บทที่ 7 : การป้องกันไวรัส Part1

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

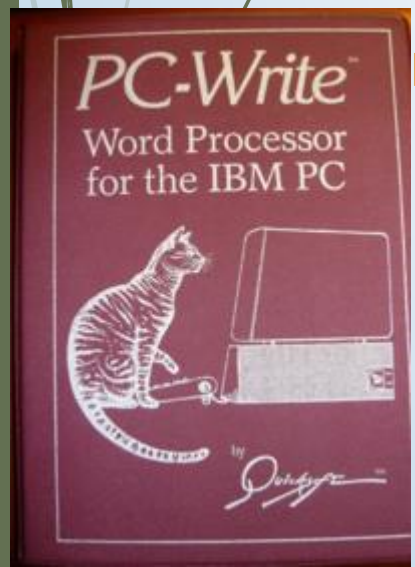
apipong.ping@gmail.com

Outline

- วิวัฒนาการของไวรัสคอมพิวเตอร์
- มัลแวร์ (Malware)
- โปรแกรมที่ไม่จัดเป็นมัลแวร์

วิวัฒนาการของไวรัสคอมพิวเตอร์

- ไวรัสคอมพิวเตอร์เริ่มมีมาตั้งแต่ทศวรรษ 1980 โดยเป็นไวรัสที่พัฒนาเพื่อใช้ในห้องทดลองเท่านั้น ซึ่งลักษณะของไวรัสก็เป็นแค่การก๊อปปี้ตัวเองไปเรื่อยๆ และแสดงข้อความตลกๆเท่านั้น



- ในปี 1986 มีรายงานว่ามีไวรัสโจมตีคอมพิวเตอร์ในระบบ MS-DOS เป็นครั้งแรก ชื่อว่าไวรัสเบรน (Brain Virus) และโทรจันตัวแรกมีชื่อว่า PC-Write ซึ่งอยู่ในรูปแบบของโปรแกรมประมวลผลคำ

วิวัฒนาการของไวรัสคอมพิวเตอร์ [2]

- ในปี 1988 อินเทอร์เน็ตเวิร์มตัวแรกได้ปรากฏขึ้น มีชื่อว่า Morris Worm มีผลทำให้อินเทอร์เน็ตช้าลงอย่างมาก
- เมื่อมีการระบาดของไวรัสมากขึ้น จึงได้มีการตั้งศูนย์ประสานงาน CERT (Computer Emergency Response Team) เพื่อช่วยเหลือข้อมูลด้านไวรัสที่แพร่กระจายบนอินเทอร์เน็ต
- ปี 1990 เกิดไวรัสประเภท Polymorphic Virus ขึ้นตัวแรก ซึ่งมีความสามารถในการเปลี่ยนแปลงตัวเองในทุกๆการแบ่งตัว

วิวัฒนาการของไวรัสคอมพิวเตอร์ [3]

- หลังจากนั้นไวรัสก็มีพัฒนาการเรื่อยมา ไวรัสบางตัวสามารถส่งอีเมล์เองได้ สามารถแฝงตัวไปกับไฟล์ประเภทออฟฟิศได้ ไวรัสบางตัวสามารถสร้าง Backdoor เพื่อเปิดทางให้แฮกเกอร์เข้าโจมตีได้ และยังมีการใช้ Social Engineering ในการหลอกดึงดูดความสนใจของผู้ดูหรือผู้อ่าน ทำให้ไวรัสแพร่กระจายไปอย่างรวดเร็ว
- โปรแกรมป้องกันไวรัสส่วนใหญ่เป็นแบบ Signature-based ซึ่งมีฐานข้อมูลของไวรัสแต่ละตัวอยู่ แต่ข้อเสียคือจะยังไม่สามารถตรวจพบไวรัสใหม่ๆได้ในช่วงแรกของการปล่อยไวรัส

มัลแวร์ (Malware)

- Malware ย่อมาจาก Malicious Software หมายถึง โปรแกรมประสงค์ร้ายต่างๆ เช่น ไวรัส เวิร์ม และโทรจันฮอร์ส

มัลแวร์ (Malware) : Trojan Horse

- โทรจันฮอร์สไม่จัดว่าเป็นไวรัสหรือเวิร์ม เพราะไม่สามารถแพร่กระจายด้วยตัวเองได้ แต่ไวรัสหรือเวิร์มอาจก็อปปี้โทรจันฮอร์สไปยังระบบอื่นด้วยก็ได้ ปกติโทรจันฮอร์สจะอยู่ในรูปโปรแกรมที่ดูแล้วไม่มีอันตรายทั่วไป
- จุดมุ่งหมายของโทรจันฮอร์สก็เพื่อสร้างความรำคาญ ขัดขวางการทำงานประจำ หรือสร้างช่องทางเพื่อเปิดทางให้แฮคเกอร์เข้ามาขโมยข้อมูลหรือคอนฟิกระบบใหม่

มัลแวร์ (Malware) : Trojan Horse [2]

ชื่อเรียกอื่นตามลักษณะการทำงาน เช่น

- Remote Access Trojan : สามารถสร้างแบ็คดอร์ให้แฮคเกอร์เข้ามาโจมตีหรือควบคุมระบบจากระยะไกลได้
- Rootkits : เป็นชุดโปรแกรมที่แฮคเกอร์นิยมใช้สำหรับเจาะเพื่อควบคุมระบบหรือขโมยข้อมูล อาจใช้วิธีการเฝ้าดูคีย์ที่ผู้ใช้พิมพ์ รูทคิทจะเป็นชุดโปรแกรมที่ใช้สำหรับโจมตีระบบปฏิบัติการประเภทใดประเภทหนึ่งโดยเฉพาะ

มัลแวร์ (Malware) : Worm

- เป็นมัลแวร์ที่สามารถแพร่กระจายตัวเองได้ด้วยตัวมันเอง โดยที่ไม่ต้องรอให้ผู้ใช้เปิดไฟล์
- เวิร์มจะพยายามก็อปปี้ตัวเองไว้ในระบบคอมพิวเตอร์ แล้วใช้ช่องทางการสื่อสารของระบบหรือเครือข่ายในการแพร่กระจายไปยังเครื่องอื่น

มัลแวร์ (Malware) : Virus

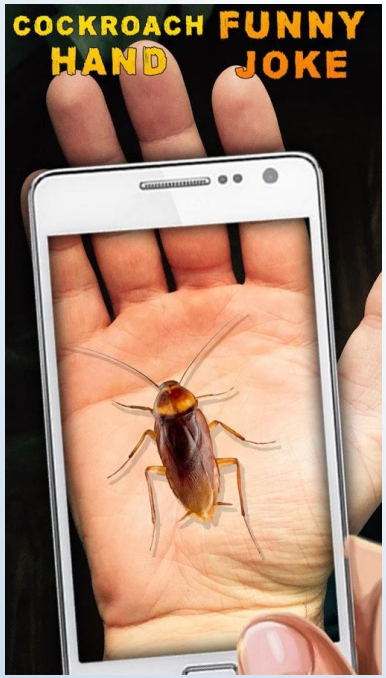
- เป็นมัลแวร์ที่ก็อปปี้ตัวเองให้เป็นส่วนหนึ่งของไฟล์ หรือบูตเซกเตอร์ของดิสก์เพื่อแพร่กระจายตัวเอง
- ไวรัสต้อง**อาศัยพาหะ**ในการกระจายตัวเอง เช่น ไฟล์ อีเมล์ บูตเซกเตอร์บนดิสก์ เป็นต้น
- ไวรัสอาจทำให้ไฟล์ข้อมูลใช้งานไม่ได้ ใช้พื้นที่ในการจัดเก็บ ใช้ทรัพยากรของระบบ และใช้แบนด์วิดธ์ของเครือข่ายในการแพร่กระจายตัวเอง

โปรแกรมที่ไม่จัดเป็นมัลแวร์

- มีโปรแกรมบางประเภทที่ถือว่าเป็นภัยอันตรายแต่ไม่จัดว่าเป็นมัลแวร์ เนื่องจากไม่ได้เขียนมาเพื่อทำลาย แต่อาจสร้างความรำคาญให้แก่ผู้ใช้ อาจกระทบต่อระบบรักษาความปลอดภัย หรือมีมูลค่าความเสียหาเข้ามาเกี่ยวข้อง
- โปรแกรมประเภทนี้ ได้แก่ Joke Application, Hoaxes, Scams, Spam, Spyware, Adware และ Internet Cookies

โปรแกรมที่ไม่จัดเป็นมัลแวร์ : Joke Application

- ออกแบบมาเพื่อสร้างความสนุกสนาน หรือทำให้เสียเวลา
- มีตั้งแต่การแสดงภาพตลกๆ หรือบางครั้งก็เป็นเกมสนุกๆ



โปรแกรมที่ไม่จัดเป็นมัลแวร์ : Hoaxes

- เป็นโปรแกรมที่หลอกให้ผู้ใช้ทำบางอย่างให้ โดยใช้เทคนิคทางวิศวกรรมสังคม
- เช่น การส่งอีเมล์เพื่อหลอกกว่ามีไวรัสตัวใหม่กำลังระบาด และหลอกให้ส่งต่ออีเมล์นี้ไปเรื่อยๆ ทำให้ผู้ใช้เสียเวลา เกิดความรำคาญ หรือตื่นตระหนก


Global Associated News - TOP STORIES

Actor - Tom Cruise Dies In Queensland Australia Car Crash

Like 7.8k Tweet 646

THIS STORY IS STILL DEVELOPING...
December 3, 2013 *30 minutes ago...*
(Local News 9 - Queensland Australia) Actor Tom Cruise died in a single vehicle crash between Ipswich and Willowbank in Queensland as confirmed by Royal Queensland Police - December 3, 2013

BREAKING NEWS

The accident occurred at approximately 5:30 a.m. (UTC/GMT +10). Tom Cruise is believed to have been in the area while on vacation. He was identified by photo ID found at the scene. Alcohol and drugs do not appear to have been a factor in this accident.

The Ipswich - Willowbank connector highway is known to be one of the most dangerous stretches of road in Australia due to road quality conditions and tight curves in the road.

Additional details and information will be forthcoming as they become available.

โปรแกรมที่ไม่จัดเป็นมัลแวร์ : Scams

- คือการใช้ช่องทางการสื่อสารโดยอาชญากรเพื่อพยายามหลอกให้คนอื่นช่วยเหลือตนเองในการทำอาชญากรรมบนอินเทอร์เน็ต
- มีชื่อเรียกอีกชื่อหนึ่งว่า Phishing ซึ่งเป็นการหลอกเอาข้อมูลส่วนตัวจากผู้ใช้ไปทำการที่ผิดกฎหมาย

โปรแกรมที่ไม่จัดเป็นมัลแวร์ : Spam

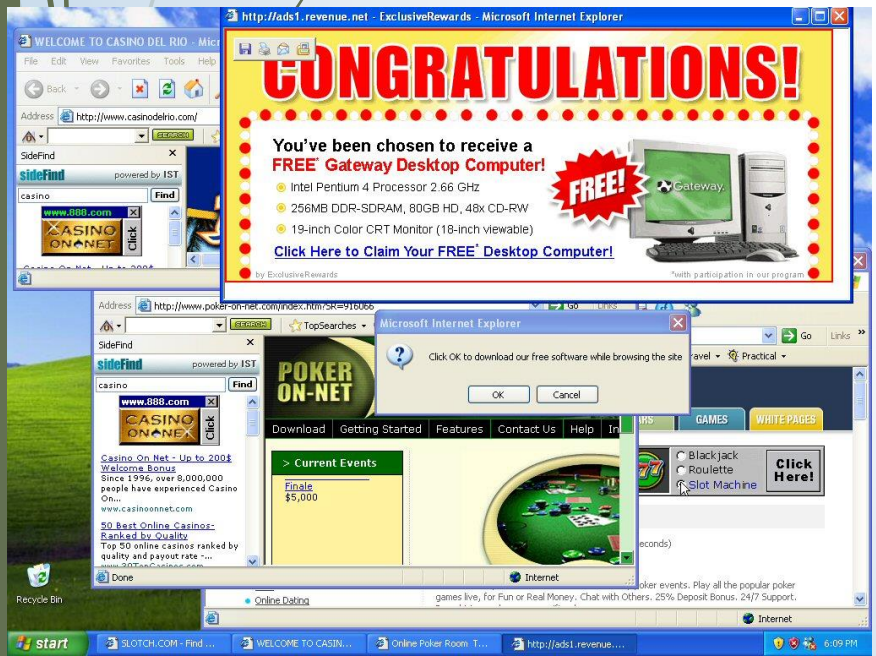
- คือการส่งอีเมลไปยังผู้ใช้จำนวนมาก โดยมีวัตถุประสงค์เพื่อการโฆษณาสินค้าหรือบริการ
- จัดอยู่ในประเภทสิ่งที่ก่อความน่ารำคาญ แต่ไม่ใช่มัลแวร์
- ข้อเสียอย่างร้ายแรงคือการเพิ่มโหลดให้กับเมลเซิร์ฟเวอร์
- ผู้ไม่ประสงค์ดีอาจใช้สแปมเพื่อการกระจายมัลแวร์ได้

โปรแกรมที่ไม่จัดเป็นมัลแวร์ : Spyware

- เป็นโปรแกรมที่ใช้บางอย่างเพื่อลวงตาแต่แอบทำกิจกรรมบางอย่างในคอมพิวเตอร์โดยที่ไม่ได้รับอนุญาตจากผู้ใช้
- เช่น การเก็บข้อมูลส่วนตัวของผู้ใช้ การเปลี่ยนแปลงค่าในเว็บเบราเซอร์
- เทคนิคการหลอกล่อให้ผู้ใช้ติดตั้งสปายแวร์ เช่น ให้คลิกปุ่มบางปุ่มบนป็อปอัพ หรือมาพร้อมกับโปรแกรมที่ให้ดาวน์โหลดได้ฟรี

โปรแกรมที่ไม่จัดเป็นมัลแวร์ : Adware

- เป็นโปรแกรมโฆษณาสินค้าซึ่งจะเปิดป๊อปอัพขึ้นมา ส่วนใหญ่จะอยู่ในฟรีแวร์ ซึ่งจะติดตั้งได้ก็ต่อเมื่อผู้ใช้ยินยอมเท่านั้น จึงไม่ใช่โปรแกรมผิดกฎหมายแต่อย่างใด



โปรแกรมที่ไม่จัดเป็นมัลแวร์ : Internet Cookies

- เป็น Text File ที่เก็บข้อมูลการเข้าชมเว็บไซต์ไว้ที่เครื่องของผู้ใช้เอง เพื่อการเข้าชมครั้งต่อไปจะได้เรียกใช้หน้าเว็บได้อย่างต่อเนื่อง
- แต่ละเว็บไซต์ควรจะเรียกดูคุกกี้จากเว็บตัวเองเท่านั้น ถ้าเว็บไซต์ใดเรียกดูคุกกี้ของเว็บไซต์อื่น อาจจะเป็นการละเมิดสิทธิส่วนบุคคลได้ มีหลายเว็บไซต์ที่พยายามละเมิดการเรียกใช้คุกกี้โดยที่ไม่แจ้งให้ผู้ใช้รู้