CPE17 Autorun Killer
User Manual
คู่มือการใช้งานโปรแกรมป้องกันไวรัสจาก Autorun

Revision 2.0: 18 February 2010

http://www.cpe17.com

1. คุณสมบัติของโปรแกรม

- โปรแกรมนี้สร้างขึ้นเพื่อแก้ไขปัญหาต่างๆ ที่เกิดขึ้นจากการกระทำของไวรัสที่ใช้ Flash หรือ Thumb drive หรือ เป็นหลัก ซึ่งต้องใช้ควบคู่กับ antivirus software
- ป้องกันปัญหาที่ต้นเหตุ โดยบล็อกการทำงานของ autorun จากทุกทาง ทั้ง ไดรฟ์ถอดเปลี่ยนได้ทุกแบบ ไดรฟ์ CD/DVD หรือ เน็ตเวิร์กไดรฟ์ก็ตาม
- โปรแกรมเขียนขึ้นด้วยภาษา C++ แท้ มีขนาดเล็ก ~0.1MB ทำงานรวดเร็ว
- ไม่กินทรัพยากรมากนัก สามารถใช้ได้แม้แต่เครื่องที่ความเร็วช้าก็ตาม
- ดับเบิ้ลคลิกเพียงครั้งเดียว โปรแกรมก็พร้อมจะทำงานทันที ไม่ต้องติดตั้งให้เสียเวลา
- สามารถเปลี่ยนแปลง option ได้โดย เลือกให้ลบอัตโนมัติ หรือถามก่อนทุกครั้ง, มีเสียงเตือนหรือไม่, แสดงหน้าจอผลลัพธ์หรือไม่, จะตรวจ CD/DVD หรือไม่
- โปรแกรมสามารถแก้ไขปัญหาต่างๆ ที่ถูกไวรัสปิดไป ทั้ง regedit, taskmanager, folder option และการกระทำต่างๆ รวมทั้ง title bar ของ ie
- สามารถป้องกันการรัน exe และการประมวลผล autorun file เฉพาะ windows xp ขึ้นไป
- สามารถสร้างภูมิคุ้มกันให้กับไดร์ฟ flash ได้
- แก้ hacked by ... ได้ด้วย
- ปิด auto run แบบ ถาวร อัตโนมัติ เพื่อไม่ให้เกิดปัญหาขึ้นอีก
- ป้องกันแบบถาวร ไม่ต้องอัพเดตฐานข้อมูลไวรัสบ่อยๆ
- เพิ่มการทำงานพิเศษ สำหรับเครื่องที่ติดไวรัสไปแล้ว โดยมีฟังก์ชันพยายามติดตามฆ่าไวรัส โดยอัตโนมัติ
- สามารถตั้งให้ตรวจสอบ และลบไฟล์ที่เป็นรูปแบบของไวรัส เช่น ชื่อเดียวกับโฟลเดอร์ หรือไวรัสที่ copy ตัวเองซ้ำ โดยอัตโนมัติได้
- เพิ่มคุณสมบัติพิเศษ kill process ไวรัสในเครื่องได้เอง ผ่านเมนู kill process in memory
- ใช้เป็นตัวเปิด/ปิด ถาด CD/DVD ได้ด้วย
- พิสูจน์ความน่าใช้ ได้ทันที ที่ Google หรือ ที่ YaHOO! มั่นใจได้ในคุณภาพ มีคนบอกใช้แล้วบอกต่อมากมาย ^^"

2. ระบบที่ต้องการ

- Windows 95/98/ME/NT/2000/XP/Vista/7 (สำหรับ vista ขึ้นไป กรุณารันด้วยสิทธิ administrator ถ้าต้องการเช็ก HDD)

ระบบที่ทดสอบแล้วว่าใช้ได้แน่นอนจากตัวผู้พัฒนา คือ

- Windows XP
- Vista (อาจมีปัญหาเรื่องภาษาในบางเครื่อง)
- Windows 7

3. วิธีการติดตั้ง

*** ถ้ามีเวอร์ชันเดิมอยู่ให้ข้ามไปอ่านส่วนถอนการติดตั้งก่อน

- ต้องการใช้งานใน flash drive

ให้ copy โปรแกรม ลงไป ใน flash drive และดับเบิ้ลคลิกเพื่อเรียกใช้งานโปรแกรม

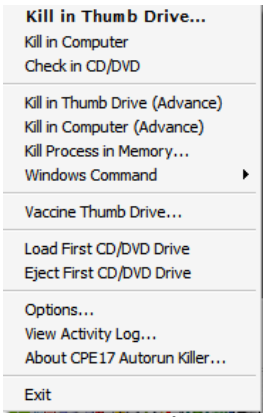
- ต้องการใช้งานในเครื่องเพื่อใช้งานคุณสมบัติปกป้องตลอดเวลา

ให้ copy โปรแกรม ลงไป ในเครื่องตัวเอง เช่น C:\Program files\CPE17AntiAutorun1580.exe และดับเบิ้ลคลิกเพื่อเรียกใช้งานโปรแกรม

4. วิธีการถอนการติดตั้ง

- ให้ปิดโปรแกรมก่อนโดย ดูที่ไอคอนด้านล่างขวาบริเวณใกล้ๆ นาฬิกา ดังรูป

- คลิกขวาที่ไอคอนดังกล่าว เลือก exit ตามรูป

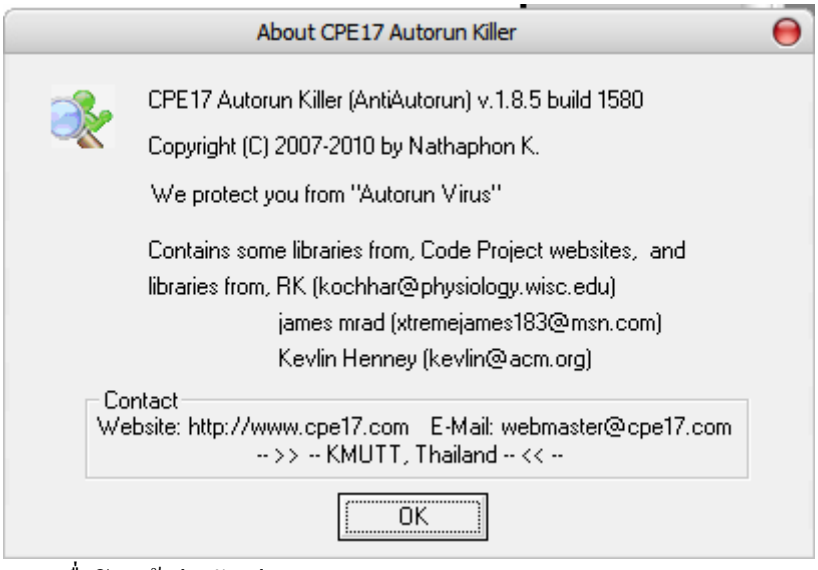


- ตอบ yes เพื่อ ปิดโปรแกรม
- จากนั้นลบไฟล์โปรแกรมทิ้งไปได้เลย

*** กรณีอัพเกรด version ใหม่ ให้นำโปรแกรม version ใหม่ไปวางที่ต้องการ แล้วดับเบิ้ลคลิกเพื่อรันโปรแกรม

5. วิธีตรวจสอบ version ของโปรแกรม และตรวจสอบตำแหน่งการรันของโปรแกรม

ให้คลิกขวาที่ไอคอนโปรแกรม เลือกเมนู About CPE17 Autorun Killer… จะปรากฏหน้าต่างดังรูป



คลิก OK เพื่อปิดหน้าต่างดังกล่าว

*** ในหน้าต่างนี้ จะแสดงรูปแบบการรันของโปรแกรมด้วย หากถูกรันจาก flash drive จะปรากฏข้อความบอกตำแหน่ง drive ที่รันขึ้นมา ในบรรทัดแรก บริเวณท้ายบรรทัด

6. วิธีการใช้งานแบบปกติ

โปรแกรมนี้จะทำงานแบบอัตโนมัติทันทีที่เสียบ อุปกรณ์ตระกูล flash drive, thumb drive, รวมทั้ง CD/DVD และ Network Drive ที่ map เข้ามา

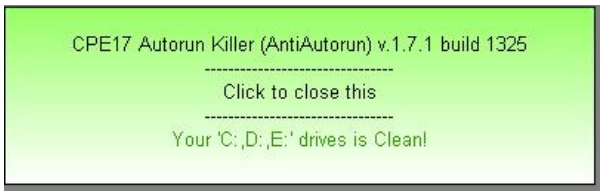
- ถ้าโปรแกรมตรวจพบระบบที่ทำงานอัตโนมัติ จะทำการลบไฟล์สั่งงานนั้นทันที (autorun.inf) และลบไฟล์ที่ไฟล์สั่งงานเรียกใช้ให้อัตโนมัติ (กรณีติดตั้งครั้งแรก และยังไม่ได้ปรับแต่งค่าใดๆ) จากนั้น จะแสดงผลการทำงานเป็นสีแดง ซึ่งหมายความว่าตรวจพบไฟล์ต้องสงสัยเป็นไวรัส และจัดการลบเป็นที่เรียบร้อยแล้วดังรูป

หลังจากนั้น เมื่อคุณคลิกที่ข้อความดังกล่าวเพื่อปิดหน้าจอแล้ว โปรแกรมจะหน่วงเวลาเพื่อรอตรวจสอบไวรัสซ้ำอีกครั้ง ถ้าหากไม่พบอะไรจะแสดงข้อความ

ซึ่งหมายความว่า น่าจะไม่มีไวรัสแล้ว แต่ให้ลองสังเกตดูอีกทีว่าเครื่องมีอะไรผิดปกติอีกหรือไม่ แต่ถ้าหากพบไวรัสอีกครั้ง แสดงว่ามีโอกาสเป็นไปได้สูงมาก ว่าเครื่องจะติดไวรัสอยู่ โปรแกรมจะแสดงข้อความเป็นสีแดงเพื่อเตือนให้ตรวจสอบ ในกรณีนี้ แนะนำให้ไปที่ http://www.cpe17.com/hijackthis และทำ

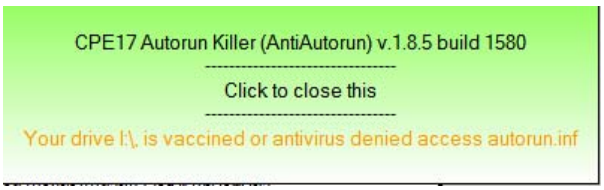
ตามขั้นตอนในหน้านั้น ซึ่งจะใช้โปรแกรม HijackThis ทำการตรวจสอบแบบ manual โดยมีฐานข้อมูลบนเว็บเพื่อระบุว่าไฟล์ใดในเครื่องน่าจะเป็นไวรัส

- ถ้าไม่พบสิ่งผิดปกติ จะแสดงผลการทำงานเป็นสีเขียว คือไม่พบไฟล์อะไรต้องสงสัย ดังรูป

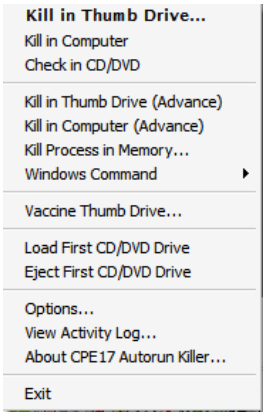


*** ค่ามาตรฐาน จะปิดการตรวจสอบไฟล์ขั้นสูงไว้เนื่องจาก จะเสียเวลาในการตรวจสอบมากขึ้น หากต้องการเปิดใช้ให้อ่านส่วนถัดไป

- ถ้าพบไฟล์ autorun.inf หรือ folder autorun.inf ที่เกิดจากการทำงานของระบบ vaccine ทั้งของโปรแกรมเองหรือโปรแกรมอื่นในสายเดียวกัน หรือโปรแกรมป้องกันไวรัสห้ามการเข้าถึงไฟล์ไว้ จะแสดงผลการทำงานเป็นสีเขียว แต่มีข้อความระบุเป็นสีเหลือง ดังรูป



7. วิธีการใช้งานแบบขั้นสูง



จากรูปจะพบเมนูต่างๆ มากมาย ซึ่งเป็นที่รวมฟังก์ชันต่างๆ ของโปรแกรม
เมนูดังกล่าวสามารถพบได้โดยคลิกขวาที่ไอคอนของโปรแกรมใกล้ๆ นาฬิกา

7.1 Kill in Thumb Drive จะเรียกการทำงานเหมือนการ ตรวจอัตโนมัติซ้ำอีกครั้ง กรณีหากไม่แน่ใจสามารถตรวจสอบซ้ำอีกครั้งได้จากเมนูนี้

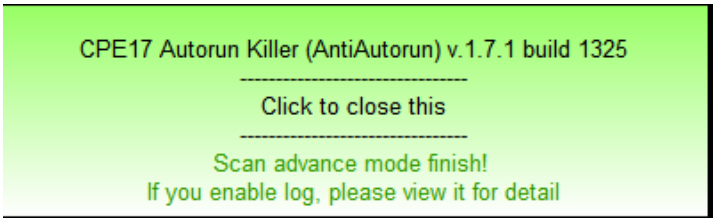
7.2 Kill in Computer ใช้สำหรับตรวจหาไฟล์ที่น่าจะเป็นไวรัส autorun ภายใน Hard disk กรณีติดไวรัสไปแล้ว ฯลฯ ซึ่งจะปรากฏผลต่างๆ เหมือนข้อแรก

7.3 Check in CD/DVD ใช้สำหรับตรวจหาไฟล์ที่น่าจะเป็นไวรัส autorun ภายใน CD/DVD แต่เนื่องจาก drive ดังกล่าว ไม่สามารถเขียนทับได้ดังนั้น จึงแสดงผลต่างกันกับสองข้อแรก โดย

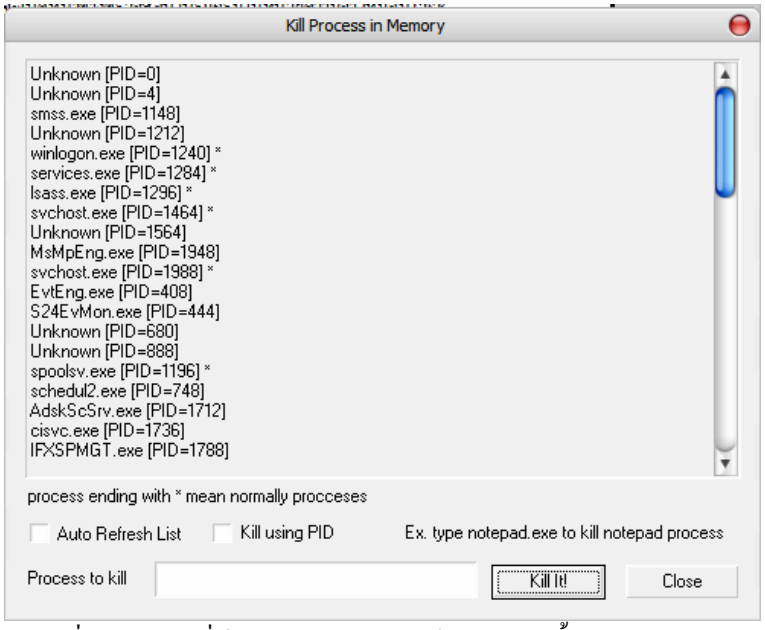
จะเสนอทางเลือกให้สามทางเมื่อเจอไฟล์ต้องสงสัย คือ ดีดแผ่นออก, เปิดดูแผ่นผ่านคำสั่งพิเศษเพื่อหลีกเลี่ยงการติดไวรัส และปล่อยผ่านไปในกรณีแน่ใจว่าแผ่นดังกล่าว

7.4 Kill in Thumb Drive (advance) ใช้สำหรับตรวจหาไฟล์ ตาม 7.1 และเพิ่มการตรวจหาไฟล์ที่ใกล้เคียงกับที่เจอใน 7.1 รวมทั้ง ไฟล์ที่มีชื่อตามโฟลเดอร์ต่างๆ

7.5 Kill in Computer (advance) เหมือน 7.4 แต่เปลี่ยนมาตรวจจากภายใน hard disk แทน ซึ่งจะใช้เวลานานกว่า



7.6 Kill Process in memory จะเปิดหน้าต่างตรวจสอบโปรแกรมในหน่วยความจำ เหมือน task manager ขนาดจิ๋ว ใช้ในกรณีไม่สามารถเปิด Task manager ขึ้นมาได้เลยด้วยวิธีอื่นๆ ซึ่งสามารถเลือก kill process ต่างๆ ได้โดยตรงจากที่นี่ (อาจฆ่าไม่ได้บางตัว เนื่องจากโปรแกรมนี้รันในสิทธิที่ต่ำกว่าโปรแกรมที่จะฆ่า) ดังรูป



ให้คุณ copy ชื่อโปรแกรมที่ต้องการฆ่า จาก list ด้านบน จากนั้นนำมาวางในช่อง Process to kill แล้วกด Kill It! ซึ่งโปรแกรมจะทำการวนฆ่า process ทุกตัวที่มีชื่อเหมือนทั้งหมด ดังนั้นจึงใช้จัดการไวรัสที่มีการเรียกใช้เป็นหลายๆ process ได้เป็นอย่างดี

*** ถ้าหากคุณไม่สามารถเลือกชื่อ process ได้เนื่องจาก list มีการ refresh อยู่ตลอดเวลา ให้คุณคลิ๊กที่ Auto Refresh List เพื่อให้เครื่องหมายถูกออก จะเป็นการหยุด refresh list ให้คุณ copy ชื่อได้อย่างง่ายๆ

*** หาก Process มีชื่อแปลกๆ หรือพิมพ์ไม่สะดวก ให้คุณคลิกที่ Kill using PID แล้วเปลี่ยนเป็นพิมพ์ตัวเลขในวงเล็บหลังชื่อแทน ซึ่งเป็นเลขแทนตัวของ process นั้นๆ

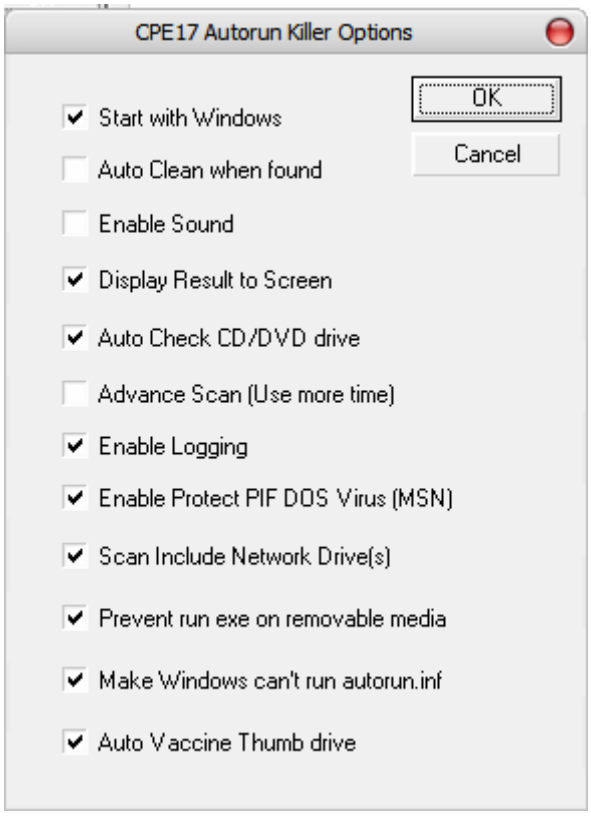
เมื่อใช้งานเสร็จแล้วสามารถปิดโดยใช้ปุ่ม Close หรือกากบาทบนขวา

7.7 Windows Command ใช้สำหรับเรียกคำวสั่งพื้นฐานต่างๆ ในเครื่องเอง เช่น Registry Editor, Task manager, System configuration, Command prompt ซึ่งมักถูกไวรัสปิดการทำงานไป ซึ่งโปรแกรมนี้สามารถทำการปลดล็อก และเรียกใช้คำสั่งดังกล่าวขึ้นมาได้โดยส่วนมาก นอกจากนั้น ยังสามารถเรียกใช้ Task manager ในโหมดพิเศษ ซึ่งมีสิทธิสูงสุดในเครื่อง คือ system (ไม่ใช่ administrator นะครับ system ใหญ่สุดในระบบ ลองดูในเว็บ Microsoft ก็ได้) เพื่อให้ได้สิทธิในการฆ่า process ไวรัสได้ง่ายขึ้นในบางกรณี

7.8 Vaccine Thumb drive คำสั่งนี้ใช้เพื่อสั่งเขียน folder autorun.inf แบบพิเศษลงใน drive ของคุณเพื่อป้องกันไม่ให้ไวรัสเขียนไฟล์ autorun ปกติได้ ซึ่งอาจป้องกันไม่ได้ 100% แต่ก็ทำให้ไวรัสระบาดได้ยากขึ้น โดยกรณีที่เรากลัวว่า เวลาเอาไดร์ฟเราเปิดที่อื่นแล้วจะติดมา

7.9 Load & Eject First CD/DVD drive คำสั่งนี้ใช้เปิด/ปิด drive CD/DVD อำนวยความสะดวก สำหรับหลายคนที่ชอบดูหนังฟังเพลง แต่จะใช้ได้เฉพาะ drive CD drive แรก เนื่องจากปกติบางเครื่องจะมี drive จำลองมากกว่า 1 แต่มักจะตั้งค่าให้ drive จริง อยู่ที่ drive แรก จึงตัดสินใจทำเป็นแบบนี้นะครับ

7.10 Option ในหน้าต่าง option จะเป็นส่วนที่ใช้ตั้งค่าโปรแกรมให้ทำงานอย่างที่คุณต้องการ โดยมีตัวเลือกดังรูป



- Start with Windows ใช้ตั้งค่าให้โปรแกรม ทำงานพร้อมการเปิดเครื่องหรือไม่ หากไม่ต้องการให้ติ๊กออกได้ (ค่ามาตรฐานติ๊กถูก)

- Auto Clean when found ใช้ตั้งค่าให้โปรแกรม ทำการลบไฟล์ที่สงสัยว่าเป็นไวรัสทันทีหรือไม่ (ค่ามาตรฐานติ๊กถูก)

- Enable Sound ใช้ตั้งค่าให้โปรแกรม เล่นเสียงเตือนเมื่อเสียบ drive หรือ พบไวรัสหรือไม่ (ค่ามาตรฐาน ปิด)

- Display Result to Screen ใช้ตั้งค่าให้โปรแกรมแสดงผลลัพธ์การทำงาน ทางหน้าจอด้วยหรือไม่ (ค่ามาตรฐานติ๊กถูก)

- Auto Check CD/DVD drive ใช้ตั้งค่าให้โปรแกรมทำการตรวจสอบไฟล์ใน drive CD/DVD ด้วยหรือไม่ เนื่องจากปัจจุบัน หนังหลายเจ้านิยมใส่ไวรัสไว้เพื่อป้องกันการ copy หนัง และจะรันโดยเราไม่รู้ตัว โปรแกรมนี้สามารถช่วยเตือนท่านได้ มันจะเตือนเมื่อเสียบแผ่นใหม่แล้วพบไฟล์ autorun (ค่ามาตรฐาน ติ๊กถูก)

- Advance Scan ใช้ตั้งค่าให้โปรแกรมจรวจสอบไฟล์เหมือน และไฟล์ชื่อเหมือนโฟลเดอร์ดดยอัตโนมัติหรือไม่ ถ้าหากเลือกไว้การสแกนแต่ละครั้งจะใช้เวลานานขึ้น ถ้าเครื่องคุณไม่แรงพอแนะนำไม่ให้เปิดการทำงานตรงนี้ แล้วถ้าต้องการตรวจสามารถเลือกจากเมนูด้านบนได้ (ค่ามาตรฐาน ปิด)

- Enable Logging ใช้ตั้งค่าให้โปรแกรม บันทึกการทำงานไว้ดูด้วย (โปรแกรมจะล้างผลทุกครั้งที่มีการตรวจครั้งใหม่) ควรเปิดไว้ แต่อาจทำให้โปรแกรมใช้หน่วยความจำเพิ่มขึ้นเล็กน้อย (ค่ามาตรฐาน ปิด)

- Enable Protect PIF DOS Virus (MSN) ป้องกันการรันไฟล์ประเภท .pif ซึ่งไวรัสทาง MSN เรียกใช้ ซึ่งถ้าหากคุณใช้งานโปรแกรม DOS รุ่นเก่าๆ อาจจะมีปัญหา ให้ปิด option นี้ (ค่ามาตรฐาน เปิด)

- Scan Include Network Drive(s) เนื่องจากมี user บางท่านไม่ต้องการให้ตรวจสอบ ไดร์ฟที่แมพ จาก network โดยอัตโนมัติ จึงทำตัวเลือกนี้ขึ้นมา โดยเวอร์ชั่นก่อนๆ จะตรวจทั้งหมด (ค่ามาตรฐานเปิด)

- Prevent run exe on removable media เพิ่ม การป้องกันการรัน ไฟล์ตระกูล exe และไฟล์พิเศษอื่นๆ ในไดร์ฟ โดย option นี้อาจมีบั๊ค ไม่มีผลในบางเครื่อง และ option นี้เกิดขึ้นเพื่อป้องกันไวรัสฉวยโอกาส สร้างตัวเองให้คล้าย folder เพื่อหลอก user แต่หากท่านต้องการใช้ไฟล์เหล่านั้น ให้มาปิด option นี้แล้วค่อยใช้งาน (ค่ามาตรฐานเปิด)

- Make Windows can’t run autorun.inf บังคับให้วินโดว์ไม่สนใจไฟล์ autorun.inf เพื่อเพิ่มความมั่นใจอีกชั้น (ค่ามาตรฐานเปิด)

- Auto Vaccine Thumb drive สั่งให้โปรแกรม ทำการ vaccine drive โดยอัตโนมัติ (อ่านรายละเอียดข้างบน) (ค่ามาตรฐานปิด)

*** หากพบข้อผิดพลาดประการใด ในเอกสารนี้ หรือในตัวโปรแกรม มีข้อสงสัยต่างๆ ไปโพสไว้ที่กระดานข่าว CPE17 Autorun Killer ได้นะครับ อยู่ที่ http://www.cpe17.com ตามลิงค์กระดานข่าวไปนะครับ
*** download version ล่าสุด ได้ที่ http://www.cpe17.com เช่นกันครับ