เรื่อง : VBS.Solow (Rundll64.dll.vbs)
เรียบเรียงโดย : กิติศักดิ์ จิรวรรณกุล นายพรินทร์ แก้วซิม และ นายปองภพ เหล่าชัยกุล
เผยแพร่เมื่อ : 15 พฤษภาคม 2550

การใช้ภาษาสคริปต์ในการเขียนเว็บเพจนั้นเป็นการเพิ่มลูกเล่นแปลกใหม่ให้กับหน้าเว็บ เพื่อให้มีความสวยงามหรือมีการทำงานหลากหลายขึ้น แทนที่เว็บเพจจะเป็นแค่หน้าที่ดูเรียบง่าย ภาษาสคริปต์ที่ได้รับความนิยมในการเขียนเว็บเพจเช่น จาวาสคริปต์ (JS) หรือ วิชวลเบสิคสคริปต์ (VBS) เป็นต้น ด้วยประโยชน์ที่มีมากมาย จึงทำให้มีผู้ที่ไม่ประสงค์ดีคิดที่จะนำเอาภาษาสคริปต์เหล่านี้ไปสร้างเครื่องมือที่ใช้โจมตีระบบเครือข่ายคอมพิวเตอร์

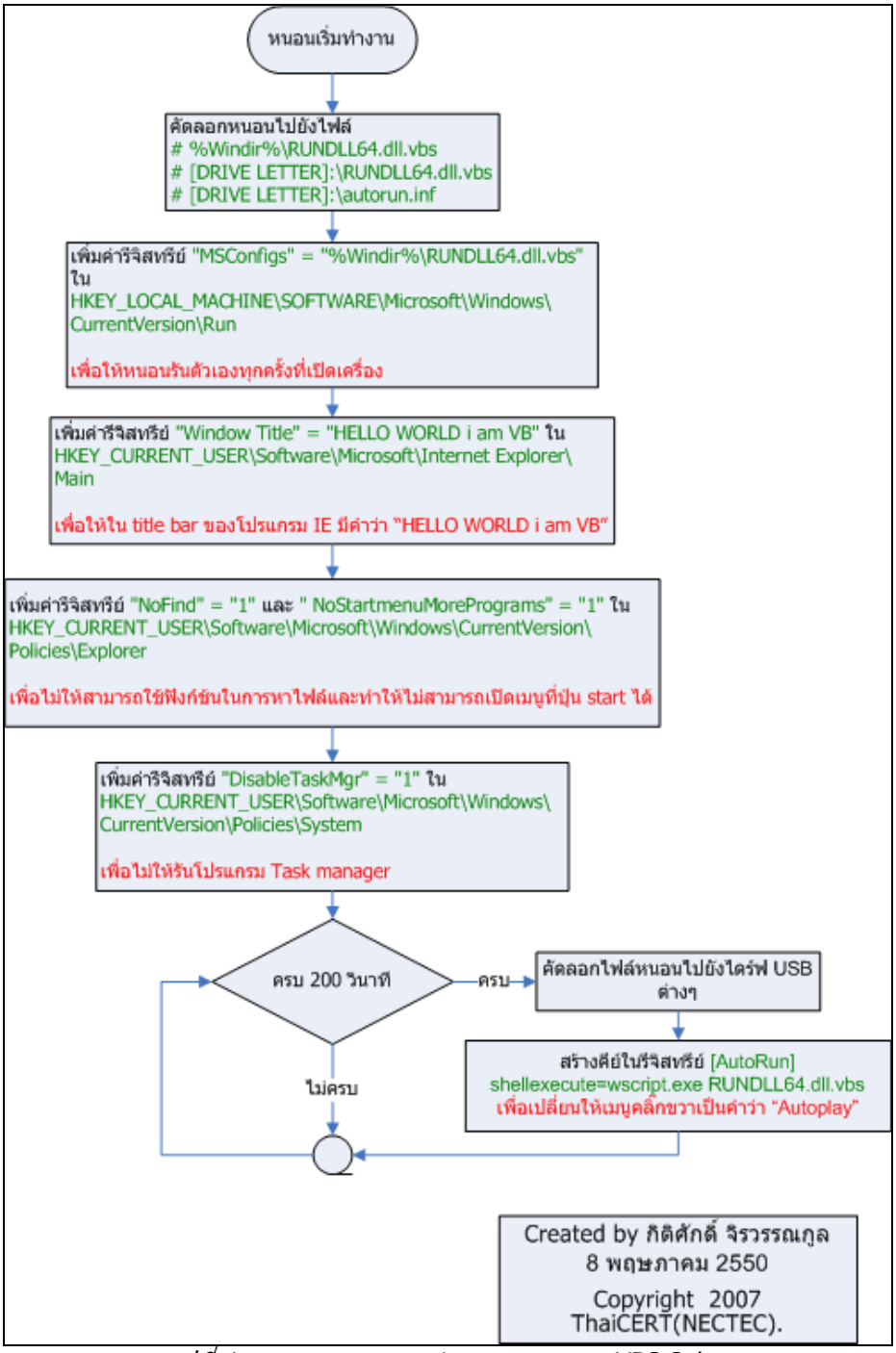
ซึ่งหนอนประเภทที่ถูกเขียนด้วยภาษาสคริปต์นั้นได้รับความนิยมสูงมาก เนื่องจากเขียนได้ง่าย และมีการเปิดเผยโค้ดมากมาย จุดมุ่งหมายของหนอนประเภทนี้คือการแพร่กระจายผ่านไดร์ฟต่างๆ โดยเฉพาะไดร์ฟ USB ที่จะถูกเรียกให้รันโดยไฟล์ autorun.inf โดยทุกครั้งที่ดับเบิลคลิกใช้งานที่ไดร์ฟต่างๆ ใน My Computer จะมีการเรียกไฟล์หนอนขึ้นมาทำงานได้ ตัวอย่างของหนอนประเภทนี้ได้แก่ VBS.Redlof.A VBS.Godzilla.A JS.Menger.Worm และ VBS.Solow เป็นต้น

ในบทความนี้จะเป็นการแนะนำให้รู้จักกับความน่ากลัวของหนอนชื่อ VBS.Solow ซึ่งจะแสดงภาพอาการผิดปกติเมื่อถูกหนอนชนิดนี้คุกคาม รวมทั้งวิธีการแก้ไขด้วยโปรแกรม ThaiCERT Hotfix V.1.0 ที่ถูกพัฒนาโดยทีมงาน ThaiCERT ด้วย

รายละเอียดของหนอนชนิดนี้
ชื่อ : VBS.Solow (Rundll64.dll.vbs)
ชื่ออื่นที่เป็นที่รู้จัก : VBS/Small.NAC (NOD32), VBS.Solow (Symantec) และ VBS/Monker.A (Panda)
ชนิด : หนอนอินเทอร์เน็ต (Worm)
ระบบที่มีผลกระทบ : Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP
ค้นพบเมื่อ : 3 พฤษภาคม 2550

กระบวนการทำงานของหนอนชนิดนี้

หนอน VBS.Solow เป็นสายพันธุ์ต่อเนื่องจากหนอนตระกูล Godzilla (สามารถอ่านรายละเอียดเพิ่มเติมได้ที่ http://www.thaicert.org/paper/virus/godzilla.pdf) ที่ถูกเขียนด้วยภาษา Visual Basic Script (VBS) อาศัยไดร์ฟ USB ในการแพร่กระจายด้วยไฟล์ที่มีชื่อว่า rundll64.dll.vbs อีกทั้งยังมีการแก้ไขค่าในรีจิสทรีย์ (Registry) เพื่อให้ระบบปฏิบัติการทำงานผิดพลาด เช่น ไม่สามารถเรียกใช้งาน Task Manager หรือไม่ให้แสดงเมนู All Programs ในเมนู Start รวมทั้งการแก้ไข Title bar ของโปรแกรม Internet Explorer (IE) ให้แสดงคำว่า "Hello World I am VB" เป็นต้น



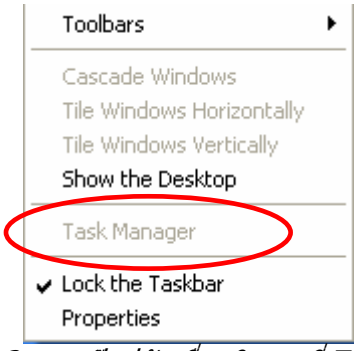
รูปที่ 1 แสดงกระบวนการทำงานของหนอน VBS.Solow

ลักษณะอาการที่เกิดขึ้น

1. สร้างรีจิสทรีย์คีย์ เพื่อทำให้ Title bar ของโปรแกรม IE มีคำว่า "HELLO WORLD I an VB" ทุกครั้งที่เปิดโปรแกรมขึ้นมาใช้งาน ไม่ว่าจะเข้าเยี่ยมชมเว็บไซต์ใดก็ตาม ดังรูปที่ 2

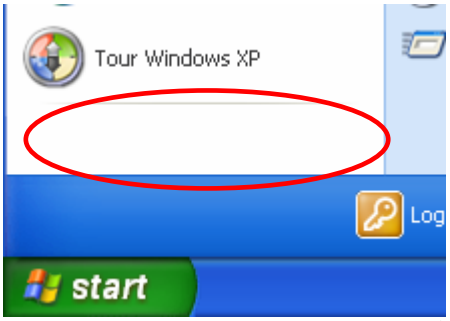
รูปที่ 2 แสดงหน้าต่างโปรแกรม Internet Explorer ที่มีข้อความที่ Title bar

2. สร้างรีจิสทรีย์คีย์ เพื่อให้ไม่สามารถเรียกใช้งานโปรแกรม Task Manager ได้ดังรูปที่ 3



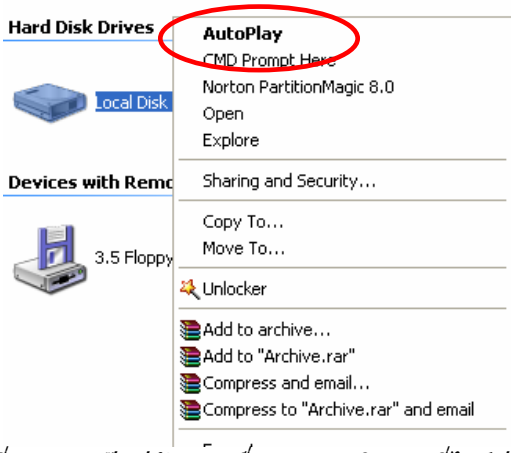
รูปที่ 3 แสดงป๊อปอัพเมื่อคลิกขวาที่ Task bar

3. สร้างรีจิสทรีย์คีย์ เพื่อให้ไม่สามารถมองเห็นเมนู All program ของ Start menu ของระบบปฏิบัติการวินโดวส์ ดังรูปที่ 4



รูปที่ 4 แสดงเมนู Start ของระบบปฏิบัติการวินโดวส์ XP

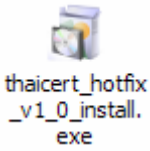
4. สร้างรีสทรีย์คีย์ เพื่อให้เมนูคลิ๊กขวาเปลี่ยนเป็นคำว่า "Autoplay" ดังรูปที่ 5



รูปที่ 5 แสดงป๊อปอัพเมนูเมื่อทำการคลิกขวาที่ไดร์ฟต่างๆ

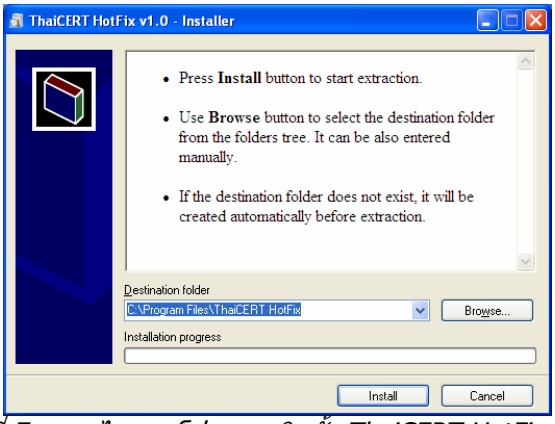
วิธีการกำจัดหนอนชนิดนี้

1. ดาวน์โหลดไฟล์ ThaiCERT HotFix Engine v1.0 จาก http://www.thaicert.org/thaicert_hotfix/thaicert_hotfix_v1_0_install.exe
2. ทำการติดตั้งโดยดับเบิลคลิกไฟล์ thaicert_hotfix_v1_0_install.exe ดังรูปที่ 6



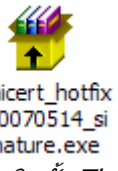
รูปที่ 6 แสดงไอคอนโปรแกรมติดตั้ง ThaiCERT HotFix v1.0

3. เมื่อโปรแกรมติดตั้งปรากฏดังรูปที่ 7 ให้เลือกโฟลเดอร์ที่จะทำการติดตั้ง ThaiCERT HotFix เช่น C:\Program Files\ThaiCERT HotFix\



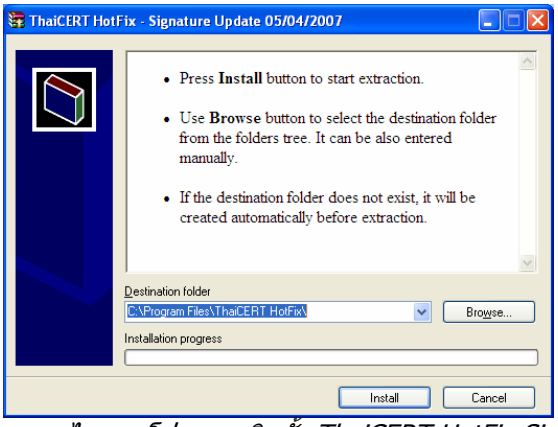
รูปที่ 7 แสดงไอคอนโปรแกรมติดตั้ง ThaiCERT HotFix v1.0

4. ทำการดาวน์โหลดไฟล์อัพเดต ThaiCERT HotFix Signature จาก http://www.thaicert.org/thaicert_hotfix/thaicert_hotfix_20070514_signature.exe
5. ทำการติดตั้งโดยดับเบิลคลิกไฟล์อัพเดตที่ดาวน์โหลดมาเช่น thaicert_hotfix_20070514_signature.exe ดังรูปที่ 8



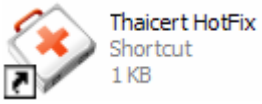
รูปที่ 8 แสดงไอคอนโปรแกรมติดตั้ง ThaiCERT HotFix Signature

6. เมื่อโปรแกรมติดตั้งปรากฏดังรูปที่ 9 เลือกโฟลเดอร์ที่ทำการติดตั้ง ThaiCERT HotFix ไว้เช่น C:\Program Files\ThaiCERT HotFix\



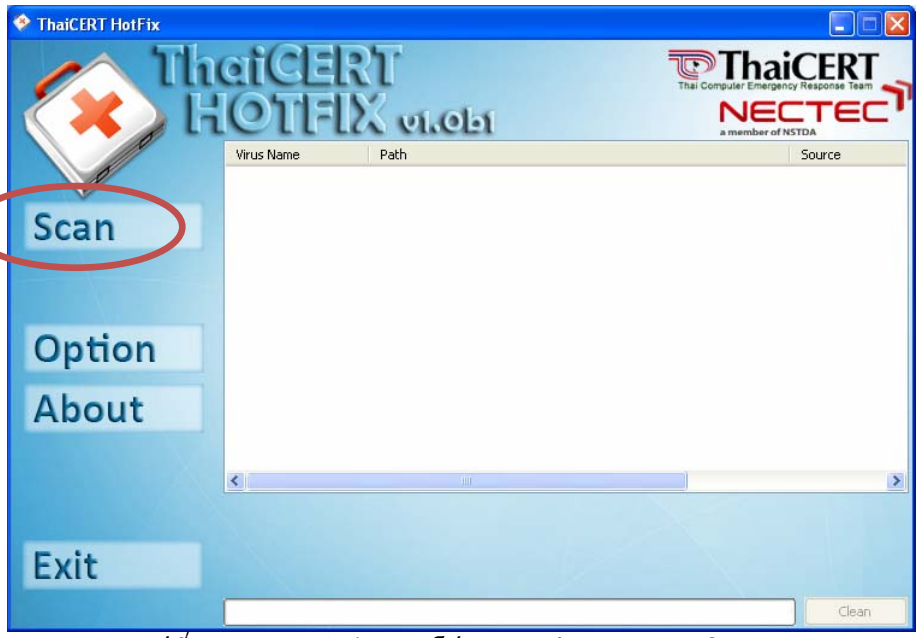
รูปที่ 9 แสดงไอคอนโปรแกรมติดตั้ง ThaiCERT HotFix Signature

7. หลังจากติดตั้งเสร็จแล้วก็สามารถเรียกใช้งานได้จาก shortcut ที่ desktop ดังรูปที่ 10



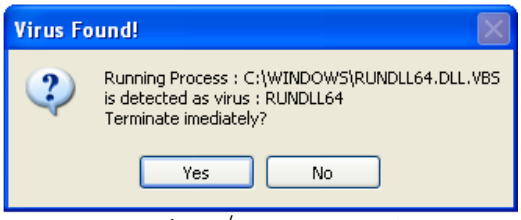
รูปที่ 10 แสดง Shortcut ของโปรแกรม ThaiCERT HotFix v1.0

8. เริ่มต้นเรียกใช้งานโปรแกรมโดยการดับเบิลคลิกที่ Shortcut จะปรากฏหน้าต่างดังรูปที่ 11 แล้วจึงกดปุ่ม Scan



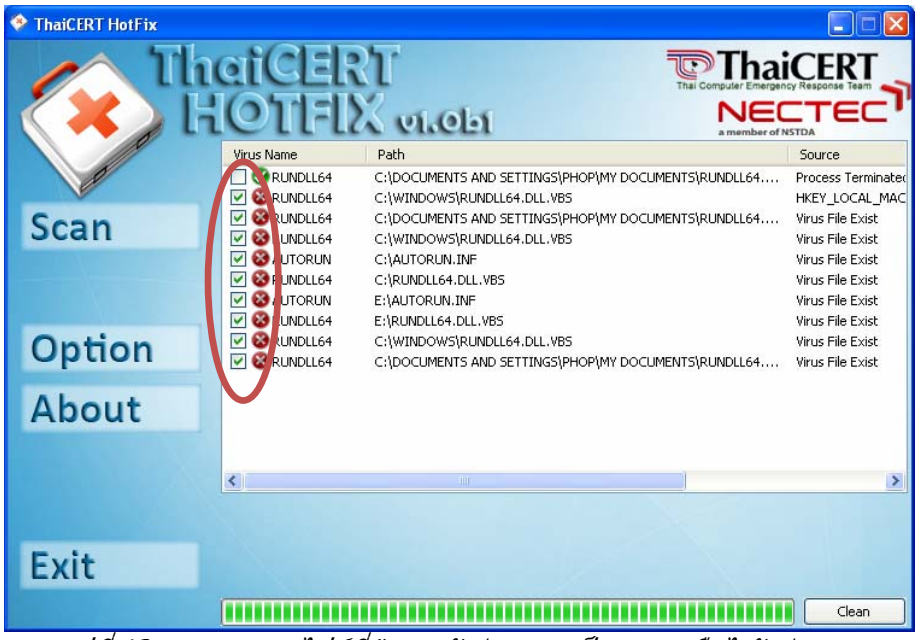
รูปที่ 11 แสดงหน้าต่างของโปรแกรม ThaiCERT Hotfix V1.0

9. เมื่อมีการตรวจสอบพบไวรัส โปรแกรมจะสร้างไดอะล็อกเพื่อให้ผู้ใช้ยืนยันก่อนจะทำการยุติโพรเซสของไวรัส โดยการกดปุ่ม Yes ดังรูปที่ 12



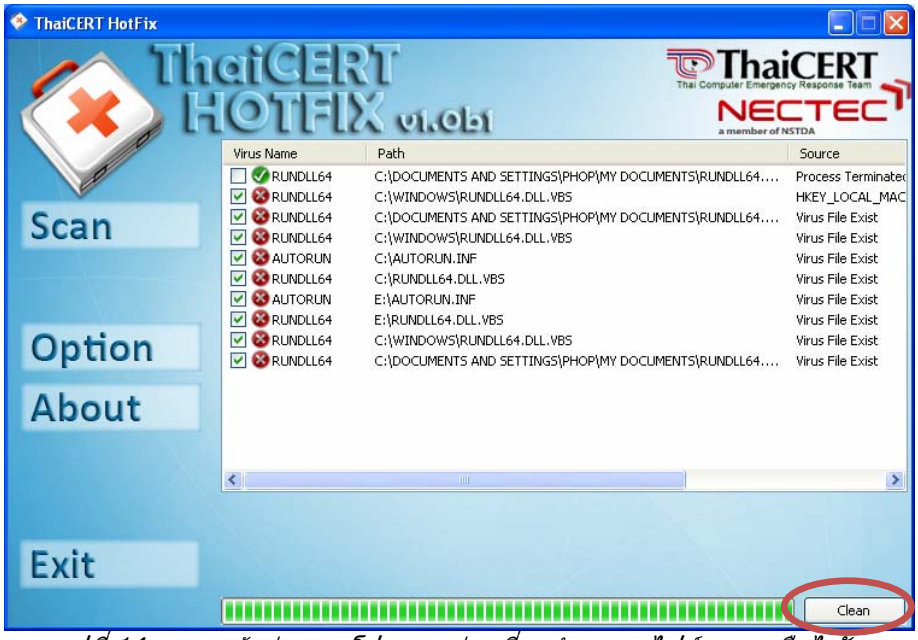
รูปที่ 12 แสดงไดอะล็อกเพื่อยืนยันการปิดโพรเซสของหนอน

10. เมื่อตรวจสอบพบไฟล์ของหนอนหรือไวรัสอื่นๆ โปรแกรมจะแสดงรายการไฟล์เหล่านั้น ถ้าหากพบไฟล์ที่ไม่ใช่หนอนหรือไวรัสให้คลิกเครื่องหมายออก ดังรูปที่ 13



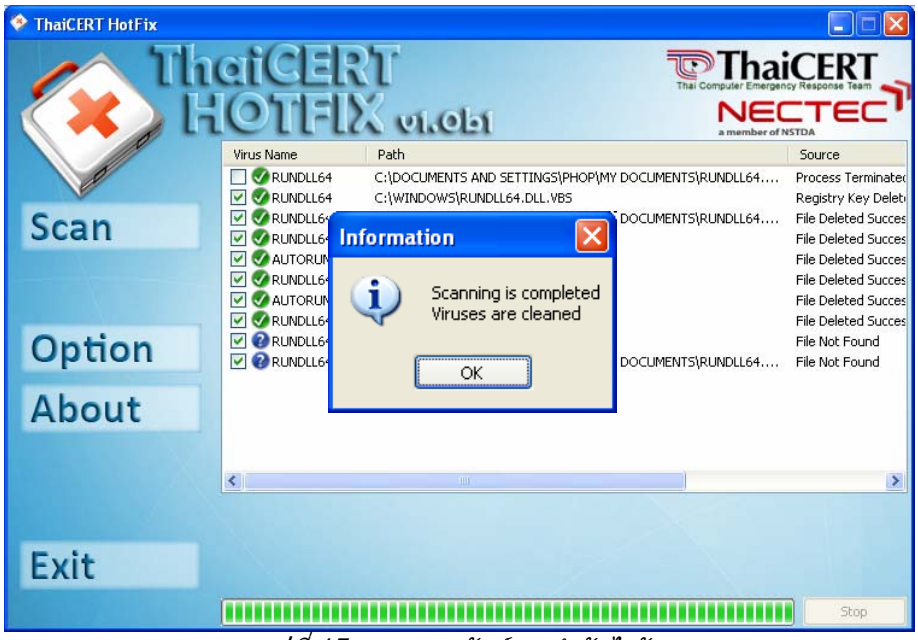
รูปที่ 13 แสดงรายการไฟล์ที่ต้องสงสัยว่าอาจจะเป็นหนอนหรือไวรัสก่อนลบ

11. กด Clean เพื่อลบหนอนออกจากเครื่องคอมพิวเตอร์ ดังรูปที่ 14



รูปที่ 14 แสดงหน้าต่างของโปรแกรมก่อนที่จะทำการลบไฟล์หนอนหรือไวรัส

12. โปรแกรมจะรายงานผลเมื่อทำการกำจัดหนอนหรือไวรัสเสร็จสิ้น และเปลี่ยนสถานะของผลการรายงาน ดังรูปที่ 15



รูปที่ 15 แสดง ผลลัพธ์การกำจัดไวรัส

หมายเหตุ
หากการลบไฟล์ต่างๆ ไม่สำเร็จโปรแกรมจะเตือนให้ผู้ใช้ทราบก่อนจะทำการลองลบอีกครั้ง

13. หลังจากทำการลบไฟล์ของหนอนเสร็จเรียบร้อยแล้ว แต่ค่ารีจิสทรีย์ที่ถูกหนอนเปลี่ยนแปลงนั้น จำเป็นจะต้องแก้ไขคืนเพื่อให้ระบบปฏิบัติการทำงานได้อย่างถูกต้อง โดยสามารถดาวน์โหลดและรันตัวแก้ไขได้จาก http://www.thaicert.org/thaicert_hotfix/HotFix_RegFix_RUNDLL64.zip