

W32.Barcalid, W32.Barcalid!inf 病毒 !!

針對 Barcalid 這隻病毒, 賽門鐵克於 9/1 當天 Release 病毒定義程式, 已經可以偵測/刪除該病毒, 但該病毒擴散及感染的動作很快, 若是沒有全部的電腦都清除乾淨時, 會不斷的透過網芳及檔案傳遞 (USB) 時感染其他電腦。

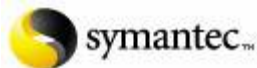
建議各位立刻採取以下的行動:

(1) 針對來不及更新病毒定義程式而遭感染的電腦:

- a. 提交病毒 Sample 以供分析。
已購買金級 (Symantec Gold Maintain, 5x8) 客戶:
<https://submit.symantec.com/gold>
已購買白金級 (Symantec Platinum Maintain, 7x24) 客戶:
<https://submit.symantec.com/platinum>
- b. 已購買金級或白金級技術支援的客戶, 請撥打 Symantec Support 專線 **00801 861032** 建立 Case, 以利追蹤及提供更多的客戶支援。
- c. 隔離已中毒的電腦的網路連線, 用安全模式開機後, 更新病毒定義檔, 執行全系統掃描。
- d. 使用安全模式掃毒完之後, 再執行一次全系統掃描。
- e. 使用防火牆阻止到以下網站的連線, 避免該病毒連線到這些網站而下載新的變種。
[\[http://www.clubzio.com/File/Gam\]](http://www.clubzio.com/File/Gam)
[\[http://www.gallup.co.kr/news/Gam\]](http://www.gallup.co.kr/news/Gam)
[\[http://200.61.224.41/news/gam\]](http://200.61.224.41/news/gam)
[\[http://www.darcania.com/down/Gam\]](http://www.darcania.com/down/Gam)
[\[http://www.shuaiad.com/down/6\]](http://www.shuaiad.com/down/6)
[\[http://www.shuaidd.com/script/src/ad0\]](http://www.shuaidd.com/script/src/ad0)
[\[http://www.jackeryy.com/script/adco\]](http://www.jackeryy.com/script/adco)
[\[http://www.fkall.com\]](http://www.fkall.com)
- f. 刪除已感染的檔案, 用乾淨的原始檔案還原。
- g. 關閉檔案分享, 阻止感染來源, 若有一定要共用的程式, 應設成唯讀, 避免有中毒的電腦感染它, 立刻再感染其他的電腦, 造成疫情爆發。
- h. 啟動/安裝個人防火牆, 阻止病毒的感染或攻擊。
- i. Windows2000 系統管理員帳號 (Administrator) 不可使用空白密碼, 避免病毒利用系統預設的 Share Folder (如: C\$, Admin\$, D\$) 去感染
- j. 更新 Windows 的修補程式: MS06-014. 此一病毒利用微軟的漏洞, 當使用者使用 IE 瀏覽被植入木馬的網頁時, 會將木馬程式安裝到使用者的電腦上。若是沒有安裝這個修補程式, 攻擊者做一下木馬的變種, 將持續不斷的造成公司感染木馬。
<http://www.microsoft.com/taiwan/technet/security/bulletin/MS06-014.mspx>

(2) 未感染的電腦 (預防感染):

- a. 關閉檔案分享, 阻止感染來源, 若有一定要共用的程式, 應設成唯讀, 避免有中毒的電腦感染它, 立刻再感染其他的電腦, 造成疫情爆發。
- b. 啟動/安裝個人防火牆, 阻止病毒的感染或攻擊。
- c. Windows2000 系統管理員帳號 (Administrator) 不可使用空白密碼, 避免病毒用系統預設的 Share Folder (如: C\$, Admin\$, D\$) 去感染。
- d. 更新 Windows 的修補程式: MS06-014. 此一病毒利用微軟的漏洞, 當使用者使用 IE 瀏覽被植入木馬的網頁時, 會將木馬程式安裝到使用者的電腦上。若是沒有安裝這個修補程式, 攻擊者做一下木馬的變種, 將持續不斷的造成公司感染木馬。
<http://www.microsoft.com/taiwan/technet/security/bulletin/MS06-014.mspx>



(3) 檔案修復工具:

當使用者有被感染的檔案，無法以乾淨的檔案復原時，可以使用賽門鐵克針對這隻病毒的檔案修復工具修復。

<< 下載: >>

<https://fileshare.symantec.com/>

User: bacalid_tool

Pass: w32Bacalid

<< 使用方法 >>:

- a. 使用安全模式開機，執行此修復工具。
- b. 掃描完成之後，使用正常開機後，再執行一次。
- c. 執行完之後，檢視 Log 檔，看是否都修復成功。
- d. 若有已經被病毒破壞的檔案，將無法完全修復，需要用乾淨的檔案覆蓋還原。

注意: 詳細使用說明，請參閱底下附件說明

更多病毒資訊:

http://www.symantec.com/security_response/writeup.jsp?docid=2006-090109-5610-99&tabid=1

若有任何問題，請與您的賽門鐵克經銷商連絡。

關於賽門鐵克

賽門鐵克公司是全球解決方案的領導廠商，致力為個人和企業用戶提供資訊的安全性、可用性和完整性。賽門鐵克企業總部設在美國加州Cupertino，營運據點遍及全球 40 多個國家。欲知更多相關資訊，歡迎瀏覽賽門鐵克企業網站<http://www.symantec.com>。

台灣賽門鐵克股份有限公司

台北市 105 南京東路五段 188 號 2 樓之 7

電話 +886-2-8761-5800 傳真 +886-2-2742-2838

附件說明: W32.Bacalid 移除工具(v1.03)

Symantec 已完成 W32.Bacalid 移除工具(v1.03)。此工具已通過 QA 檢查程序，透過此工具可以讓客戶大大縮減修復的時間，有效控制感染情形。但因為受限於有些感染檔案程式本身已遭破壞，可能無法修復，因此本工具並無法 100% 清除還原中毒檔案。如果屬於這種狀況，請以乾淨原始檔案覆蓋被感染檔案。

使用此工具時，須注意底下幾點事項：

- 此工具在安全模式下運作，清除效果最好。假如在正常模式下運作，此工具無法保證可以成功清除。客戶應該在安全模式下，執行一次掃描清除動作。完成後，重開機，再一次進入安全模式執行第二次清除工作，如此可以確保清除的最佳結果。
- 此工具可能無法修復某些檔案，有可能是檔案已遭病毒破壞，或是檔案感染已超過此工具能處理的範圍，此情況建議以乾淨原始檔案覆蓋被感染的檔案。
- 任何檔案無法修復，將被紀錄在此工具的 Log 檔。使用此移除工具掃描後，客戶可以用 SAV 對系統作一次完整掃描，讓 SAV 將無法修復的檔案刪除或隔離。注意：病毒可能已破壞某些檔案，這些檔案無法修復。

最後，此工具可能無法修復所有感染檔案，但感染情形將被控制住。任何感染的檔案，雖無法修復但可透過 SAV 即時防護功能，偵測刪除或隔離中毒檔案。