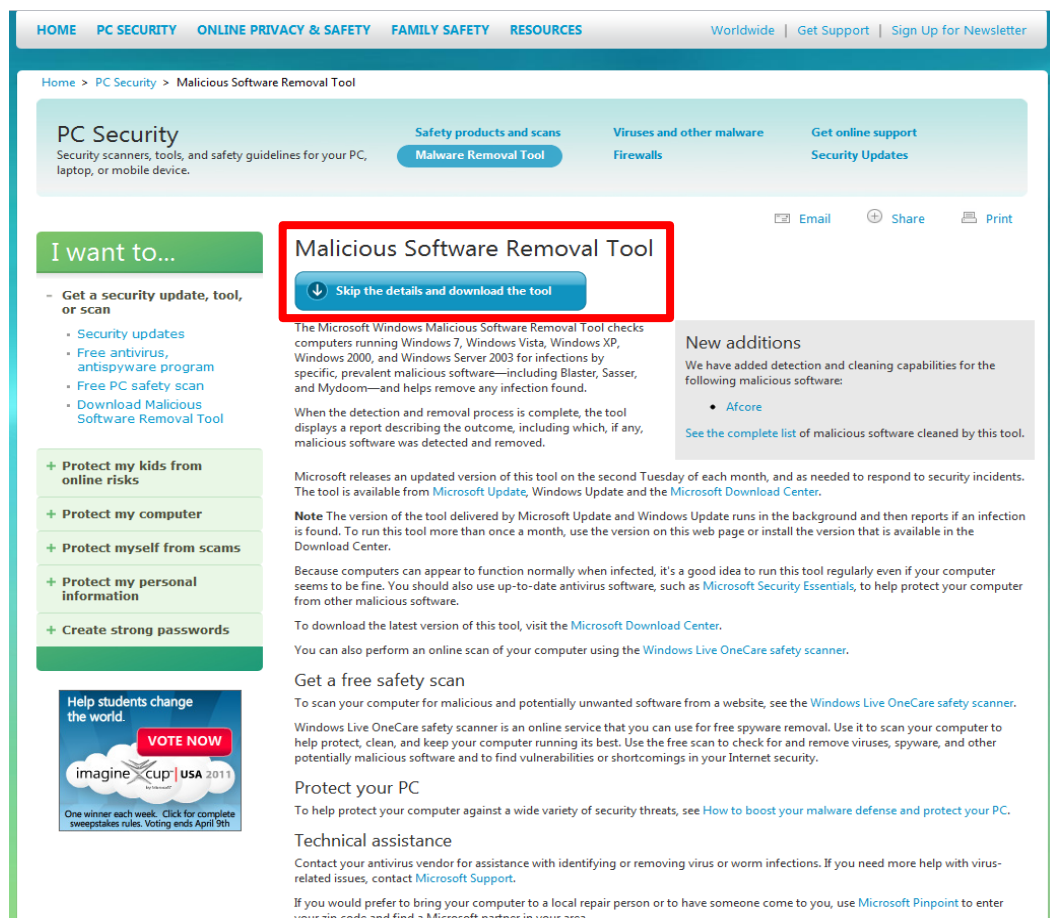
## 二、Rustock 電腦病毒清除流程

### (一) 移除被 Rustock 電腦病毒感染的程式

Microsoft Windows 的使用者可以利用微軟官方釋出的惡意程式移除工具進行 Rustock 病毒的移除。

- 下載 Microsoft Windows 惡意程式移除工具(Malicious Software Removal Tool)：

<http://www.microsoft.com/security/pc-security/malware-removal.aspx>



HOME PC SECURITY ONLINE PRIVACY & SAFETY FAMILY SAFETY RESOURCES Worldwide | Get Support | Sign Up for Newsletter

Home > PC Security > Malicious Software Removal Tool

**PC Security**  
Security scanners, tools, and safety guidelines for your PC, laptop, or mobile device.

Safety products and scans  
**Malware Removal Tool**

Viruses and other malware  
Firewalls

Get online support  
Security Updates

Email Share Print

**I want to...**

- Get a security update, tool, or scan
  - Security updates
  - Free antivirus, antispyware program
  - Free PC safety scan
  - Download Malicious Software Removal Tool
- Protect my kids from online risks
- Protect my computer
- Protect myself from scams
- Protect my personal information
- Create strong passwords

**Malicious Software Removal Tool**

Skip the details and download the tool

The Microsoft Windows Malicious Software Removal Tool checks computers running Windows 7, Windows Vista, Windows XP, Windows 2000, and Windows Server 2003 for infections by specific, prevalent malicious software—including Blaster, Sasser, and Mydoom—and helps remove any infection found.

When the detection and removal process is complete, the tool displays a report describing the outcome, including which, if any, malicious software was detected and removed.

Microsoft releases an updated version of this tool on the second Tuesday of each month, and as needed to respond to security incidents. The tool is available from [Microsoft Update](#), Windows Update and the [Microsoft Download Center](#).

**Note** The version of the tool delivered by Microsoft Update and Windows Update runs in the background and then reports if an infection is found. To run this tool more than once a month, use the version on this web page or install the version that is available in the Download Center.

Because computers can appear to function normally when infected, it's a good idea to run this tool regularly even if your computer seems to be fine. You should also use up-to-date antivirus software, such as [Microsoft Security Essentials](#), to help protect your computer from other malicious software.

To download the latest version of this tool, visit the [Microsoft Download Center](#).

You can also perform an online scan of your computer using the [Windows Live OneCare safety scanner](#).

**Get a free safety scan**

To scan your computer for malicious and potentially unwanted software from a website, see the [Windows Live OneCare safety scanner](#).

Windows Live OneCare safety scanner is an online service that you can use for free spyware removal. Use it to scan your computer to help protect, clean, and keep your computer running its best. Use the free scan to check for and remove viruses, spyware, and other potentially malicious software and to find vulnerabilities or shortcomings in your Internet security.

**Protect your PC**

To help protect your computer against a wide variety of security threats, see [How to boost your malware defense and protect your PC](#).

**Technical assistance**

Contact your antivirus vendor for assistance with identifying or removing virus or worm infections. If you need more help with virus-related issues, contact [Microsoft Support](#).

If you would prefer to bring your computer to a local repair person or to have someone come to you, use [Microsoft Pinpoint](#) to enter your zip code and find a Microsoft partner in your area.

**New additions**

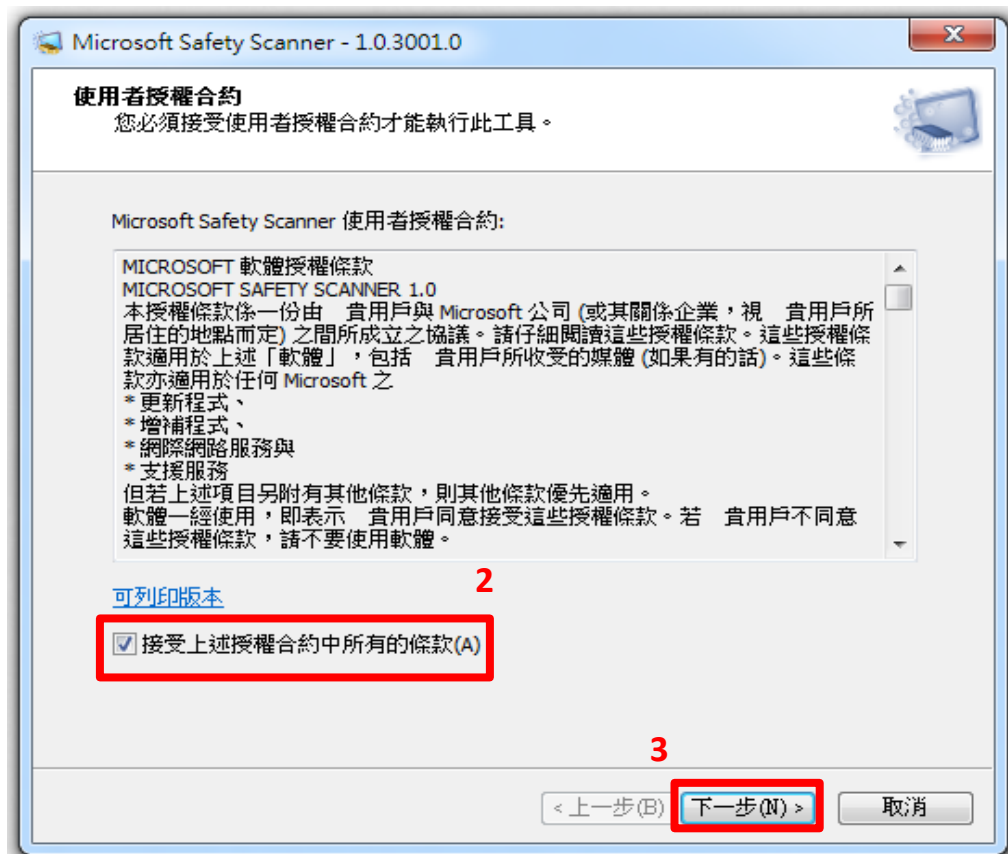
We have added detection and cleaning capabilities for the following malicious software:

- Afcore

[See the complete list](#) of malicious software cleaned by this tool.

Help students change the world.  
**VOTE NOW**  
imagineCup USA 2011  
One winner each week. Click for complete sweepstakes rules. Voting ends April 9th.

- 執行 Microsoft Windows 惡意程式移除工具：





## (二)掃描是否還有潛藏其他惡意程式

Microsoft Windows 的使用者可以利用微軟官方釋出的電腦安全掃描工具進行主機安全性檢查，確認是否有其他病毒、間諜軟體存在。

- 下載 Microsoft Safety Scanner：

<http://www.microsoft.com/security/scanner/zh-tw/default.aspx>

## Microsoft Safety Scanner

取得免費的電腦安全掃描

繁體中文 (台灣)

**立即下載**

需要在不同 PC 上執行？[選取您的版本。](#)

### Microsoft Safety Scanner

您認為您的電腦有病毒嗎？

Microsoft Safety Scanner 是免費下載的安全性工具，您可隨時用來掃描電腦並移除病毒、間諜軟體和其他惡意軟體。它可與您現有的防毒軟體搭配運作。

請注意：Microsoft Safety Scanner 將於下載後的第 10 天到期。若要使用最新的反惡意程式碼定義檔重新執行掃描，請重新下載並執行 Microsoft Safety Scanner。

Microsoft Safety Scanner 並不可取代提供持續防護的防毒軟體程式。

若需要即時防護以協助您的家用電腦或小型商用電腦防禦病毒、間諜軟體和其他惡意軟體，請下載 [Microsoft Security Essentials](#)。

### 說明和資源

- Microsoft Safety Scanner 疑難排解
- Microsoft 病毒與安全性解決方案中心
- Microsoft Consumer Security Support Center (英文)
- Microsoft Safety and Security Center (英文)
- Microsoft Malware Protection Center (英文)
- Microsoft Security Intelligence Report (英文)
- Microsoft Safety Scanner 系統需求
- Microsoft Safety Scanner 隱私權聲明
- Microsoft Safety Scanner 授權合約

### 擁有更安全的電腦和 Web 瀏覽體驗

Microsoft®

#### Security Essentials

正版 Windows 客戶可免費訂閱 Microsoft Security Essentials，此為獲獎的防毒軟體可協助您防護電腦。



取得最新更安全的 Microsoft 瀏覽器 (內含 SmartScreen Filter)，讓您在 Web 上瀏覽時避開社交工程惡意軟體釣魚網站以及線上詐騙。



Windows Live Family Safety 可協助您透過個人化的規則，讓您的小孩在使用網路網路時受到更好的保護。您也可以取得工具來監視他們正在線上進行什麼活動。

### 重大桌上型電腦威脅

- Worm:Win32/Conficker.B
- Worm:Win32/Conficker.C
- Virus:Win32/Sality.AM
- Virus:Win32/Sality.AT
- Rogue:Win32/Winwebsec
- Trojan:Win32/Rimecud.A
- Virus:Win32/Virut.BN
- Rogue:Win32/FakeSysinfo
- Backdoor:Win32/FlyAgent.F
- Virus:Win32/Slugin.Adlil

[詳細資訊](#)

管理設定檔 | 連絡我們 | 使用規定 | 商標 | 隱私權聲明

**Microsoft**

© 2011 Microsoft

## ● 執行 Microsoft Safety Scanner

Microsoft Safety Scanner - 1.0.3001.0

**歡迎使用 Microsoft Safety Scanner**

此工具會掃描及移除病毒、間諜軟體及其他潛在的垃圾軟體

按一下 [下一步] 即可掃描並協助移除電腦中的病毒、間諜軟體及其他潛在的垃圾軟體。

此工具並不能取代反惡意程式碼解決方案。若要協助保護您的電腦，您應該使用反惡意程式碼解決方案。如需詳細資訊，請參閱[保護您的電腦](#)。

如需隱私權的資訊，請參閱 [Microsoft Safety Scanner 隱私權聲明](#)。

< 上一步(B) **下一步(N) >** 取消

## 三、電腦主機的安全性建議設定

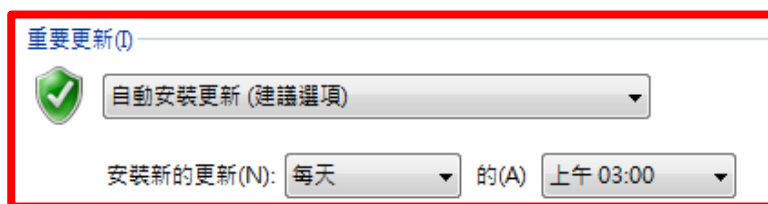
### (一)開啟微軟的自動更新功能

『控制台』->『系統及安全性』->『Windows Update』->『變更設定』


選擇 Windows 安裝更新的方式。

當您的電腦上線時，Windows 可以使用這些設定自動檢查並安裝重要更新。有可用的更新時，您也可以在此關機之前安裝。

[自動更新如何協助我？](#)



重要更新(I)

 自動安裝更新 (建議選項)

安裝新的更新(N): 每天 的(A) 上午 03:00

建議的更新

☒ 提供建議更新與接收重要更新的方式相同(R)

可以安裝更新的人員

☒ 允許所有使用者在此電腦安裝更新(U)

Microsoft Update

☒ 提供給我 Microsoft 產品的更新，並在我更新 Windows 時檢查新的選用 Microsoft 軟體(G)

軟體通知

☒ 顯示有新 Microsoft 軟體可用的詳細通知(S)

注意: Windows Update 可能會在檢查其他更新之前，先自動進行自我更新。請閱讀我們的[線上隱私權聲明](#)。

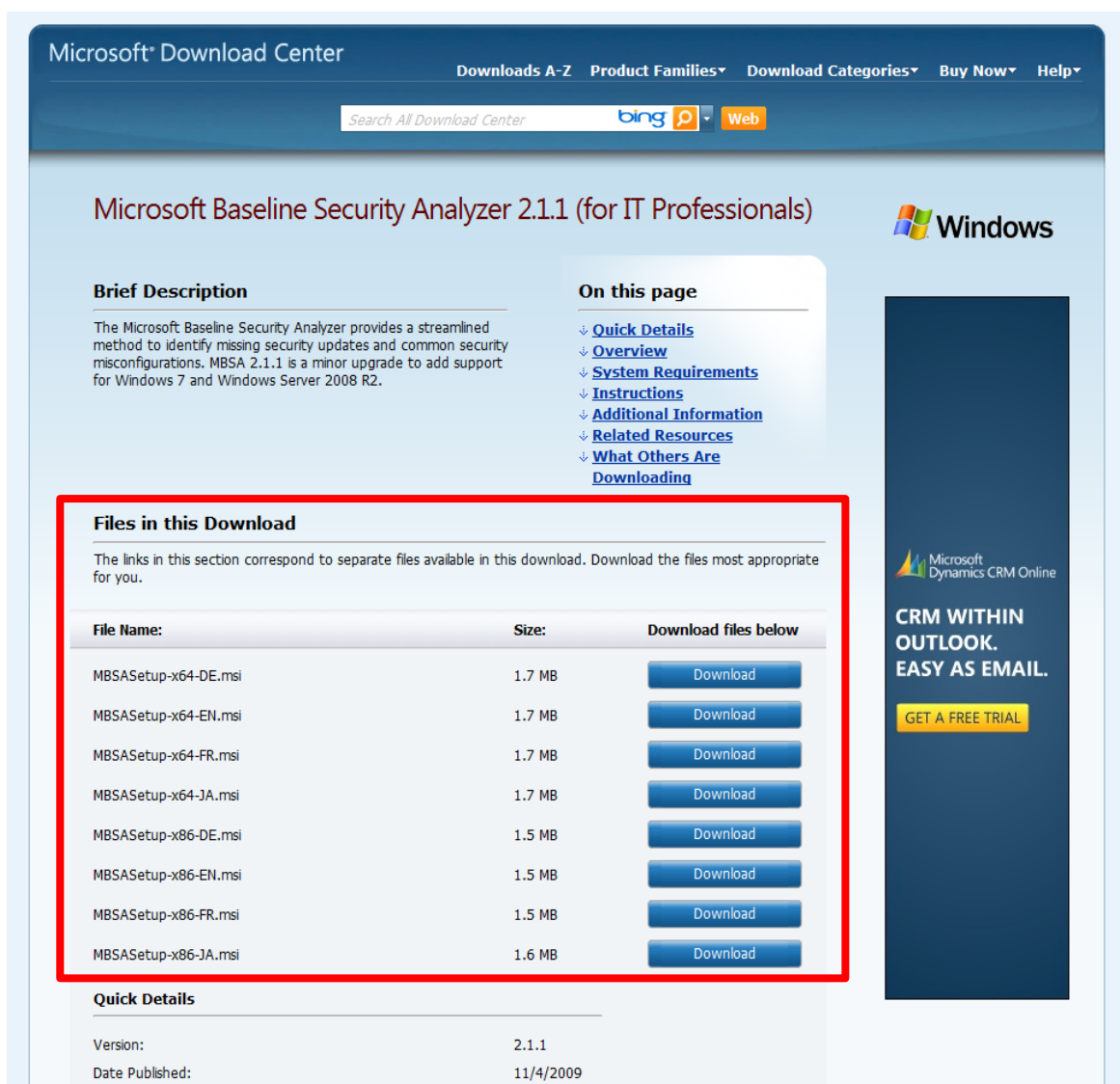


## (二) 確認是否已安裝最新系統更新檔

使用 Microsoft Baseline Security Analyzer 檢查本機作業系統及其他主要應用程式是否已安裝最新的安全性修正檔：

- 下載 Microsoft Baseline Security Analyzer：

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=b1e76bbe-71df-41e8-8b52-c871d012ba78&displaylang=en>



Microsoft® Download Center

Downloads A-Z Product Families Download Categories Buy Now Help

Search All Download Center

Microsoft Baseline Security Analyzer 2.1.1 (for IT Professionals)

Windows

**Brief Description**

The Microsoft Baseline Security Analyzer provides a streamlined method to identify missing security updates and common security misconfigurations. MBSA 2.1.1 is a minor upgrade to add support for Windows 7 and Windows Server 2008 R2.

**On this page**

- Quick Details
- Overview
- System Requirements
- Instructions
- Additional Information
- Related Resources
- What Others Are Downloading

**Files in this Download**

The links in this section correspond to separate files available in this download. Download the files most appropriate for you.

File Name:	Size:	Download files below
MBSASetup-x64-DE.msi	1.7 MB	<a href="#">Download</a>
MBSASetup-x64-EN.msi	1.7 MB	<a href="#">Download</a>
MBSASetup-x64-FR.msi	1.7 MB	<a href="#">Download</a>
MBSASetup-x64-JA.msi	1.7 MB	<a href="#">Download</a>
MBSASetup-x86-DE.msi	1.5 MB	<a href="#">Download</a>
MBSASetup-x86-EN.msi	1.5 MB	<a href="#">Download</a>
MBSASetup-x86-FR.msi	1.5 MB	<a href="#">Download</a>
MBSASetup-x86-JA.msi	1.6 MB	<a href="#">Download</a>

**Quick Details**

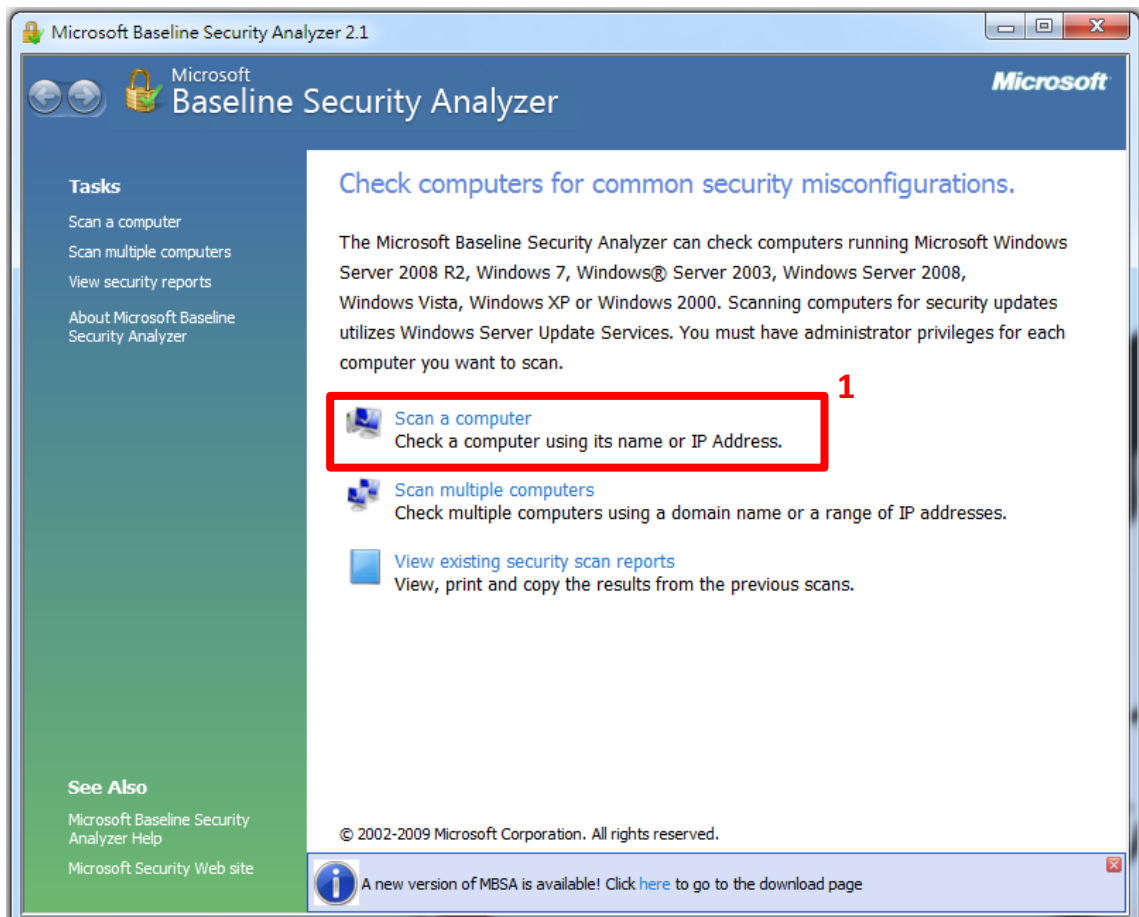
Version: 2.1.1  
Date Published: 11/4/2009

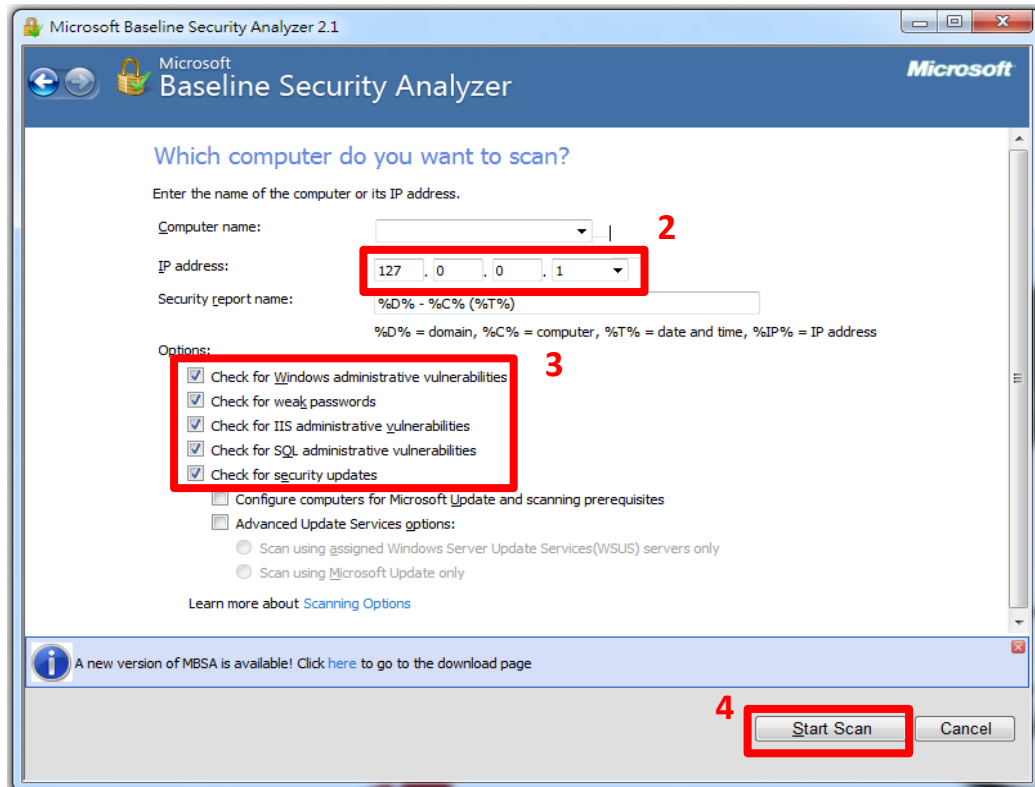
Microsoft Dynamics CRM Online

CRM WITHIN OUTLOOK. EASY AS EMAIL.

GET A FREE TRIAL

- 執行 Microsoft Baseline Security Analyzer(詳細的使用方式，請參考文件 MBSA 安裝暨使用說明)，並依據 Microsoft Baseline Security Analyzer 的掃描結果，尤其是標示為紅色的重大系統安全性更新部份，立刻進行修補。





### (三)開啟本機防火牆

『控制台』->『系統及安全性』->『Windows 防火牆』。

#### 自訂每個網路類型的設定

您可以為您使用的每個網路位置類型修改防火牆設定。

什麼是網路位置?

#### 家用或工作場所 (私人) 網路位置設定

- ☒ 開啟 Windows 防火牆
  - ☐ 封鎖所有連入連線，包括允許的程式清單中的連入連線
  - ☒ 當 Windows 防火牆封鎖新的程式時請通知我
- ☐ 關閉 Windows 防火牆 (不建議)

#### 公用網路位置設定

- ☒ 開啟 Windows 防火牆
  - ☐ 封鎖所有連入連線，包括允許的程式清單中的連入連線
  - ☒ 當 Windows 防火牆封鎖新的程式時請通知我
- ☐ 關閉 Windows 防火牆 (不建議)



## (四)更新防毒軟體的病毒碼

每日更新電腦主機安裝的防毒軟體的病毒碼。

## (五)提高密碼強度

- 增加密碼複雜性：建議混合使用英文字母、阿拉伯數字以及特殊字元，增加密碼的複雜性。
- 加強密碼長度：主機管理員與使用者的密碼強度建議至少需有 8 碼，並定期更換。

## 四、參考資料

- Microsoft on Rustock,  
[http://blogs.technet.com/b/microsoft\\_on\\_the\\_issues/archive/2011/03/18/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx](http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/03/18/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx)
- Rustock Recovery Steps,  
<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fRustock>
- Microsoft Malicious Software Removal Tool,  
<http://www.microsoft.com/security/pc-security/malware-removal.aspx>
- Microsoft Safety Scanner,  
<http://www.microsoft.com/security/scanner/zh-tw/default.aspx>
- Microsoft Baseline Security Analyzer,  
<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=b1e76bbe-71df-41e8-8b52-c871d012ba78&displaylang=en>