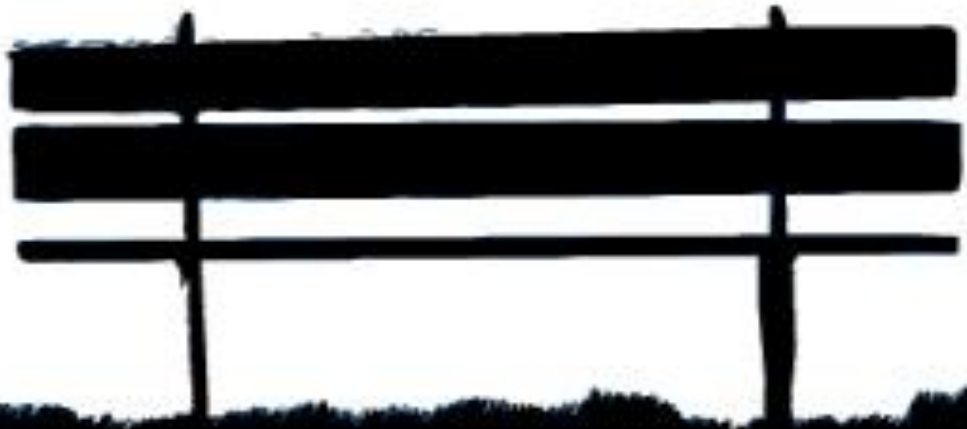
STUXNET

Stuxnet (Win32/Stuxnet) Virus Threat



237211

COMPUTER NETWORKING FOR EDUCATION

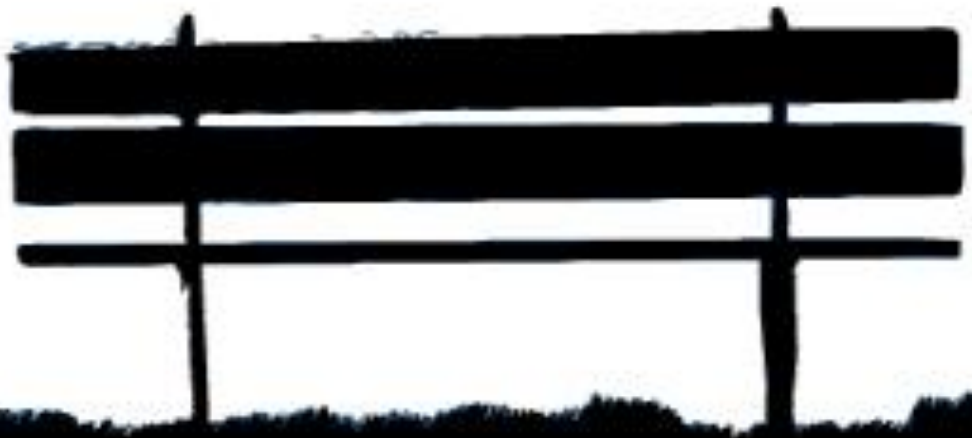
STUXNET

Stuxnet (Win32/Stuxnet) Virus Threat

SMP BOOK Editor

นายณัฐภัทร ปานทอง 533050182-7
นายนาวิน ชัยไธสง 533050200-1
น.ส.อลิษา ผลสมหวัง 533050211-6

สาขาคอมพิวเตอร์ศึกษาชันปีที 2
คณะศึกษาศาสตร์
มหาวิทยาลัยขอนแก่น



237211

COMPUTER NETWORKING FOR EDUCATION

INTRODUCTION

คู่มือการป้องกันไวรัส Stuxnet เล่มนี้ กลุ่มข้าพเจ้าได้เรียบเรียบเนื้อหาขึ้นเพื่อประโยชน์ในการศึกษาค้นคว้า สำหรับนักษาที่เรียนในรายวิชา 237211 เครือข่ายคอมพิวเตอร์เพื่อการศึกษา ตลอดท่านที่สนใจวิชานี้ ทุกท่านได้อ่านศึกษาหาความรู้

หวังว่า คู่มือเล่มนี้คงเป็นประโยชน์ในการศึกษาค้นคว้าของนักศึกษา และผู้สนใจ หากมีข้อผิดพลาดประการใดผู้เรียบเรียงยินดีและพร้อมที่จะรับข้อเสนอแนะ เพื่อจะได้นำไปปรับปรุงแก้ไขในโอกาสต่อไป และขอขอบคุณที่มีส่วนช่วยให้รายงานเล่มนี้สำเร็จด้วยดี

คณะผู้จัดทำ

CONTENT

Page

STUXNET VIRUS

Stuxnet คืออะไร
What's Stuxnet

รายละเอียดทางเทคนิค
Technical Information

อาการ
Symptoms

วิธีการป้องกัน
How to Prevent

วิธีการแก้ไข
How to Solve

WHAT'S STUXNET?

Stuxnet คืออะไร?

ไวรัส Stuxnet โจมตี Windows ผ่านช่องโหว่ความปลอดภัยของ Windows Shell Win32/Stuxnet หรือ Stuxnet เป็นมัลแวร์แบบหลายคอมโพเนนต์ (Multi-component)คือเป็นทั้งประเภท โทรจัน (Trojan) และเวิร์ม (Worm) มีการค้นพบครั้งแรกเมื่อ 16 กรกฎาคม 2553 ที่ผ่านมา เป็นมัลแวร์ที่โจมตี Windows ผ่านช่องโหว่ความปลอดภัยของ Windows Shell (มีกระทบกับ Windows ทุกเวอร์ชัน) ซึ่งไมโครซอฟท์ได้ออกอัปเดทหมายเลข MS10-046 เป็นกรณีพิเศษเพื่อปิดช่องโหว่นี้เมื่อวันที่ 3 สิงหาคม 2553 ตามรายละเอียดในไมโครซอฟท์ออกแพตช์ MS10-046 เป็นกรณีเร่งด่วนเพื่อแก้ปัญหาช่องโหว่ความปลอดภัย Windows

WHAT'S STUXNET?

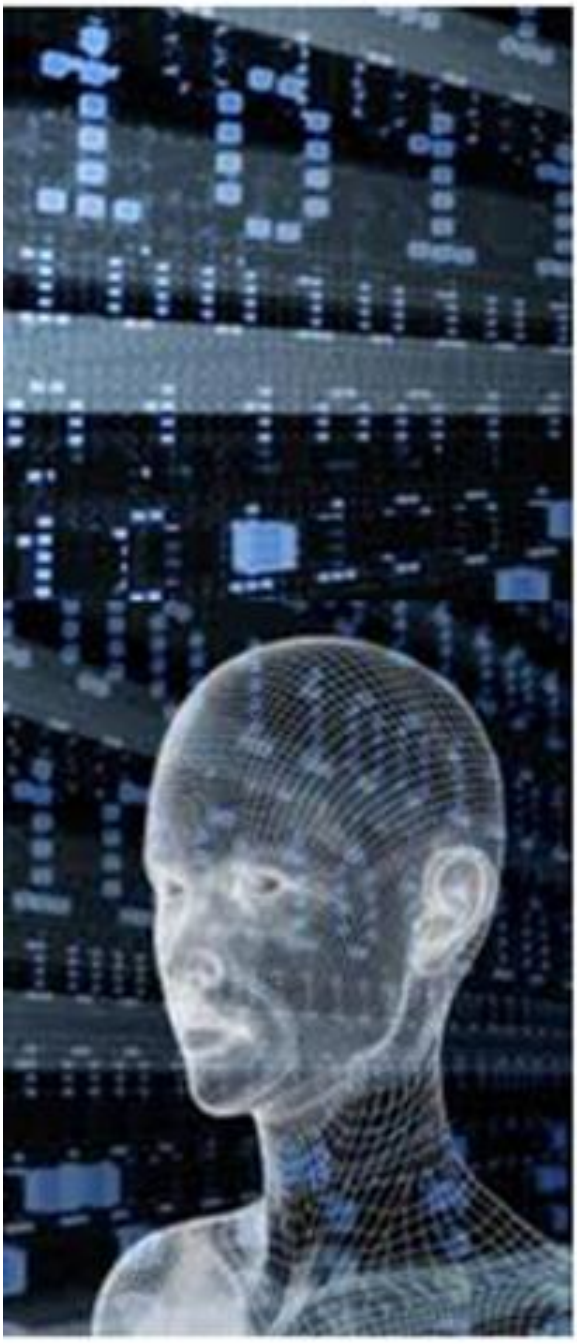
Stuxnet สามารถทำการติดตั้งและดร็อปคอมโพเนนต์ ทำการฉีดโค้ด (Injecting code) เข้าสู่โปรเซสระบบที่กำลังทำงานอยู่เพื่อสร้างช่องทางให้แบ็คดอร์ใช้ในการเข้าถึงและควบคุมเครื่องคอมพิวเตอร์ที่ติดไวรัส

หมายเหตุ: McAfee ระบุว่าเป้าหมายการโจมตีของ Stuxnet คือระบบที่รันซอฟต์แวร์WinCC SCADA

ประเภท (Type): Trojan
ประเภทรอง (SubType): Worm
ชื่ออื่นๆ (Aliases): Stuxnet
ระดับการเตือนภัย (Alert Level): Severe

TECHNICAL INFORMATION

รายละเอียดทางเทคนิค ;



Stuxnet เป็นมัลแวร์แบบหลายคอมโพเนนต์ มีการแพร่ระบาดผ่านทางอุปกรณ์เก็บข้อมูลแบบพกพาโดยอาศัยช่องโหว่ความปลอดภัยของ Windows Shell เมื่อเวิร์ม Stuxnet ถูกทำการรันมันจะทำการดร็อปไฟล์ชอร์ตคัท(.Lnk) ที่มีการฝังโค้ดอันตราย (Malicious shortcut) ลงในไดรฟ์อุปกรณ์เก็บข้อมูลแบบพกพา เมื่อมีการใช้งานไดรฟ์ดังกล่าวจากโปรแกรมแอพพลิเคชันที่ทำการแสดงไอคอนของชอร์ตคัท (เช่น Windows Explorer) ถ้าคอมพิวเตอร์เครื่องดังกล่าวมีช่องโหว่ความปลอดภัยWindows Shell ก็จะทำให้ไฟล์ชอร์ตคัทถูกรันโดยอัตโนมัติในทันที สำหรับไฟล์ชอร์ตคัทที่เวิร์ม Stuxnet ดร็อปลงในเครื่องนั้นโปรแกรมป้องกันไวรัสจะตรวจพบในชื่อ Exploit:Win32/CplLnk.A

TECHNICAL INFORMATION

Stuxnet นั้นมีหลายคอมโพเนนต์ ได้แก่

- TrojanDropper:Win32/Stuxnet เป็นคอมโพเนนต์ที่ทำหน้าที่ดร็อปและติดตั้งคอมโพเนนต์ต่างๆ ของ Stuxnet
- Trojan:WinNT/Stuxnet เป็นไดรเวอร์คอมโพเนนต์ที่ทำหน้าที่โหลด/รันคอมโพเนนต์ที่เป็น Worm:Win32/Stuxnet
- Worm:Win32/Stuxnet เป็นคอมโพเนนต์ที่ทำหน้าที่แพร่กระจายไวรัส

SYMPTOMS

อาการ :

สำหรับเครื่องคอมพิวเตอร์ที่ติดไทรจัน จะมีการเปลี่ยนแปลงระบบดังนี้

- มีไฟล์ shortcut (.lnk) อยู่ในไดรฟ์เก็บข้อมูลแบบพกพา
- มีไฟล์ดังนี้อยู่ในเครื่อง

- ~WTR4132.tmp
- %System%\drivers\mrxcls.sys
- %System%\drivers\mrxnet.sys
- %Windir%\inf\mdmcpq3.PNF
- %Windir%\inf\mdmeric3.PNF
- %Windir%\inf\oem6C.PNF
- %Windir%\inf\oem7A.PNF

SYMPTOMS

- มีการแก้ไขรีจีสทรีย์ดังนี้
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxCls
  - Description: "MRXCLS"
  - DisplayName: "MRXCLS"
  - ErrorControl: 0x00000000
  - Group: "Network"
  - ImagePath: "%system%\Drivers\mrxcls.sys"
  - Start: 0x00000001
  - Type: 0x00000001
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxCls\Enum
  - 0: "Root\LEGACY_MRXCLS\0000"
  - Count: 0x00000001
  - NextInstance: 0x00000001

SYMPTOMS

- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxNet
  - Description: "MRXNET"
  - DisplayName: "MRXNET"
  - ErrorControl: 0x00000000
  - Group: "Network"
  - ImagePath: "%system%\Drivers\mrxnet.sys"
  - Start: 0x00000001
  - Type: 0x00000001
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxNet\Enum
  - 0: "Root\LEGACY_MRXNET\0000"
  - Count: 0x00000001
  - NextInstance: 0x00000001

How to Prevent

วิธีการป้องกัน Stuxnet

ทำการติดตั้งอัปเดทหมายเลข MS10-046 และเพื่อเพิ่มระดับความปลอดภัยในการป้องกันการโจมตีจากไวัส แนะนำให้ดำเนินการ ดังนี้

- เปิดใช้งาน Firewall
- ทำการอัปเดทวินโดวส์และซอฟต์แวร์ต่างๆ ให้เป็นอัปเดทล่าสุดเสมอ
- ทำการอัปเดทโปรแกรมป้องกันไวรัส
- จำกัดจำนวนผู้ใช้ที่มีสิทธิพิเศษบนเครื่องคอมพิวเตอร์
- ใช้ความระมัดระวังเป็นพิเศษในการเปิดไฟล์ที่แนบมากับอีเมลหรือไฟล์ที่ได้จากอินเทอร์เน็ต
- ใช้ความระมัดระวังเป็นพิเศษในคลิกลิงก์ที่แนบมาทางอีเมล
- หลีกเลี่ยงการดาวน์โหลดซอฟท์แวร์ผิดกฎหมาย
- ระมัดระวังและปกป้องตนเองจากการโจมตีด้วยวิธีการวิศวกรรมทางสังคม (social engineering)
- ใช้รหัสผ่านที่มีความแข็งแกร่งยากต่อการคาดเดา

How to Solve

วิธีการแก้ไข Stuxnet

สามารถกำจัดWin32/Stuxnet
โดยการสแกนด้วยโปรแกรมป้องกันไวรัส เช่น
Microsoft Security Essentials,
AVG Anti-Virus Free Edition,
Avast! Free Antivirus
ทั้งนี้ให้ทำการอัปเดทไวรัสเดฟินิชันให้เป็นเวอร์ชัน
ใหม่ล่าสุดก่อนทำการสแกน

REFERENCE

Thai Windows Administrator Blog. 2010.

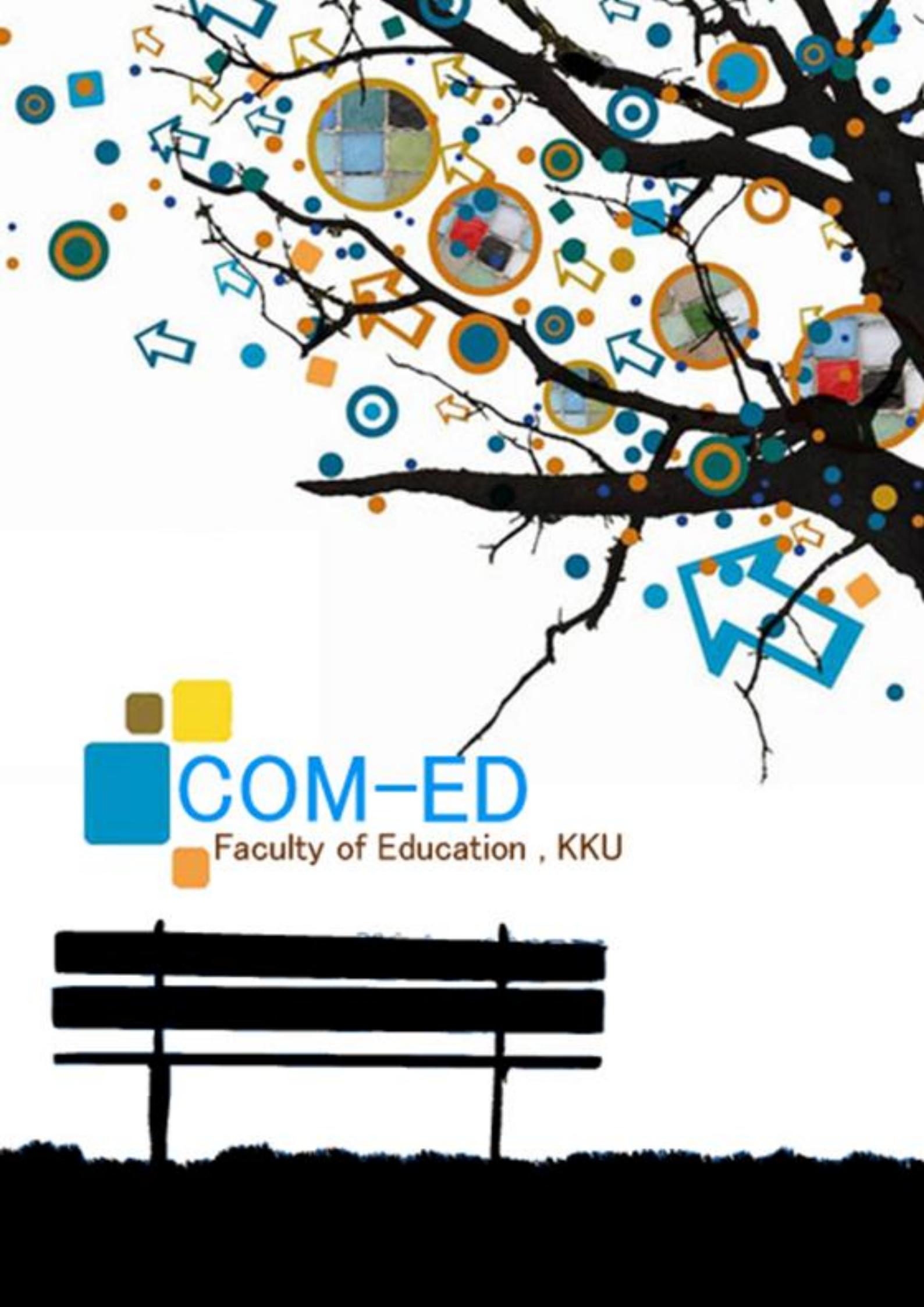
ค้นเมื่อ 25 กันยายน 2554, จาก

http://linuxunix54321.tripod.com/Linux03.htm.

SMP-graffic

บริการ ตกแต่งภาพ ออกแบบกราฟฟิก โลโก้
ออกแบบป้ายโฆษณา นอร์ดงาน หนังสือออนไลน์
เว็บไซต์ ออกแบบงานนำเสนอรูปแบบต่าง ๆ
เพาเวอร์พอยต์ ,ฟันสิชเชอร์ ออกแบบแผ่นฝัน นามบัตร ไนซ์ชวร์

ติดต่อ : Tell 080-7812091
Email ; Panna_sirisit@hotmail.com
Facebook ; Poko At Kku ComED


COM-ED
Faculty of Education , KKU