您真的了解電腦病毒嗎？ 勒索病毒示範

http://www.seekinfo.com.tw/
更新日期：2015/12/23

有些人的防毒策略是這樣… 公司內的電腦，伺服器或某些重要的電腦會安裝防毒軟體，其餘的電腦就隨便它。又或者某些電腦也不管它是不是有裝防毒，或者舊版本用了幾年也不想更新。也許您認為那些電腦不重要，但是它卻是很大的風險來源。

想必這一年來大家都有聽過勒索病毒，甚至直接或間接見過勒索病毒，本文就以勒索病毒來示範，您可能沒想過的問題。

我使用的勒索病毒樣本並不是很新的版本，幾乎各家防毒軟體都能偵測。這裡有檢測的結果 – https://goo.gl/U7PIK5

我假設的場景是這樣… 在一部 File Server 上安裝了最新版本的 Kaspersky Endpoint Security 10 SP1 MR1 v10.2.2.10535，病毒碼也更新到最新版本，從上面網址的資料來看，也確定卡巴斯基可以偵測這個病毒，當然也確定這部 Server 本身是沒有中毒的。照很多人的想法，應該是認為這部 Server 是安全的，至少對這個已經能偵測的勒索病毒來說是安全的。

之後我找了一部電腦，沒有安裝防毒軟體，並且故意讓它中毒。猜猜看，會發生什麼事？我錄製了一小段影片，網址是 https://youtu.be/Byl8iLU9ITg 一鏡到底，完全沒有剪接。

影片一開始，可以看到這部電腦安裝了卡巴斯基，在 Share 資料夾裡面有幾個檔案，我逐一打開來，證明檔案都是好的。時間從 00:50 開始，畫面是靜止的，這時我到另外一部電腦去執行前面說的勒索病毒。時間來到 02:20 的時候，突然 Share 資料夾裡的檔案被改變了，多了一個通知付款的圖檔 HELP_YOUR_FILES.PNG，其他檔案打不開了。而卡巴斯基呢？完全沒有反應。

強調一下，這不是卡巴斯基的問題，換作其他防毒軟體仍然是相同的結果。因為勒索軟體並沒有將含有病毒碼的檔案複製到 Server，所以防毒軟體根本無從偵測。從 Server 的角度來看，它就只是寫入一些亂碼的檔案，所以防毒軟體根本不會有動作。

結論是：防毒是全面性的，沒有重要或不重要電腦的區別。當您忽略某些電腦，其實正好為病毒開啟了一扇門。

如果對本文的內容有疑問，請聯絡**席克資訊 TEL: 04-22132276**