# รู้ทันภัยที่มากับอินเตอร์เน็ท

นักเรียนคิดว่าอะไรคือภัยที่มาจาก Internet

E-Mail

Chat

Virus

Cookie

Free ware

# ภัยที่มาจากการใช้งาน อินเตอร์เน็ท และการใช้งานคอมพิวเตอร์

## Malware

- Virus
- Worm
- Trojan

## Non Malware

- Spam mail
- Spyware
- Adware
- Phishing
- Use Internet Application to do crime : chat.....

# ไวรัสมาจากแหล่งใดบ้าง ??

e-mail

www

mp3

LAN,

shares

IM & P2P

Floppy, CD, USB

- Malware: Malicious Software ซึ่งหมายถึง
  - ชุดคำสั่งทางคอมพิวเตอร์ โปรแกรมหรือซอฟต์แวร์ใดๆ ที่ได้รับการจัดทำขึ้นมาโดยมีจุดมุ่งหมายที่จะสร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ อาจมีความสามารถในการเคลื่อนที่จากคอมพิวเตอร์หนึ่งไปยังอีกเครื่องหนึ่งหรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่งได้ด้วยตัวเอง รวมถึง ไวรัส, เวอร์ม, โทรจัน

- Virus
  - โปรแกรมที่สร้างปัญหาและก่อให้เกิดความเสียหายต่างๆ กับเครื่องคอมพิวเตอร์ สามารถแพร่กระจาย โดยต้องอาศัย file เป็นสื่อกลาง เพื่อเกาะติดไป เช่น file type ที่เป็น exe, txt, jpg, bmp, avi, dat ... etc.
  - แพร่กระจายตัวเองจากไฟล์หนึ่งไปยังไฟล์อื่นๆ ภายในเครื่องคอมพิวเตอร์
  - ไม่สามารถแพร่กระจายข้ามเครื่องคอมพิวเตอร์ได้ด้วยตัวเอง ซึ่งการที่ไวรัสคอมพิวเตอร์สามารถแพร่กระจายข้ามเครื่องคอมพิวเตอร์ได้นั้นมี สาเหตุมาจากการที่ผู้ใช้นำไฟล์ที่มีไวรัสคอมพิวเตอร์ไปใช้บนเครื่องคอมพิวเตอร์อื่นๆ เช่น USB thumb drive หรือ USB flash drive สื่อบันทึกข้อมูลต่างๆ ที่มีไฟล์ของไวรัสคอมพิวเตอร์ฝังตัวอยู่มาใช้งาน เป็นต้น

# ข้อใดคือภัยที่มาจาก Internet

เทคโนโลยีใหม่ๆ

ข้อมูลสารสนเทศ

ไวรัสอินเตอร์เน็ต

Chat (IM)

# การป้องกันและกำจัด

**<u>กรณีที่ 1. ยังไม่มีไวรัสติดในเครื่องคอมพิวเตอร์</u>**

- ติดตั้งโปรแกรมป้องกันไวรัส และกำหนดฟังชั่นการทำงานให้ครบถ้วน
- Update signature ใหม่ๆอยู่เสมอเพื่อเป็นภูมิคุ้มกันข้อมูล
- Clear temp file บ่อยๆ

* หมายเหตุ : ความแตกต่างของโปรแกรมป้องกันไวรัส แต่ละ Brand วัดกันที่ ความเร็วในการพิสูจน์ไวรัสใหม่ ได้มากกว่าและเร็วกว่า รวมทั้งการใช้ทรัพยากรของเครื่อง

# กรณีที่ 2. ไวรัสติดในเครื่องคอมพิวเตอร์แล้ว

- ขึ้นอยู่กับประเภทไวรัส และสายพันธุ์
- ระดับของความรุนแรง และความเสียหาย
- ระดับเล็กน้อย ใช้โปรแกรมป้องกันไวรัส กำจัด
- ระดับรุนแรง ต้องใช้ Remove Tool ทำการกำจัด และซ่อมแซมส่วนที่เสียหาย
- การใช้ Remove Tool ต้องเลือกให้ถูกสายพันธ์ไวรัส

* หมายเหตุ : ความแตกต่างของ Remove Tool ของแต่ละ Brand วัดกันที่ ความครบถ้วนในการซ่อมแซมส่วนที่ซึกหรอได้มากกว่ากัน

# วิธีการกำจัดไวรัสคือการ Format ใช่หรือไม่

ใช่.. ต้อง Format เท่านั้น

ไม่ใช่... ใช้โปรแกรมฆ่าไวรัสสิ

# Worm

- เป็นไฟล์ที่ขยายตัวมันเองได้ ในการแพร่กระจาย
- ไม่ต้องอาศัย file อื่นเป็นสื่อกลาง หรือพาหะ
- แพร่กระจายผ่านทาง internet และ network
- ส่งตัวมันเองผ่านทาง e-mail ใน address book ต่อไปเรื่อยๆ หรือแพร่โดยการ share file
- ไม่แพร่เชื้อไปติดไฟล์อื่น แต่จะแอบเปลี่ยนชื่อไฟล์เพื่อหลอกผู้ใช้งาน
- เป็นไฟล์โดยตัวมันเอง (body)

# การป้องกันและกำจัด

## กรณีที่ 1. ยังไม่มี Worm ติดในเครื่องคอมพิวเตอร์

- ติดตั้งโปรแกรมป้องกันไวรัส และกำหนดฟังชั่นการทำงานให้ครบถ้วน
- Update signature ใหม่ๆอยู่เสมอเพื่อเป็นภูมิคุ้มกันข้อมูล
- Clear Internet Temp file และ Windows Temp file

## กรณีที่ 2. ติด Worm ในเครื่องคอมพิวเตอร์แล้ว

- ต้องใช้ Remove Tool เท่านั้น เช่น Brontok เป็นต้น

คุณสมบัติของ Worm คือสามารถเพิ่มจำนวนไปเรื่อยๆ ใช่หรือไม่

ใช่.... ฉันเพิ่มจำนวนตัวเองได้

เปล่า... ฉันเพิ่มจำนวนตัวเองไม่ได้

# Trojan

- โปรแกรมจะบรรจุด้วยโค๊ดที่หลบซ่อนอยู่ และมันจะทำงานเมื่อเครื่องทำงาน
- โปรแกรมจะถูกส่งไปหาผู้ใช้อื่นๆในรูปแบบของไฟล์แนบไปกับอีเมล์ โดยจะหลอกผู้ใช้ให้เปิดอ่าน เช่น การ์ดอวยพร หลอกให้ผู้ใช้เปิดอ่าน แล้วมันจะเข้าไปควบคุมหรือเก็บข้อมูลของเครื่อง หรือเรียกว่า spy
- ทำให้เครื่องทำงานช้าลง

# การป้องกันและกำจัด

## กรณีที่ 1. ยังไม่มี Trojan ติดในเครื่องคอมพิวเตอร์

- ติดตั้งโปรแกรมป้องกันไวรัส และกำหนดฟังชั่นการทำงานให้ครบถ้วน
- Update signature ใหม่ๆอยู่เสมอเพื่อเป็นภูมิคุ้มกันข้อมูล
- Clear Internet Temp file และ Windows Temp file

## กรณีที่ 2. ติด Trojan ในเครื่องคอมพิวเตอร์แล้ว

- ต้องใช้ Remove Tool เท่านั้น เช่น Trojan.Clicker.Qhost.A เป็นต้น

การแก้ไขปัญหาคอมพิวเตอร์ที่ติด Trojan คือ

ใช้โปรแกรมป้องกันไวรัส

ใช้ Remove Tools

# Non Malware.

- Non-Malware : ก่อความรำคาญ
  - Spam mail : จดหมายโฆษณา, จดหมายขยะ
    - มี เยอะๆ Server H/D ไม่พอ

BookHerb - Central European (Windows)

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

**From:** Sex Geocodes
**Date:** 3 กรกฎาคม 2549 10:28
**To:** info@amphonet.com
**Subject:** BookHerb

**Need some love pills?**

*So, why go to your local drugstore? Why waste time and extra money?*
*Why let people know about your intimate life?*
Evil-wishers are always around to spread rumors.
We give you the issue! Make a quick, secure and **ABSOLUTELY CONFIDENTIAL** purchase online and receive your **LICENSED** love life enhancer right to your door!

**No privacy exposure, no time wasted, no exorbitant prices! Start a super life now!**

| | |
|---|---|
| Cialis Soft Tabs - $5.78 | Viagra Professional - $4.07 |
| Viagra Soft Tabs - $4.1 | Cialis - $5.67 |
| Valium - $2.85 | Generic Viagra - $3.5 |
| Xanax - $2.54 | Tamiflu - $3.78 |
| Soma - $1.22 | Ambien - $2.86 |
| Human Growth Hormone - $43.37 | Meridia - $3.32 |
| Tramadol - $1.8 | Levitra - $11.97 |

# Non Malware.

- Non-Malware : ก่อความรำคาญ
  - Hoax : จดหมายหลอกลวง เป็นจดหมายลูกโซ่

CONGRATULATIONS !!! . - Turkish (ISO)

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

**From:** europrimitiva
**Date:** 1 กรกฎาคม 2549 18:39
**To:** none
**Subject:** CONGRATULATIONS !!! .

LA PRIMITIVA ESPAÑOL
INTERNATIONAL DEPARTMENT,
Guzman El Bueno137, 28003
Madrid, España.

REF Nº: ES-0415-2006/MAD.
BATCH Nº: ES-0006997-EU.

The Spanish Lottery board wishes to inform the beneficiary to this email address the results of the email address ballot lottery international program held on 15th of April. 2006. Your email account have been picked as a winner of a lump sum pay out of EURO € 502,185 (FIVE HUNDRED AND TWO THOUSAND, ONE HUNDRED AND EIGHTY FIVE EUROS) in cash credited to file REF Nº: ES-0415-2006/MAD.

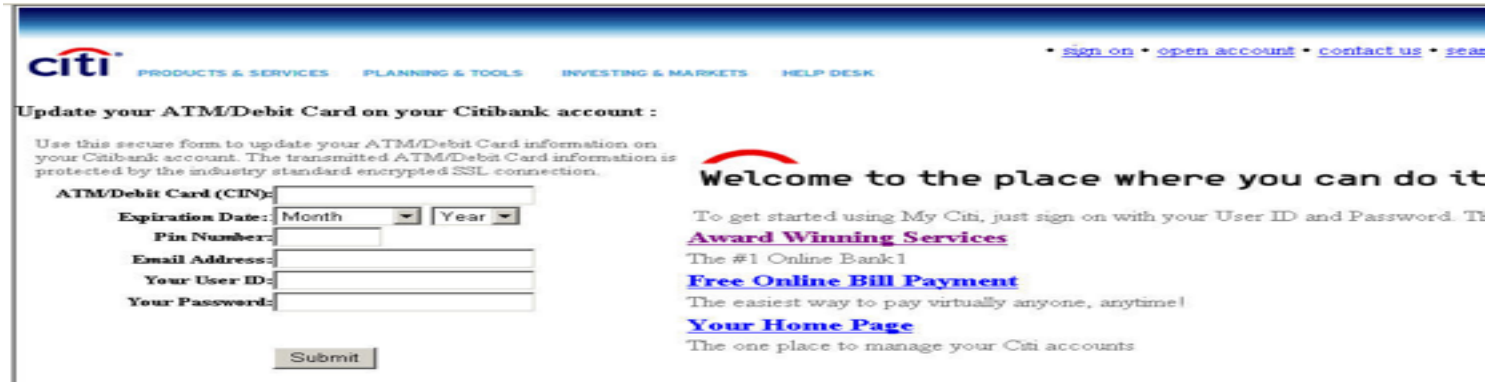
All participants for the online version were selected randomly from World Wide Web through computer balloting system drawn from over 100,000 names database, union
associations and corporate bodies that are listed online. This promotion is this year Spanish Easter Bonanza International Lottery Program of LA PRIMITIVA ESPAÑOL INTERNATIONAL LOTTERY.

# Non Malware.

- Non-Malware : ก่อความรำคาญ
  - Spyware/Adware :  Windows pop-up โฆษณาขายของ

# Non Malware.

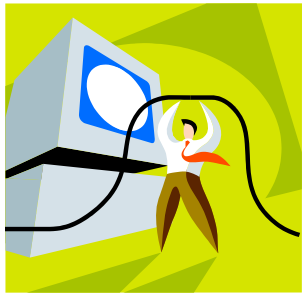
- Non-Malware : ก่อความรำคาญ
  - Phishing : การปลอมแปลงอี-เมล์ และทำการสร้างเว็บไซต์ปลอมที่มีเนื้อหาเหมือนกับเว็บไซต์ของจริงและมี Address ใกล้เคียงกับเว็บไซต์จริง เพื่อทำการหลอกลวงให้เหยื่อหรือผู้รับอี-เมล์เปิดเผยข้อมูลทางด้านการเงิน ,หมายเลขบัตรเครดิต บัญชีผู้ใช้ (Username) และ รหัสผ่าน (Password) หมายเลขบัตรประจำตัวประชาชน หรือข้อมูลส่วนบุคคลอื่นๆ



# การวินิจฉัยอาการ : Overall effects.

- อาการของเครื่องที่ติดไวรัส : Overall effects

1. เมื่อไวรัสฝังตัวในหน่วยความจำ (Memory resident program)
    - ฝังตัวในหน่วยความจำหลัก
    - คอยทำงานเมื่อ เขื่อนไขการทำงาน ตรงกับที่ไวรัสกำหนดไว้ เช่น
        - ไวรัส Nyxim ทำงานทุกวันที่ 3 ของเดือน
    - จะปรากฏ โปรแกรมที่ run ใน Task Manager (กด Ctrl-Alt-Del)
    - หาก Delete อาจจะเกิด อาการข้างเคียง
        - Blue Screen
        - Restart Windows



# การวินิจฉัยอาการ : Overall effects.

2. สร้าง Process หลอกลวง (Spoof)

- ตรวจเช็ค ใน Task Manager
- ใช้ชื่อที่คล้ายกับ Process จริง เช่น
  - WSOCK32.DLL สร้าง Process หลอก เป็น WSOCK33.DLL
  - KERNEL32.DLL สร้าง Process หลอก เป็น KERNE132.DLL

# การวินิจฉัยอาการ : Overall effects.

3. มีการกระจายตัวเอง (Spread)

- ด้วยการส่ง e-mail
- ด้วยการ Share file
- ส่งข้อมูลเข้า-ออก ในระบบเครื่อข่าย
- Virus จะแพร่กระจายโดยอาศัยสื่อกลาง และจะต้องมีการ execute เช่น แฟ้มข้อมูล word, excel, exe, รูปภาพ
- Trojan , Worm จะแพร่กระจายโดยไม่อาศัยสื่อกลาง เช่น
  - ถูกส่งทาง e-mail หากผู้ใช้เปิดอ่าน ก็จะเริ่มทำงาน

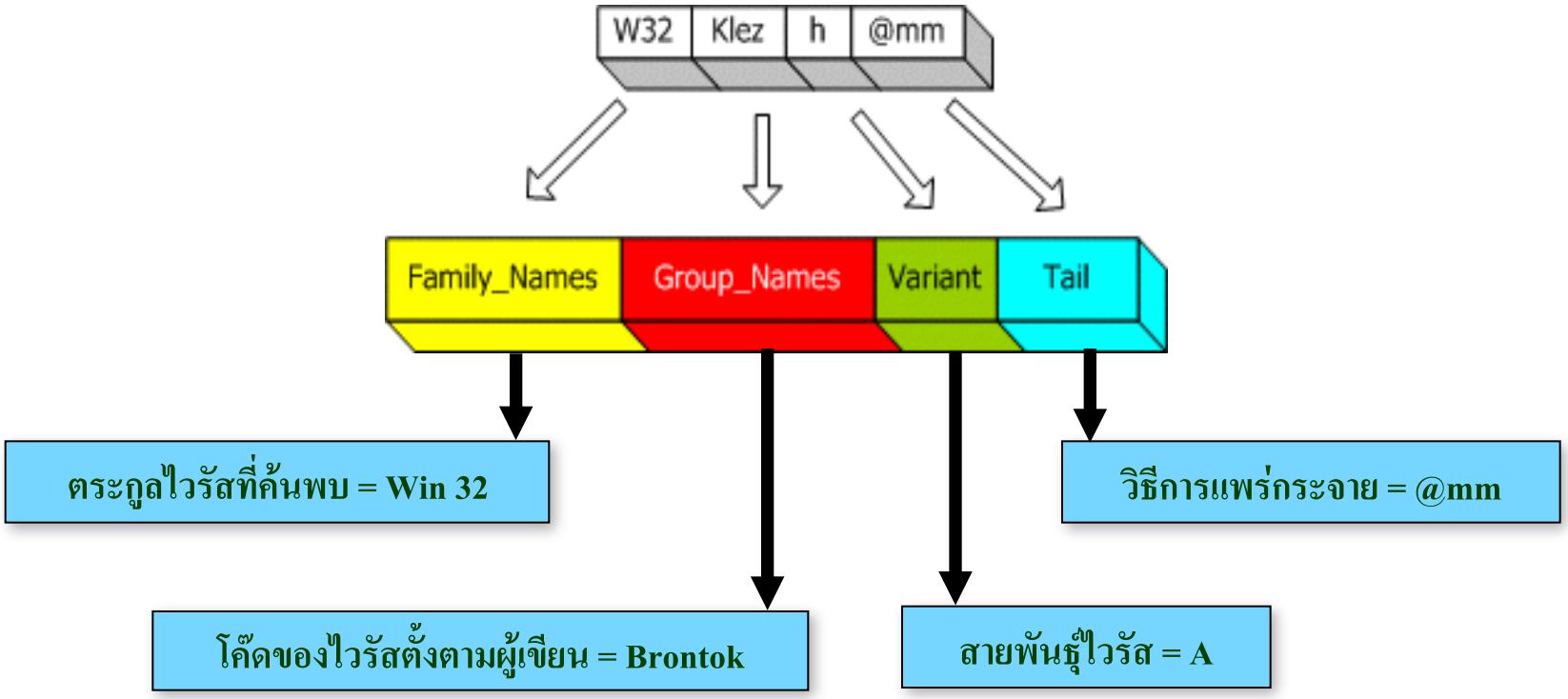
# การวินิจฉัยอาการ : Overall effects.

4. แก้ไขระบบทะเบียนของ Windows (Registry)
    - เพิ่มค่าใน Registry ผลทำให้ โปรแกรมไวรัสถูกเรียกทำงานแน่นอน
    - เปลี่ยนแปลงค่าใน Registry ทำให้ไม่สามารถเรียกทำงานบางโปรแกรมได้
5. สร้างโปรแกรมใน Start Up
    - กำหนดตำแหน่งให้ โปรแกรมทำงานที่ system.ini , win.ini

# การวินิจฉัยอาการ : Overall effects.

6. เครื่องคอมพิวเตอร์ทำงานช้า (Slow performance)
    - เพราะมีการสร้างโปรแกรมที่ทำงานเพิ่ม
    - ใช้หน่วยความจำสูง
    - สร้างข้อมูลเพิ่มใน Hard Disk
7. อื่นๆ
    - Keyboard error
    - อื่นๆ

# การเรียกชื่อไวรัส



# มี Antivirus Software แล้ว ทำไมต้องมี Remove tools ?.

- Antivirus Software's function
  - ป้องกัน Malware
  - พิสูจน์ Malware
  - กำจัด Malware Body
- Remove tool's function
  - กำจัด Malware เฉพาะสายพันธ์
  - ซ่อมแซมระบบส่วนที่เสียหาย

# การป้องกัน Malware

| Malware | ป้องกันโดย |
|---|---|
| Computer Virus | Antivirus |
| Internet Worm | Antivirus |
| Trojan | Antivirus |
| Expoit | Antivirus |
| Spy ware, Ad ware and Hack | AntiSpyware and Firewall |
| Hoax, phishing and Spam Mail | AntiSpam |
| Sex , Game, Gamble Website | Parental Control : Internet Security |
| Internet Using | Internet Security |

# คุณสมบัติของ Virus คือข้อใด

เพิ่มจำนวนได้ด้วยตัวเอง

เป็นโปรแกรมที่มีโค้ดซ่อนอยู่

แพร่กระจายโดยอาศัย File เป็นสื่อ

ก่อความรำคาญ

ข้อใดไม่ใช่การป้องกันเครื่องให้ปลอดภัย
จาก Virus ,Trojan, Malware

Update signature อยู่เสมอ

ใช้โปรแกรมสแกนไวรัส

ใช้ Remove Tools

เคลียร์ Temp File บ่อยๆ