ท่าจัด!!

Virus Godzilla

237211 COMPUTER NETWORKING

FOR EDUCATION

คำนำ

ไวรัส Godzilla เล่มนี้ เป็นส่วนหนึ่งของวิชา [237211-2554 COMPUTER NETWORKING FOR EDUCATION] ได้จัดทำเรื่อง“ ไวรัส Godzilla ” โดยมีเนื้อหาที่กล่าวถึงไวรัส Godzilla และวิธีกำจัดไวรัส Godzilla เพื่อให้บุคคลที่สนใจ ได้ศึกษาหาความรู้ คณะผู้จัดทำหวังเป็นอย่างยิ่งว่า รายงานเล่มนี้ จะเป็นประโยชน์แก่กลุ่มของข้าพเจ้าและบุคคลที่สนใจไม่มากก็น้อย

หาก ผิดพลาดประการใด ทางคณะผู้จัดทำก็ขออภัยมา ณ ที่นี้ด้วย

จัดทำโดย

คณะผู้จัดทำ

สารบัญ

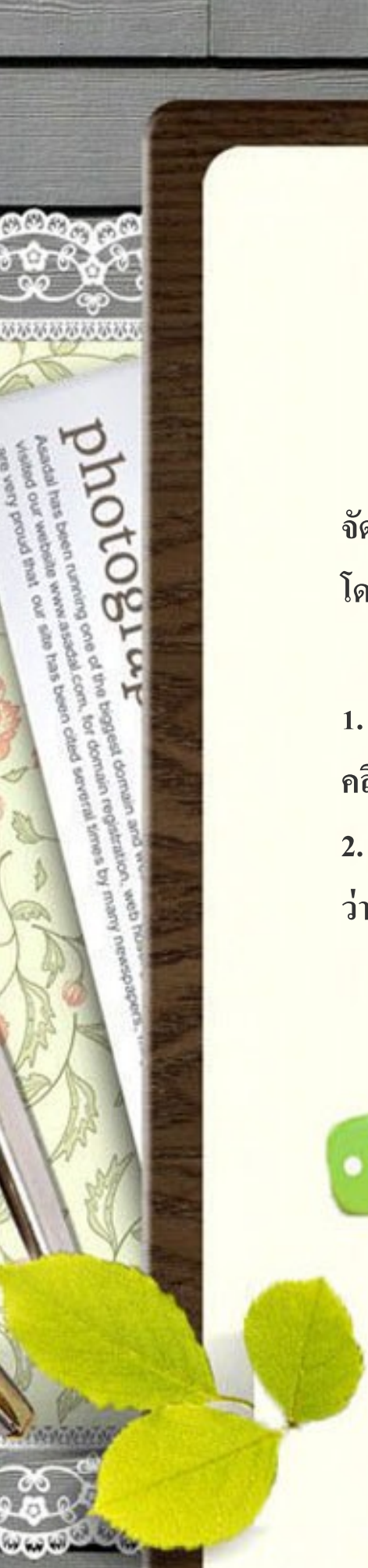
ไวรัส Godzilla

Hacked By Godzilla เป็นไวรัส ตัวใหม่ที่กำลังระบาดอยู่ จัดเป็น spyware ที่ก่อกวนการทำงานมากกว่าจะทำลายข้อมูล โดยจะเป็นการติดผ่าน Handy Drive และ Floppy Disk เท่านั้น

<u>ลักษณะอาการ</u>

1. เครื่องจะไม่สามารถ Double Click เปิดไดร์ฟต่างๆได้ แต่จะคลิกเมาส์ขวาเพื่อเปิดไดร์ฟโดยเลือกเมนู Open หรือExplore

2. มีข้อความปรากฏบน Title Bar ของ Internet Explorer ว่า “Hacked By Godzilla”



มีข้อความปรากฏบน Title Bar ว่า “Hacked By Godzilla”

วิธีการแก้ไขเมื่อติดไวรัส Godzilla

1. Double Click ไอคอน My Computer ที่ Desktop เลือกเมนู Tools –> Folder Options

2. ปรากฏไดอะล็อก Folder Options คลิกแท็บ View

2.1) คลิกเลือก Show Hidden files and folders

2.2) เอาเครื่องหมาย / ในช่องสี่เหลี่ยมหน้า Hide extention… และ Hide protected operating system file ออก

2.3) คลิก OK

3. กดปุ่ม Ctrl+Alt+Delete ที่คีย์บอร์ด

4. ปรากฏไดอะล็อกบ็อก Windows Task Manager คลิกเลือกแท็บ Processes

4.1) คลิกเลือกเมนู Image Name (เพื่อ sort File)

4.2) คลิกเลือกไฟล์ wscript.exe (ทีละตัว)

4.3) คลิกปุ่ม End Process

5. เปิด ไดร์ฟ (โดยคลิกเมาส์ขวาเลือก Explore ห้าม Double Click ไดร์ฟ) ทำการลบไฟล์ autorun.inf และ MS32DLL.dll.vbs ออก (โดยกด Shift+Delete) ทุกไดร์ฟที่มีอยู่ในเครื่องคอมพิวเตอร์ซึ่งรวมทั้ง Handy Drive และ Floppy disk ด้วย

6. เปิดโฟลเดอร์ C:WINDOWS เพื่อลบไฟล์ MS32DLL.dll.vbs ออก (โดยกด Shift+Delete)

7. ไปที่ปุ่ม Start-->Run ปรากฏไดอะล็อกบ็อก Run พิมพ์คำสั่ง regedit กดปุ่ม OK

ปรากฏไดอะล็อกบ็อก Registry Edit

8. คลิกเลือก HKEY_LOCAL_MACHINE --> Software --> Current Version –> Run เพื่อลบไฟล์ MS32DLL (โดยการกดปุ่ม Delete ที่คีย์บอร์ด)

9. คลิกเลือก HKEY_CURRENT_USER --> Software --> Microsoft --> Internet Explorer –> Main เพื่อลบไฟล์ที่ Window Title “Hacked by Godzilla” ออก (โดยการกดปุ่ม Delete ที่คีย์บอร์ด)

10. คลิกปุ่ม Start --> Run ปรากฏไดอะล็อกบ็อก Run พิมพ์คำสั่งgpedit.msc กดปุ่ม OK ปรากฏไดอะล็อกบ็อก Group Policy

11. คลิกเลือก User Configuration --> Administrative Templates --> System –> Double Click ไฟล์ Turn Off Autoplay ปรากกฏไดอะล็อกบ็อก Turn Off Autoplay Properties

11.1) คลิกเลือก Enabled

11.2) คลิกเลือก All drives

11.3) คลิก OK

วิธีกำจัด ไวรัส Godzilla

อีกวิธีเหมือนวิธีกำจัด Flashy

ก่อนอื่นต้องไปดาว์โหลดไฟร์แก้ไวรัสมาก่อน Taskmanager ก่อนอื่น ลง โปรแกรม Taskmanager พอลงเสร็จโปรแกรมจะถามว่ารันไหมตอบไปเลยว่า รัน

สังเกตหา คำว่า MS32Dll.dll.vbs ในช่องด้านซ้ายสุดติดอันดับต้นๆเลยถ้าเจอแล้วก็กดที่หนึ่งให้ขึ้นแถบสีน้ำเงิน หรือว่าสีเทาขึ้นอยู่กับ Themes ที่เราใช้เอาเป็นว่าให้มันเป็นแถบแล้วถือว่าใช้ได้หลังจากนั้น หาปุ่ม **X** สีแดงเขียนว่า Remove อยู่ด้านบน กดที่หนึ่ง จะมีหน้าต่างขึ้นมา ตรงหน้าคำว่า End Process จะมีจุดสีเขียงอยู่ ตอบ OK ดูในรูป

ไม่แน่ใจว่าจะหน้าต่างขึ้นมาถามอะไรอีกไหมถ้ามีตอบ YES เป็นการถามยืนยัน ไม่มีอะไร จากนั้นก็ปิดโปรแกรม เท่านี้ก็เป็นอันว่าเราได้หยุดการทำงานของเจ้าตัวร้ายแล้ว

บางเว็บก็บอกว่ามีอีกตัว ชื่อ wscript.exe ถ้ามีก็หยุดการทำงานทำตามวิธีข้างบน

จากนั้น ก็เปิด My Computer ขึ้นมา เลือก Tools--> FolderOption

จะมีหน้าต่าง folderoption ขึ้นมา

ทำตามให้เหมือนในรูป

1.View

2. Show Hidden files and foldres

3. เอาเครื่องหมายถูกหน้า Hide extention และ Hide protected opeating system file

4. OK

ขั้นตอนต่อไปทำที่ละไดร์ และต้องทำทุกไดร์ รวมทั้งเจ้า Handy Drive ตัวโปรดด้วย

เปิด My Computer ขึ้นมา แล้วกดตามรูป Folders

ผลจะออกมาเป็นแบบนี้ในกรอบด้านซ้าย

กดเปิดไดร์กดในกรอบสีน้ำเงินผลที่ได้คือ ภาพนอกกรอบด้านขวาเห็นไฟล์จางๆไหมนั้นคือไฟล์ที่ระบบ หรือตัวเราด้วยที่ซ่อนเอาไว้แต่ของเราเรารู้จักดีใช่ไหม อันที่ไม่รู้จักคือระบบเป็นตัวซ่อน เอาละ ทีนี้เราก็มาลบเจ้าตัวร้ายกันเถอะ ชื่อของมันคือ **MS32DLL.dll.vbs**

และ**autorun.inf** ตัวนี้สำคัญใน**ไดร์ C** สังเกตจากลูกศรแดง ในไดร์มี **AUTOEXE.BAT** อยู่ด้วยนะดูให้ดีก่อนลบ บางคนลบผิด ผลที่ได้คือเข้าวินโดว์ไม่ได้ ส่วนวิธีการลบก็ห้ามกด Delete อย่างเดียว คิดว่าเดี๋ยวไป Empty Recycle bin เอาที่หลัง ลืมแน่ๆ เอาเป็นว่าที่เดียวเลย กด Shift+Delete เผ่าออกจากเครื่องไปซะเลย อย่าลืมนะ ต้องทำทุกไดร์เพราะมันฝังอยู่ทุกไดร์ ไดร์ไหนไม่มีไม่เป็นไร ผ่านได้ สังเกตนะ ไดร์อื่นๆนอกจากไดร์ C ถ้าหากมี **autorun.inf** อยู่ตัวเดียวก็ให้ลบเลยเพราะปกติไม่มี

หลังจากที่ทำตามวิธีข้างตนแล้ว เราก็มาลบ ตัวแม่ หรือตัวเรียกให้ไวรัสทำงานกันเพราะถ้าไม่ลบ พอ รีสตาร์ส ก็กลับมาเป็นเหมือนเดิม

ไปที่ไดร์ C ใน folder windows

จากนั้นเรามาแก้ข้อความ ที่ปรากฏที่ Interent Explorer ไปที่ Start Menu\Run พิมพ์ Regedit จะมีหน้าต่าง

HKEY_CURRENT_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\ จะมี MS32DLL อยู่ กดปุ่ม Delete ตัวเดียวเพื่อลบ

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\ ขวามือ หาข้อความที่เขียนว่า Hacked By GodZilla แล้วกดปุ่ม Delete ตัวเดี่ยวเพื่อลบ

ต่อไปก็ ไปที่ Start Menu\Run พิมพ์ MSCONFIG จะมีหน้าต่าง

ไปที่ช่อง startup เอาเครื่องหมายถูกหน้า MS32DLL แล้ว OK เครื่องจะถาม ว่า รีสตาร์ท เลยไหม ตอบ ไม่ เหมือนในกรอบสีแดงในรูปข้างล่าง

กลับมาปิดไฟล์ที่ระบบซ่อนไว้อีกที

เปิด My Computer ขึ้นมา เลือก Tools--> Folder Option

1. View

2. Do not Show Hidden files and foldres

3. ใส่เครื่องหมายถูกหน้า Hide extention และ Hide protected opeating system file ออก

4. OK

พอเสร็จทั้งหมดแล้วเราก็ รีสตาร์ส เครื่องได้เลย เสร็จสิ้นการกำจัดไวรัส

<u>วิธีการแก้ไขเมื่อติดไวรัส Godzilla โดยใช้โปรแกรม</u> Kill_Gozilla

ให้ Download โปรแกรม Kill_Gozilla

<u>วิธีใช้</u> เมื่อ Download มาแล้วให้คลิกที่ start.exe โปรแกรมจะทำการกำจัดสปายแวร์ให้โดยอัตโนมัติ

บรรณานุกรม

http://computer-to-repair1.blogspot.com/

http://www.jobpub.com/articles/showarticle.asp?id=1715

http://antivirus.nabia10.com/virus-t/gosz.html

สมาชิก

SMP BOOK B0005

Editor

1. นางสาวฉัตรนภา	แก่นแก้ว	533050187-7
2. นางสาวประภัสศร	เวพุวะนารักษ์	533050202-7
3. นายรัฐปฎล	กันหะคุณ	533050207-7
4. นางสาวดลยา	โชติรื่น	533050338-2
5. นางสาวสุทธิกานต์	อาญาสิทธิ์	533050347-1

สาขา คอมพิวเตอร์ศึกษา ชั้นปีที่ 2

คณะศึกษาศาสตร์ มหาวิทยาลัยขอนแก่น

ปีการศึกษา 2554


Virus Godzilla