



หนังสือเล่มนี้เป็นส่วนหนึ่งของวิชาเครือข่ายคอมพิวเตอร์เพื่อ การศึกษา237211 เป็นเรื่องเกี่ยวกับไวรัส Flashy จัดทำขึ้นเพื่อให้ ความรู้และวิธีการกำจัดไวรัส Flashy ซึ่งคณะผู้จัดได้ตั้งใจจัดทำขึ้น อย่างเต็มที่ เพื่อเป็นประโยชน์แก่ผู้ที่ต้องการศึกษา และผู้อ่านทั่วไป แต่ถ้ามีความผิดลาดประการใด คณะผู้จัดขออภัย ณ ที่นี้ด้วย

fayos	
สารบัญ	
เรื่อง	หน้า
อาการที่พบ	1
วิธีแก้ปัญหา	2
โปรแกรมที่ใช้สแกนไวรัส Flashy	11
บรรณานุกรม	13



ੀ**ਂਤਤੱ**ਕ Flashy

(Win32/Disabler.l trojan)

<u>อาการที่พบ</u>

1. ไม่สามารถเรียกใช้ Task Manager, Registry Editor และ Folder Option ได้ ไม่ว่าจะเรียกด้วยวิธีใด

2. อยู่ดีๆเครื่องก็ตั้ง password admin ให้ทั้งๆที่เราไม่ เคยตั้งทำให้เราเข้าเครื่องตัวเองไม่ได้แต่พอลองใส่รหัสผ่าน ว่า hacked เข้าได้

3. เมื่อมีการเสียบ Flash Drive หรือ Memory Card เข้า ไปใน Card Reader แล้วหากว่าใน Memory Card นั้น มี Folder อยู่ Folder เหล่านั้นจะถูกเปลี่ยนให้ไปอยู่ใน สถานะ Hidden ทำให้เราไม่สามารถองเห็น Folder เหล่านั้นได้

<u>วิธีแก้ปัญหา</u>

** ขั้นตอนต่างๆต้องทำใน Safe mode ถึงจะได้ผล

เข้า Safe Mode ด้วยการกด F8 รัวๆตอน boot เครื่อง

ขั้นตอนที่ 1

ถ้าเครื่องที่มีอาการหนักจะถูกตั้ง รหัสผ่าน Administrator เอาไว้ ให้ทำการแก้ไขโดยพิมพ์ คำว่า hacked เป็นรหัสผ่าน ซึ่งหากไม่รู้วิธีแก้ปัญหาโดย การติดตั้ง Windows ใหม่อย่างเดียว

ขั้นตอนที่ 2

เมื่อเราเข้าวินโดว์ได้แล้วให้เราหยุดการทำงานของ มันก่อนโดยกด **Ctrl+Alt+Delete** จะเข้าสู่ Windows task Manager แล้วเลือกคลิก Flashy.exe แล้วคลิก End Process ตรงมุมขวาด้านล่าง

ขั้นตอนที่ 3

กรณีถ้าเข้า Windows Task Manager ไม่ได้(ถ้าเข้าได้ ให้ข้ามไปขั้นตอนที่ 6) ให้เราเข้าไปแก้ใน registry แต่ ไวรัสยังปิดการเข้าใช้งาน Registry เอาไว้อีกให้ใช้ ตัว Unhookexec.inf ปลดล็อคก่อนโดยดาวน์โหลด เมื่อ โหลดมาแล้วแตกไฟล์ แล้วก็คลิกขวาที่ ไฟล์ UnHookExec.inf แล้วเลือก Install แต่ถ้าเครื่องไหนที่ ติดไวรัสหน้าจอภาษาจีนด้วย ต้องฆ่าก่อนไม่อย่างนั้นจะ ใช้ UnHookExec.inf ไม่ได้ผล

ขั้นตอนที่ 4

จากนั้นก็จะเข้าใช้งานส่วน Registry ได้ครับ เมื่อ เข้าได้แล้วก็ไปทำการแก้ไข Registry ให้เครื่องใช้ งาน Task Manager ได้ครับ โดย ไปที่ Start > Run พิมพ์ regedit กด OK แล้วเข้าไปลบคีย์ตาม นี้ HKEY_CURRENT_USER\Software\Microsoft\Window s\Curre ntVersion\Policies\system

File Edit View Favorites Help					
😑 📕 My Computer	~	Name	Туре	Data	
HKEY_CLASSES_KOOT HKEY_CURRENT_USER HKEY_CURRENT_USER HKEY_CORRENT_USER Console Console Control Panel Finvironment Dichtities Control Panel Herbities Herbi		創(Default) 間DisableRegistryTools 認DisableTaskMgr	REG_SZ REG_DWORD REG_DWORD - ฉบออกกดปุ่ม C	(value not set) 0x0000000 (0) 0x00000000 (0)	
<	>	· · · · · · · · · · · · · · · · · · ·			>

แล้วก็ลบ DisableRedistryTools และ DisableTaskMgr ออก

ขั้นตอนที่ 5

เมื่อลบออกได้แล้วก็ไปทำตาม ข้อ 2



ขั้นตอนที่ 6

แล้วตอนนี้มันก็หยุดการทำงานแล้วครับ ต่อไปเรา ต้องเข้า regedit แล้ว ไปที่ Start > Run พิมพ์ regedit แล้ว เข้าไปลบคีย์ตามนี้ HKEY_CURRENT_USER\Software\Microsoft\Windows\C urre ntVersion\Policies\Explorer\

ลบ NoFolderOptions

Internet Se Multimedia Multimedia Policies System Run Run RunOnce Settings Settings Shell Exten: Syncmgr	Name (Default) NoDriveTypeAutoRun NoRun NoSaveSettings NoViewContextMenu NoViewContextMenu NoFolderOptions	Type REG_52 REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD	Data (value not set) 0x00000091 (145) 0x00000000 (0) 0x00000000 (0) 0x00000000 (0) 0x00000000 (0)	
	8			>

HKEY_CURRENT_USER\Software\Microsoft\Windows\Cu rre ntVersion\Explorer\Advanced\ ลบ HideFileExt



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\S ervic es\SharedAccess\

ลบ Start

1	🗄 🦲 seclogon 🛛 🧹	Name	Туре	Data
	E 🦲 SENS	DependOnService	REG MULTI SZ	Netman NLA RasMan ALG
	🗄 🦲 serenum	ab Description	REG_SZ	Provides network address translation
	🕀 🦲 Serial	ab DisplayName	REG_SZ	Internet Connection Firewall (ICF) /
	E Shoppy	ErrorControl	REG_DWORD	0×00000001 (1)
	G SharedAccess	ab ImagePath	REG_EXPAND_SZ	%SystemRoot%\System32\svchost.
	Enum	DbjectName	REG SZ	LocalSystem
	Security	B Start	REG_DWORD	0×00000002 (2)
	🗉 🧰 ShellHWDetecti	ВТуре	REG_DWORD	0x00000020 (32)
4. 5.	× × ×			

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows \Curr entVersion\Run\ ลบ Flashy.exe



จากนั้นคลิก Start\Programs\Startup\ ลบ SystemID.pif จากนั้นคลิก Start > Run พิมพ์ msconfig ไปที่ แถบ startup ยกเลิกติ๊กถูกหน้า systemID รีสตาร์ทเครื่องใหม่แล้วลองกด CtrI+Alt+Delete ดู ว่า Flashy.exe ยังมีการทำงานอีกหรือไม่ ถ้าไม่มีแสดง ว่าเรียบร้อยแล้ว



<u>การแก้ไขส่วนที่ไวรัสสร้าง ให้เราต้องใส่รหัส</u> <u>ทุกครั้ง เวลาจะเปิดเครื่อง</u>

ขั้นตอนที่ 1

คลิก Start > Setting > Control panel > User accounts เลือก User แรก (Administrator) จะสังเกตเห็นว่า มีข้อความแสดงว่า Password protected มีการใช้รหัสผ่าน ป้องกันอยู่ให้คลิกที่ User แรก (Administrator)

ขั้นตอนที่ 2

เลือกหัวข้อ Change a password พิมพ์ รหัสผ่าน Hacked ในช่องแรก (ช่องรหัสผ่านเดิม) ช่องที่เหลือเว้นว่างไว้ ยืนยันการ เปลี่ยนรหัสผ่าน แล้วลองรีสตาร์ทเครื่องใหม่ หรือ Start > Run พิมพ์ regedit > คลิก OK แล้วไปตามนี้ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Window s NT\CurrentVersion\Winlogon] แก้สตริงคีย์ตามนี้ครับหากไม่มีก็คลิกขาวเลือก New > String value ตามนี้

"AutoAdminLogon"="1" "DefaultUserName"=" ชื่อผู้ใช้" "DefaultPassword"hacked"

** หลังจากทำตามขั้นตอนเสร็จหมดแล้วให้ไปลบตัวไวรัส ชื่อ Flashy.exe ใน C:\WINDOWS\system32

😂 system 32						
File Edit View Favorite:	s Tools	Help Search 🌔 Fold	ers 🔟 หลังจากทั่	าตามขึ้นตอ ไวรัสชื่อ F	บนเสร็จหมดแล้วให้ lashv.exe ในนี้	N
Address 🛅 C:\WINDOWS\sys	stem32		K			V 🛃 Go
		Name	Size	Туре 🔺	Date Modified	^
System Tasks	(¥)	🛅 3com_dmi 🛅 1025		File Folder File Folder	12/8/2549 12:37 12/8/2549 12:37	

** ต้องเปิด Show hidden File ก่อนถึงจะเห็น วิธีการ เปิด Show hidden File ทำได้โดย Tools > Folder Option > Show hidden files and

folders > คลิก ok

0.000 million (0.000		
General VI	ew File Types Offline Files	
Folder vi	iews	
1000	You can apply the view (such as Details or T	iles) that
1.22	you are using for this folder to all folders.	447
- CAR	Apply to All Folders Reset All Fold	ders
		let let
-		
Advanced	l settings:	
🛅 Files	and Folders	~
	Automatically search for network folders and printe	ers
	Display file size information in folder tips	
	Display simple folder view in Explorer's Folders list	
	Display the contents of system folders	
	Display the full path in the address bar	
	Display the full path in the title bar	
	2 I.S. III I.S. II I.S. II.A. I.I. II.I.I.I.I.I.I.I.I.I.I.I.I.	
) o not cache thumhnails	
	Do not cache thumbnails	
	Do not cache thumbnails Hidden files and folders	
	Do not cache thumbnails Hidden files and folders Do not show hidden files and folders Show hidden files and folders	
	Do not cache thumbnails Hidden files and folders Do not show hidden files and folders Show hidden files and folders	-
	 Do not cache thumbnails Hidden files and folders Do not show hidden files and folders Show hidden files and folders Hide extensions for known file types 	~
	Do not cache thumbnails Hidden files and folders Do not show hidden files and folders Show hidden files and folders Hide extensions for known file types	•
	Do not cache thumbnails Hidden files and folders Do not show hidden files and folders Show hidden files and folders Hide extensions for known file types Restore I	▼ Defaults
	Do not cache thumbnails Hidden files and folders Do not show hidden files and folders Show hidden files and folders Hide extensions for known file types Restore I	▼ Defaults

<u>โปรแกรมที่ใช้สแกนไวรัส Flashy (**Win32**/</u>

Disabler.I trojan)

😊 โปรแกรม NOD32 MyGril-Fix

🗈 activementa Flashy Trojan Remover Tool Setup					
	License Agreement Please review the license terms before installing Activemedia Flashy Trojan Remover Tool.				
Press Page Down to see the rest of the agreement.					
Copyright a 2006 A. Mees	angnil				
This software is provided 'as-is', without any express or implied warranty from the author or Activemedia (Thaland). In no event will the authors be held liable for any damages arising from the use of this software. This Software is not a product of ESET, spol. s r.o. nor affiliated by NOD32 Anti-Virus System. This Software is created by NSIS Windows Installer.					
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Activemedia Flashy Trojan Remover Tool.					
Activemedia Flashy Trojan Remover Tool 1.0					





อ้างอิง

http://intranet.gs.kku.ac.th/km/index.php? option=show&id=4 สีบคันข้อมูลเมื่อ 23/09/54 http://antivirus.nabia10.com/virus-t/girl.html สีบคันข้อมูลเมื่อ 20/09/54



สมาชิกในกลุ่ม

1.นางสาวศิริวิภา กุมปรุ 533050201-9
2.นางสาวธิดาทิพย์ ทุมวัน 533050197-4
3.นางสาวจันทรา ที่อุปมา 533050184-3
4.นางสาวจิดาภา ศิริพรรณ 533050335-8
5.นายพิท์กษ์ สมบรรณ 533050343-9
ศณะศึกษาศาสตร์ สาบาศอมพิวเตอร์ศึกษา มหาวิทยาล์ยบอนแก่น